

DLP Hash Theory

A collision resistant hash function using DLP can be formulated as follows:

$f(x, y) = g^x \times h^y \mod p$ where g is a primitive root of p , h is another generator from the same cyclic group and p is a prime.

Proof that the above formulation is collision resistant:

Assume that (x_1, y_1) and (x_2, y_2) lead to a collision. Then, $f(x_1, y_1) = f(x_2, y_2)$

That implies that,

$$g^{x_1} \times h^{y_1} \mod p = g^{x_2} \times h^{y_2} \mod p$$

Implies,

$$g^{x_1 - x_2} \mod p = h^{y_2 - y_1} \mod p$$

Assume $h = g^u \mod p$

This implies that $g^{x_1 - x_2 - u \times (y_2 - y_1)} \mod p = 1$, i.e. $g^a \mod p = 1$. This is highly improbable, as g is given to be the primitive root of p .