Fixed length Hash function :-

→ Let P be a polynomial time algorithm that on input 1^n outputs a cyclic group G of order q (length of q is n) and generator g.

Gen: on input 1^n, run $G(1^n)$ to obtain (G, q, g, h) as the key.

H^s: given a key $s = \langle G, q, g, h \rangle$ ~~as the key~~. and input $(x_1, x_2) \in Z_q \times Z_q$, output $H^s(x_1, x_2) := g^{x_1} h^{x_2}$

Security proof :-

→ If DLP is hard relative to G then the above construction is a fixed length collision resistant hash function.

$$H^s(x_1, x_2) = H^s(x_1', x_2') \Rightarrow g^{x_1} h^{x_2} = g^{x_1'} h^{x_2'} \Rightarrow g^{x_1 - x_1'} = h^{x_2' - x_2}$$

$\Delta \overset{def}{=} x_2' - x_2$

$$g^{(x - x_i)\Delta^{-1}} = \left(h^{x_2' - x_2}\right)^{[\Delta^{-1} \bmod q]} = h^{[\Delta \cdot \Delta^{-1} \bmod q]} = h^1 = h.$$