An application: collision resistance

Choose a group G where Dlog is hard (e.g. $(Z_p)^*$ for large p)

Let q = |G| be a prime. Choose generators g, h of G

For $x,y \in \{1,\ldots,q\}$ define $\boxed{H(x,y) = g^x \cdot h^y}$ **in G**

Lemma: finding collision for H(.,.) is as hard as computing $\text{Dlog}_g(h)$

Proof: Suppose we are given a collision $H(x_0,y_0) = H(x_1,y_1)$

then $g^{x_0} \cdot h^{y_0} = g^{x_1} \cdot h^{y_1} \Rightarrow g^{x_0-x_1} = h^{y_1-y_0} \Rightarrow h = g^{x_0-x_1/y_1-y_0}$ $\neq 0$