2021201041
Nvss Maneesh Gupta

Collision Resistant Fixed Hash

Assuming DL is hard to invert, we built fixed length collision resistant hash function.

Lemma: Fix a positive integer N, and say $q \leq \sqrt{2N}$ elements $y_1, \dots, y_q$ are chosen uniformly and independently at random from a set of size N. Then the probability that there exist distinct i, j with $y_i = y_j$ is at least $\frac{q(q-1)}{4N}$. i.e., $coll(q, N) \geq \frac{q(q-1)}{4N}$.

"Smaller the value of q w.r.t N, higher is the collision resistance"

Proof:

PROPOSITION A.4 *For all x with $0 \leq x \leq 1$ it holds that*

$$e^{-x} \leq 1 - \left(1 - \frac{1}{e}\right) \cdot x \leq 1 - \frac{x}{2}.$$

- NoColl_i : Denotes the event of NO COLLISION upto i

$$\Pr[\text{NoColl}_q] = \Pr[\text{NoColl}_1] \cdot \Pr[\text{NoColl}_2 \mid \text{NoColl}_1] \cdots \Pr[\text{NoColl}_q \mid \text{NoColl}_{q-1}].$$

$$\Pr[\text{NoColl}_1] = 1 \qquad \Pr[\text{NoColl}_{i+1} \mid \text{NoColl}_i] = 1 - \frac{i}{N}$$

$$\Pr[\text{NoColl}_q] = \prod_{i=1}^{q-1}\left(1 - \frac{i}{N}\right)$$

$$\Pr[\text{NoColl}_q] \leq \prod_{i=1}^{q-1} e^{-i/N} = e^{-\sum_{i=1}^{q-1}(i/N)} = e^{-q(q-1)/2N}$$

$$\Pr[\text{Coll}] = 1 - \Pr[\text{NoColl}_q] \geq 1 - e^{-q(q-1)/2N} \geq \frac{q(q-1)}{4N}$$

Construction of fixed length hash function

Assuming that DL is hard to invert (one-way 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 $h \leftarrow \mathbb{G}$. 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 $H^s(x_1, x_2) := g^{x_1} h^{x_2}$.

Proof by contradiction

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

$$H^s(x_1, x_2) = H^s(x_1', x_2') \Rightarrow g^{x_1} h^{x_2} = g^{x_1'} h^{x_2'} \Rightarrow g^{x_1 - x_1'} = h^{x_2' - x_2}$$

$$\text{let } \Delta = x_2' - x_2$$

$$g^{(x_1 - x_1').\Delta\char`^-1} = \left(h^{x_2' - x_2}\right)^{\Delta^{-1} mod\ q} = h^{\Delta.\Delta^{-1} mod\ q} = h^1 = h$$

For the given value of g, h we found an X, which contradicts the assumption of DL being a one-way function.

Hence, (Gen, H) is a collision resistant hash function.

References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html.

[3] Lecture Slides