MIRAJ
Page No.
Date:
www.mirajmulticolour.com

let $H^s(x)$ be the M-D Hash function. To be provably secure, $H^s(x) = H^s(x')$ s.t. $x \neq x'$ should be improbable

let L & L' be the lengths of x & x'

If $L \neq L'$,

the last step transforms for both x & x' will be

$$z_{B+1} = h^s(z_B \| L)$$

$$z'_{B'+1} = h^s(z'_B \| L')$$

since $H^s(x) = H^s(x')$

~~we~~ $h^s(z_B \| L) = h^s(z'_B \| L')$

since $L' \neq L$, we know that $z_B \| L$ & $z'_B \| L$ are different strings. the probability that h^s collides is negligible (DLP hash theorem)

If $L = L'$, $x_{B+1} = x'_{B+1}$

we have $x \neq x'$ & $|x| = |x'|$

so we must have an i such that $x_i \neq x'_i$

Let $i^* \leq B+1$ be the greatest such that

$z_{i^*-1} \| x_{i^*} \neq z'_{i^*-1} \| x'_{i^*}$ & $z_{i^*} = z'_{i^*}$

if $i^* = B+1$

$H^s(x) = H^s(x') \Rightarrow h^s(z_B \| x_{B+1}) = h^s(z'_B \| x'_{B+1})$

$\Rightarrow z_B \| x_{B+1}$ & $z'_B \| x'_{B+1}$ are two different strings for which h collide

improbable because of DLP hash

if $i^* \leq B+1$, i^* be the max index such that $z_{i^*-1} \| x_{i^*} \neq z'_{i^*-1} \| x'_{i^*}$

& $z_{i^*} = z'_{i^*}$

$\Rightarrow h^s(z_{i^*-1} \| x_{i^*}) = h^s(z'_{i^*-1} \| x'_{i^*})$

again these strings are different but h collides. $\Rightarrow$ improbable