Fixed Length collision resistant hash functions:

Hash functions:

Hash function takes an arbitrary length string as input and compresses them into shorter strings. These are used in data structures for improved look-up times in storage/retrieval. For two distinct inputs x and y, the hash function should give different results.

For every $x \neq y$, $H(x) \neq H(y)$.

Collision Resistance:

A collision in Hash function H is a pair of distinct input x and y such that $H(x) = H(y)$. (x and y are collide under H).

A Hash function H is collision resistant if it is infeasible for any probabilistic polynomial time algorithm to find a collision. No polynomial-time adversary should be able to find a distinct pair of values x and y such that $H(x) = H(y)$.

Here we deal with a family of hash functions indexed by s, $H^s(x) = H(s, x)$, and this key is not kept secret. It indicates a particular hash function H^s from the family.

Syntax of Hash function:

A hash function is a pair of probabilistic polynomial time algorithms (Gen, H) which satisfy below points

- Gen takes an input parameter 1^n and outputs a key s
- There exists a polynomial l such that H is polynomial time algorithm that takes an input key s and any string $x \in \{0,1\}^*$ and outputs a string $H_s(x) \in \{0,1\}^{l(n)}$.

Here input length is $l^{\iota}(n)$ > $l^{(n)}$ and we say (Gen ,H) is fixed length hash function with input length l^{ι} .

Constructing fixed length collision resistance hash functions by DLP:

Let G be a polynomial time algorithm that, on input 1^n , outputs a cyclic group Z , its order is q and length of q is n , and a generator g . Here q is prime number and below is the construction of fixed length has function.

Let $\mathcal{G}$ be as described in the text. Define a fixed-length hash function (Gen, H) as follows:

- Gen: on input 1^n, run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$ and then select a uniform $h \in \mathbb{G}$. Output $s := \langle \mathbb{G}, q, g, h \rangle$ as the key.
- H: given a key $s = \langle \mathbb{G}, q, g, h \rangle$ and input $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$, output $H^s(x_1, x_2) := g^{x_1} h^{x_2} \in \mathbb{G}$.

For given $s =< G, q, g, h >$ With $n = |q|$, the function H^s is described as taking elements of Z*Z as input, means input string length is 2.n, if we parse input as $x \in \{0,1\}^{2.n}$ as two strings x_1, x_2 each of length n.

But how to prove above construction is collision resistant?

We will prove by using DLP and if we are able to find collision then we can say **we break DLP.**

Proof of collision resistance:

If the discrete logarithm problem is hard relative to G, then the above construction of fixed length hash function is a collision resistant hash function.

Let us say we found a collision means for x, y where $x \neq y$ means $H(x) = H(y)$ and now parse x as (x_1, x_2) and y as (y_1, y_2).

$$H^s(x_1, x_2) = H^s(y_1, y_2)$$

$$g^{x_1} h^{x_2} = g^{y_1} h^{y_2}$$

$$g^{x_1 - y_1} = h^{y_2 - x_2} \text{ ------ } 1$$

$$\Delta = y_2 - x_2$$

Note that $y_2 - x_2 \neq 0 \; mod \; q$ otherwise, we would have $x_1 = y_1 \; mod \; q$ but then $x = y$, and we wouldn't have a collision. Since q is prime inverse of Δ exists. Lets call it as I and raising each side of equation (1) gives

$$I = (y_2 - x_2)^{-1} mod \; q$$

$$(g^{x_1 - y_1})^I = (h^{y_2 - x_2})^I \rightarrow h^1 = h$$

Because of collision we got 'h' value and DLP is broken which is impossible(hard). So, there is no collision.