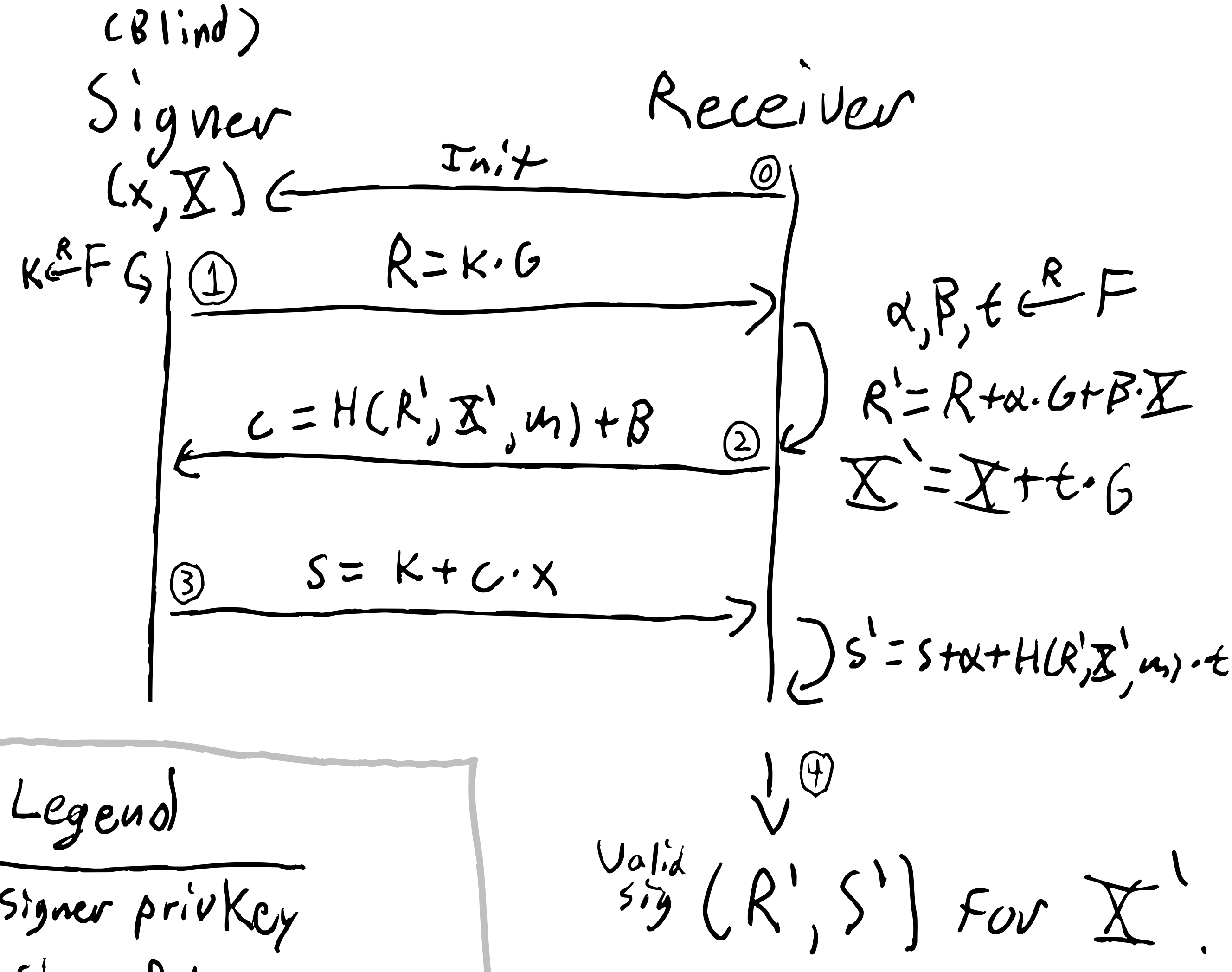
Blind Schnorr Signatures


(Blind)
Signer
Receiver
$(x, \underline{X})$
Init
0
$K \xleftarrow{R} F_G$
1
$R = K \cdot G$
$\alpha, \beta, t \xleftarrow{R} F$
$R' = R + \alpha \cdot G + \beta \cdot \underline{X}$
$\underline{X}' = \underline{X} + t \cdot G$
$c = H(R', \underline{X}', m) + \beta$
2
3
$s = K + c \cdot x$
$s' = s + \alpha + H(R', \underline{X}', m) \cdot t$
4
Valid sig $(R', S']$ for $\underline{X}'$.

Legend

x - Signer privKey

$\underline{X}$ - Signer Pubkey

(K,R) - Signer Nonce

α - nonceTweak

β - challengeTweak

t - keyTweak

$\underline{X}'$ - tweakedPubKey

R' - tweakedNonce

c - (blinded) message hash

s - (blinded) signature

s' - unblinded signature

Code Events (in Order)

Receiver inits

Signer generates and sends nonce

Receiver calls BlindingTweaks.freshBlindingTweaks

Receiver calls generateChallenge and sends it

Signer calls generateBlindSig and sends it

Receiver calls unblindSignature

Done :)