

$$k_1 = s_1^{-1} (h_1 + a r_1) \bmod q$$

$$2k_1 = s_2^{-1} (h_2 + a r_2) \bmod q$$

$$0 \equiv s_2^{-1} (h_2 + a r_2) - 2s_1^{-1} (h_1 + a r_1) \bmod q$$

$$0 \equiv (s_2^{-1} h_2 + s_2^{-1} a r_2 - 2s_1^{-1} h_1 - 2s_1^{-1} a r_1) \bmod q$$

$$-(s_2^{-1} h_2 - 2s_1^{-1} h_1) \equiv a(s_2^{-1} r_2 - 2s_1^{-1} r_1) \bmod q$$

$$a \equiv ((-s_2^{-1} h_2 + 2s_1^{-1} h_1)(s_2^{-1} r_2 - 2s_1^{-1} r_1)) \bmod q$$