$[(g_1',h_1'), \ldots, (g_{n-1}',h_{n-1}')]$ $[(g_1",h_1"), \ldots, (g_{n-1}",h_{n-1}")]$ Data encryption public key $(g_n^{"},h_n^{"})$ (g_n',h_n') Hybrid headers $AE_{pk}(k2)$ SE_{k2} $AE_{pk}(k1)$ $AE_{pk}(k1)$ Data

Routing keys

SE_{k1}(Data)

AE = Asymmetric Encryption
pk = data encryption public key

SE_{k2} SE_{k1}(Data)

SE = Symmetric Encryption
k# = ephemeral symmetric keys