5 Hash Functions

Readings: Sections 5.1–5.4 of Bellare&Rogaway

5.1 The hash function SHA1

- Let \( \{0, 1\}^{<\ell} \) denote the set of all strings of length strictly less than \( \ell \). SHA1 is a function: \( \{0, 1\}^{<2^{64}} \rightarrow \{0, 1\}^{160} \).

- SHA1 is supposed to be collision-resistant. Collisions do exist. Even if we restrict the domain of SHA1 of strings of 256 bits, many strings must have the same hash value. (By pigeonhole principal, at least \( 2^{96} \) messages must collide.

- Difficulty to formalize collision-resistance: Can we say that there does not exist an algorithm that runs with time \( t \) and output a collision?

- It is difficult to capture the idea that it is infeasible for human beings to find collisions in SHA1. E.g., cannot formalize that one number is difficult to factor.

- Formal definition uses a family of functions.

5.2 Collision-resistant hash functions

- A hash function is a family of functions \( H : K \times D \times R. H_K(M) : D \rightarrow R = H(K, M) \).

- SHA1 can be extended to a family SHF1: \( \{0, 1\}^{128} \times \{0, 1\}^{<2^{64}} \rightarrow \{0, 1\}^{160} \), by allowing variable initial value.

- Different notions of collision resistance.
  
  - \textbf{CR0 attack}: Adversary picks \((x_1, x_2)\); Challenger randomly picks \( K \leftarrow \mathcal{K} \); adversary succeeds if \( H_K(x_1) = H_K(x_2) \).
    
    A hash function resistant to such an attack is called universal (i.e., \( \forall x_1 \forall x_2 \Pr[H_K(x_1) = H_K(x_2)] \leq 1/|R| \)), or almost universal. E.g., \( H_{(a,b)}(x) = ax + b \text{ (mod } p) \).
  
  - \textbf{CR1-KK}: Adversary picks message \( x_1 \); Challenger randomly picks \( K \leftarrow \mathcal{K} \); adversary is given \( K \) and outputs \( x_2 \) and succeeds if \( H_K(x_1) = H_K(x_2) \). Needs to find a designated collision.
    
    A hash function resistant to such an attack is called universal one-way (aka. target-collision resistant).

    Consider SHF-1, this attack is similar to breaking one-wayness (or second preimage) of SHA-1 for any IV. Some formalize this by giving the adversary a random value \( y \) and a random \( K \), and the adversary needs to find \( x \) such that \( H_K(x) = y \).

    Universal One-Way Hash Functions (UOWHF) exist if and only if one-way functions exist.
– **CR2-KK**: Challenger picks $K \xleftarrow{\$} \mathcal{K}$; Adversary is given $K$, and outputs $x_1, x_2$. Adversary succeeds if $H_K(x_1) = H_K(x_2)$.

Breaking collision-resistance of SHF-1 means that one can break collision resistance of SHA-1 for any IV.

A hash function resistant to such an attack is called collision-free, collision-resistant, or collision-intractable. A Collision Resistant Hash Function (CRHF).

One-way function seems insufficient to build CRHF.

5.3 **Collision-finding attacks**

- Consider CR2-KK. One attack strategy is the birthday attack.

5.4 **One-wayness of collision-resistant hash functions**