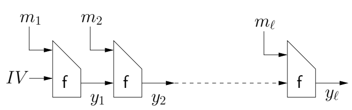
CS 6260
Applied Cryptography

Alexandra (Sasha) Boldyreva

Hash functions

Hash functions

- A hash function is a function whose output is shorter than its input.
- SHA1: $\{0,1\}^{< 2^{64}} \rightarrow \{0,1\}^{160}$
- Standardized by NIST.
- Design principles are similar to that of other hash functions MD4 and MD5 proposed by Rivest.
- The inputs are first padded and divided by blocks. Then an iterated (chaining) compression function is applied (known as Merkle-Damgård transform):



Security of hash functions

- What security properties a good hash function H should have?
- <u>Collision-resistance</u>: nobody should find M1,M2 s.t. H(M1)=H(M2)
- How to formalize this goal?
- Need to consider families of hash functions.

Collision resistance

- Let H: $\mathcal{K} \times D \rightarrow R$ be a function family. For an adversary A consider the experiments:

$\mathbf{Exp}_H^{\text{cr2-kk}}(A)$
$K \stackrel{\$}{\leftarrow} \mathcal{K}$; $(x_1, x_2) \stackrel{\$}{\leftarrow} A(K)$
if ($H_K(x_1) = H_K(x_2)$ and $x_1 \neq x_2$ and $x_1, x_2 \in D$)
then return 1 **else return** 0

$$\mathbf{Adv}_H^{\text{cr2-kk}}(A) = \Pr\left[\mathbf{Exp}_H^{\text{cr2-kk}}(A) = 1\right]$$

$\mathbf{Exp}_H^{\text{cr1-kk}}(A)$
$(x_1, st) \stackrel{\$}{\leftarrow} A()$; $K \stackrel{\$}{\leftarrow} \mathcal{K}$; $x_2 \stackrel{\$}{\leftarrow} A(K, st)$
if ($H_K(x_1) = H_K(x_2)$ and $x_1 \neq x_2$ and $x_1, x_2 \in D$)
then return 1 **else return** 0

$$\mathbf{Adv}_H^{\text{cr1-kk}}(A) = \Pr\left[\mathbf{Exp}_H^{\text{cr1-kk}}(A) = 1\right]$$

$\mathbf{Exp}_H^{\text{cr0}}(A)$
$(x_1, x_2) \stackrel{\$}{\leftarrow} A()$; $K \stackrel{\$}{\leftarrow} \mathcal{K}$
if ($H_K(x_1) = H_K(x_2)$ and $x_1 \neq x_2$ and $x_1, x_2 \in D$)
then return 1 **else return** 0

$$\mathbf{Adv}_H^{\text{cr0}}(A) = \Pr\left[\mathbf{Exp}_H^{\text{cr0}}(A) = 1\right]$$

Collision resistance

- A hash function is xx-secure if $\mathbf{Adv}_H^{xx}(A)$ is small for all efficient A.
- CR2-KK secure functions are aka collision-resistant, collision-free, collision intractable
- CR1-KK secure functions are aka universal one-way, target collision resistant
- CR0 secure functions are aka universal, almost universal.
- Claim. CR2-KK ⇒ CR1-KK ⇒ CR0

Looking for collisions

- Let's apply the birthday-attack strategy: pick q values in the domain at random. By the birthday paradox the probability of a collision is close to 1 when $q \approx \sqrt{2N}$. Here N is the size of the range.
- However, we can't apply the birthday paradox analysis directly, because the hash function does not "throw balls" at random.
- But if the function is regular: for every K

  $|H_K^{-1}(R_1)| = |H_K^{-1}(R_2)| = \cdots = |H_K^{-1}(R_N)|$ then the probability of finding a collision is close to that of the birthday attack.
- If the function is not regular then finding collisions is even easier
- So for SHA1 approximately 2^{80} trials will suffice.

Are more efficient attacks possible?

- Collisions were found for MD4, MD5.
- February 2005. Xiaoyun Wang, Lisa Yiqun Yin, and Hongbo Yu described the way to find collisions in SHA1 by using 2^{69} hash computations (much faster than the birthday attack).
- February 2005. The result by Xiaoyun Wang, Andrew Yao and Frances Yao is announced. Collisions in SHA1 can be found by using 2^{63} hash computations.
- The attacks were not implemented and still does not appear very practical.
- But the standard SHA1 will most probably be replaced.

One wayness of hash functions

- Let H: $\mathcal{K} \times D \to R$ be a function family. For an adversary A consider the experiment:
- $\mathbf{Exp}_H^{\text{ow-kk}}(A)$
- $K \xleftarrow{\$} \mathcal{K}\ ;\ x \xleftarrow{\$} D\ ;\ y \leftarrow H_K(x)\ ;\ x' \xleftarrow{\$} A(K, y)$
- If $(H_K(x') = y \text{ and } x' \in D)$ then return 1 else return 0
- We say that H is one-way if $\mathbf{Adv}_H^{\text{ow-kk}}(A) = \Pr\left[\mathbf{Exp}_H^{\text{ow-kk}}(A) = 1\right]$ is small for all efficient adversaries A.
- Q. Does one wayness imply collision resistance?
- Claim. Let H: $\mathcal{K} \times D \to R$ be a function family. Then for an adversary A there exists an adversary B with comparable resources s.t. $\mathbf{Adv}_H^{\text{ow-kk}}(A) \leq 2 \cdot \mathbf{Adv}_H^{\text{cr1-kk}}(B) + \frac{|R|}{|D|}$