HD Wallets (BIP32)

D_G = Group or Der

H = HMAC-SHA512
p = parent
c = child
S = Secret
P = pub key = G ⊛ S

Priv → Priv (normal)

① $I_{64} = H(\underbrace{chainCode_{par}}_{\text{Key}}, 0 \,||\, P_p \,||\, idx)$

② $I_{64} = I_{H32} \,||\, I_{L32}$ (split I_{64})

$S_c = I_L + S_p \pmod D$

$P_c = G \circledast S_c$

★ $P_c = G \circledast (I_L + S_p) \pmod D$

$P_c = G \circledast I_L + G \circledast S_p$

$P_c = G \circledast I_L + P_{par}$

Pub → Pub (normal)

① $I_{64} = H(chaincode_{par}, P_p \,||\, idx)$

② $P_c = G \circledast I_L + P_{par}$

★ Elliptic curve homomorphic property

$A \circledast G \oplus B \circledast G = (A + B) \circledast G$