1. Alice sends two standard transactions to Bob, generating one-time tx-keys: $P_2 = \mathcal{H}_s(r_1 A)G + B$ and $P_1 = \mathcal{H}_s(r_2 A)G + B$.

2. Bob recovers corresponding one-time private tx-keys x_1 and x_2 and spends the outputs with valid signatures and images keys $I_1 = x_1 G_2$ and $I_2 = x_2 G_2$.

3. Now Alice can link these signatures, checking the equality $I_1 - I_2 \stackrel{?}{=} (\mathcal{H}_s(r_1 A) - \mathcal{H}_s(r_2 A))G_2$.

The problem is that Alice knows the linear correlation between public keys P_1 and P_2 and in case of fixed base G_2 she also gets the same correlation between key images I_1 and I_2. Replacing G_2 with $\mathcal{H}_p(xG_2)$, which does not preserve linearity, fixes that flaw.

For constructing deterministic $\mathcal{H}_p$ we use algorithm presented in [37].