Collision Resistance

Friday, October 29, 2021 3:57 PM

Collision Resistance:

Let $\underline{\mathcal{H}}: \underline{\{0,1\}^{2\lambda}} \rightarrow \{0,1\}^{\lambda}$

- Compression function

First attempt:

$$\forall \mathcal{A}. \Pr\left[\begin{array}{c} x, x' \leftarrow \mathcal{A}(1^\lambda) \\ x \neq x' \quad \mathcal{H}(x) = \mathcal{H}(x') \end{array}\right] \leq \text{negl}(\lambda)$$

Problem. For any fixed function,
$\exists \mathcal{A}$ s.t. a collision is hardcoded.

Second: Idea: chose $\mathcal{H}$ from some family

$\mathcal{H}: \underline{\{0,1\}^\lambda} \times \underline{\{0,1\}^{2\lambda}} \rightarrow \{0,1\}^\lambda$

$$\forall \mathcal{A}. \Pr\left[\begin{array}{c} k \stackrel{\$}{\leftarrow} \{0,1\}^\lambda \\ x, x' \leftarrow \mathcal{A}(1^\lambda, k) \\ x \neq x' \quad \mathcal{H}_{\underline{k}}(x) = \mathcal{H}_k(x') \end{array}\right] \leq \text{negl}(\lambda)$$

"$\mathcal{H}$ is parameterized by a key k" $\quad 2^\lambda$ possible functions

salt

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

Let f be a PRF.

Constr: $\quad g(k, m) =$

or $k+1$

if $m \stackrel{?}{=} k$ return 0

else $f(k, m)$.

This is PRF.

Here Adv sees "K_1"
Not in PRF game.

Bad padding

3 hi 0 00

5 hi 000

padding block

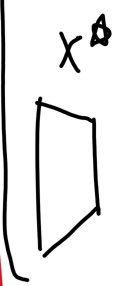
Merkle-Damgard.

given $\{0,1\}^{2\lambda} \to$ digest

we'll show how to construct $\{0,1\}^* \to$ digest (padding)

$\{0,1\}^{\ell \cdot \lambda} \to$ digest

G



Claim: If $H : \{0,1\}^{2\lambda} \to \{0,1\}^\lambda$ is Col. Res. compression

then $G(x_1 .. x_\ell)$ is collision resistant.

parts of message

Proof:

By reduction:

Assume A breaks G,

we construct A' that breaks H.

$A'(1^\lambda, k)$:

$$\underline{x_1 x_2 \ldots x_\ell} \leftarrow A(1^\lambda, k)$$

$$\underline{x'_1 x'_2 \ldots x'_\ell} \qquad \vec{x} \neq \vec{x}' \text{ but } G_k(\vec{x}) = G_k(\vec{x}')$$

Goal: Find some $x \neq x'$

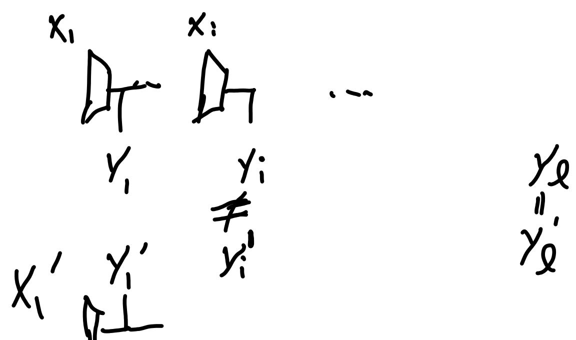
$xy, x'y'$ $\quad H(x) = H(x')$

How: Try $x = G^\circ_k(x_1 .. x_{\ell-1}) \| x_\ell$.

$$x' = \overline{G_k(x_1' \cdots x_{\ell-1}')} \mid x_\ell'$$

Some $x_i \neq x_i'$.

Either $G^\circ(x_1 \dots x_i) = G^\circ(x_1' \dots x_i')$.



Let i be smallest x_i s.t. $x_i \neq x_i'$

Must be some smallest $i < j \le \ell$

$$y_j = y_j'.$$

$$x_j\, y_{j-1} \neq x_j'\, y_{j-1}'.$$

Could clean up... main idea is some step in sequence is collision for H_1

Candidate

$$g^x \mid h^y$$

$$g^{x-1}\, g\, h^y$$

$$g^{x-1}\, h^{y+\log_h g}$$