Collision Resistance

Let \( H: \{0,1\}^* \rightarrow \{0,1\}^* \)
- Compression function

First attempt:
\[
\forall A, \forall r \left[ x, x' \in \mathcal{U}(1^r) \right] \Pr \left[ x \neq x', H(x) = H(x') \right] \leq negl(\lambda)
\]

Problem: For any fixed function, \( \forall A \) at a collision is hardened

Second:
Decide: choose \( H \) from some family
\( H: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^* \)

\[
\forall A, \forall r \left[ x, x' \in \mathcal{U}(1^r, k) \right] \Pr \left[ x \neq x', H_k(x) = H_k(x') \right] \leq negl(\lambda)
\]

"\( H \) is parameterized by a key \( k \)", \( 2^r \) possible \( k \)

Q. Can we have a PRF that is NOT collision resistant?

Salt:

Let \( S \) be a PRF:

\[
g(k, m) = \text{or } k^t
\]
\[
i f \quad m \neq k \text{ return 0}
\]
This is PRF. A hash function sees "ki" not in PRF game.

**Merkle-Damgard.**

Given $\Sigma_0, \Sigma_3 \xrightarrow{\mathcal{E}} \text{digest}$

We'll try to construct $\Sigma_0, \Sigma_3 \xrightarrow{\mathcal{E}} \text{digest}$

Claim: If $H: \Sigma_0, \Sigma_3 \xrightarrow{\mathcal{E}} \Sigma_0, \Sigma_3$ is col. res. compression then $G_k(x_1, x_2)$ is collision resistant.

**Proof:**

By reduction:

Assume $A$ breaks $G_k$.

we construct $A'$ that breaks $H$.

$A'(x, k)$:

$$x_1 x_2 \ldots x_l \xrightarrow{A} A(1^l, k)$$

$$x'_1 x'_2 \ldots x'_l \neq x_k \text{ but } G_k(x) = G_k(x')$$

**Goal:** Find $x, x'$ such that $H(x) = H(x')$.

**How:** Try $x = G^*(x_1 \ldots x_{l-1}) \| x_l$. 

...
\[ x' = G_i(x_i \ldots x_{i+1}) \mid x \] 

Since \( x_i \neq x'_i \).

Either \( G^i(x_i \ldots x_i) = G^i(x'_i \ldots x'_i) \).

\[
\begin{array}{cccc}
  x_i & x_i' & \cdots \\
  y_i & y_i' \neq y_i & y_i' \neq y_i \\
  x'_i & x'_i' & y_i' \neq y_i'
\end{array}
\]

Let \( i \) be smallest \( x_i \) s.t. \( x_i \neq x'_i \)

Must be some \( i \leq l \)

\( y_i = y_i' \).

\( x'_i, y_{i-1} \neq x'_i, y_{i-1} \).

Could clean up... main idea

is some step in sequence

is collision for \( H \).

Candidate

\[
\begin{align*}
g & \quad \mid y \\
g^{-1} & \quad \mid h \\
g^{-1} & \quad \mid h \\
g^{-1} & \quad \mid y + \log h
\end{align*}
\]