

$$k = \text{random} \in [1, q)$$

$$r = (g^k \bmod p) \bmod q$$

$$s = k^{-1} (H(M) + \textcolor{red}{x}r) \bmod q$$

$$\textit{Sign}(\textcolor{red}{x}, k, M) = \langle r, s \rangle$$

$$\textit{Verify}(\textcolor{green}{y}, r, s) :$$

$$w = s^{-1} \bmod q$$

$$u_1 = H(M) \cdot w \bmod q$$

$$u_2 = r \cdot w \bmod q$$

$$v = ((g^{u_1} \textcolor{green}{y}^{u_2}) \bmod p) \bmod q$$

$$\text{valid if } v = r$$