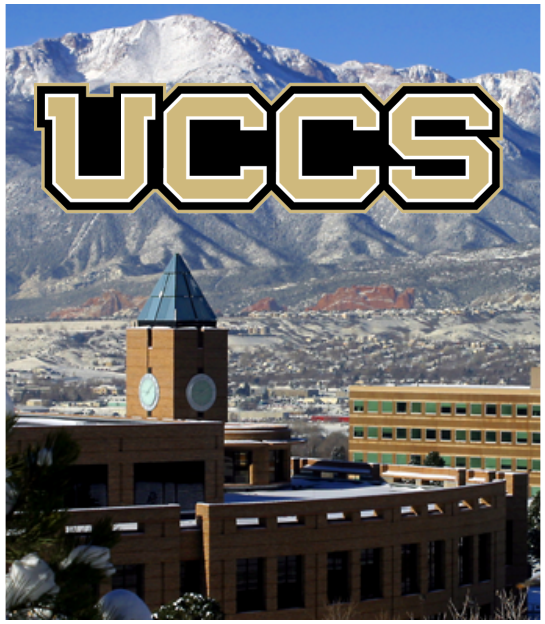


Cryptographic Hash and Integrity Protection

Cryptographic Hash Function

Sang-Yoon Chang, Ph.D.

Module: Cryptographic Hash Function

Hash Function Definitions

Insecure Hash Function Examples

Cryptographic Hash Requirements

Iterative Structure

Hash Functions

Functions transforming large input (variable size) to small fixed output

Hash Functions

Functions transforming large input (variable size) to small fixed output

Deterministic and efficient computation given the input

Hash Functions

Functions transforming large input (variable size) to small fixed output

Deterministic and efficient computation given the input

Output is uniformly distributed

Hash Functions

Functions transforming large input (variable size) to small fixed output

Deterministic and efficient computation given the input

Output is uniformly distributed

Input is also called *message* and output can be called *digest*, *fingerprint*, *hash*

Insecure Hash Functions: Checksums

Bit-by-bit XOR (parity) of multiple blocks

Insecure Hash Functions: Checksums

Bit-by-bit XOR (parity) of multiple blocks

Regularity of message blocks

=> Non-uniform output

Insecure Hash Functions: Checksums

Bit-by-bit XOR (parity) of multiple blocks

Regularity of message blocks

=> Non-uniform output

Improve by circular shifting message blocks by different amounts before XOR

Insecure Hash Functions: Checksums

Bit-by-bit XOR (parity) of multiple blocks

Regularity of message blocks

=> Non-uniform output

Improve by circular shifting message blocks by different amounts before XOR

Easy to generate collision

Hash Functions

Functions transforming large input (variable size) to small fixed output

Deterministic and efficient computation given the input

Output is uniformly distributed

Input is also called *message* and output can be called *digest*, *fingerprint*, *hash*

Cryptographic Hash (h) Requirements

The output of h is pseudo-random and exhibits avalanche effect

One-wayness Difficult to find a input that maps to a given hash output

Collision resistance Difficult to find two inputs mapping to same hash output

Cryptographic Hash (h) Requirements

(0. The output of h is pseudo-random)

1. Preimage resistance (one-wayness)

    For any output h', it is computationally infeasible to find y such that h(y)=h'

Cryptographic Hash (h) Requirements

(0. The output of h is pseudo-random)

1. Preimage resistance (one-wayness)

   For any output h', it is computationally infeasible to find y such that h(y)=h'

2. Weak collision resistance

   For any x, it is computationally infeasible to find $y \neq x$ with h(y)=h(x)

Cryptographic Hash (h) Requirements

(0. The output of h is pseudo-random)

1. Preimage resistance (one-wayness)

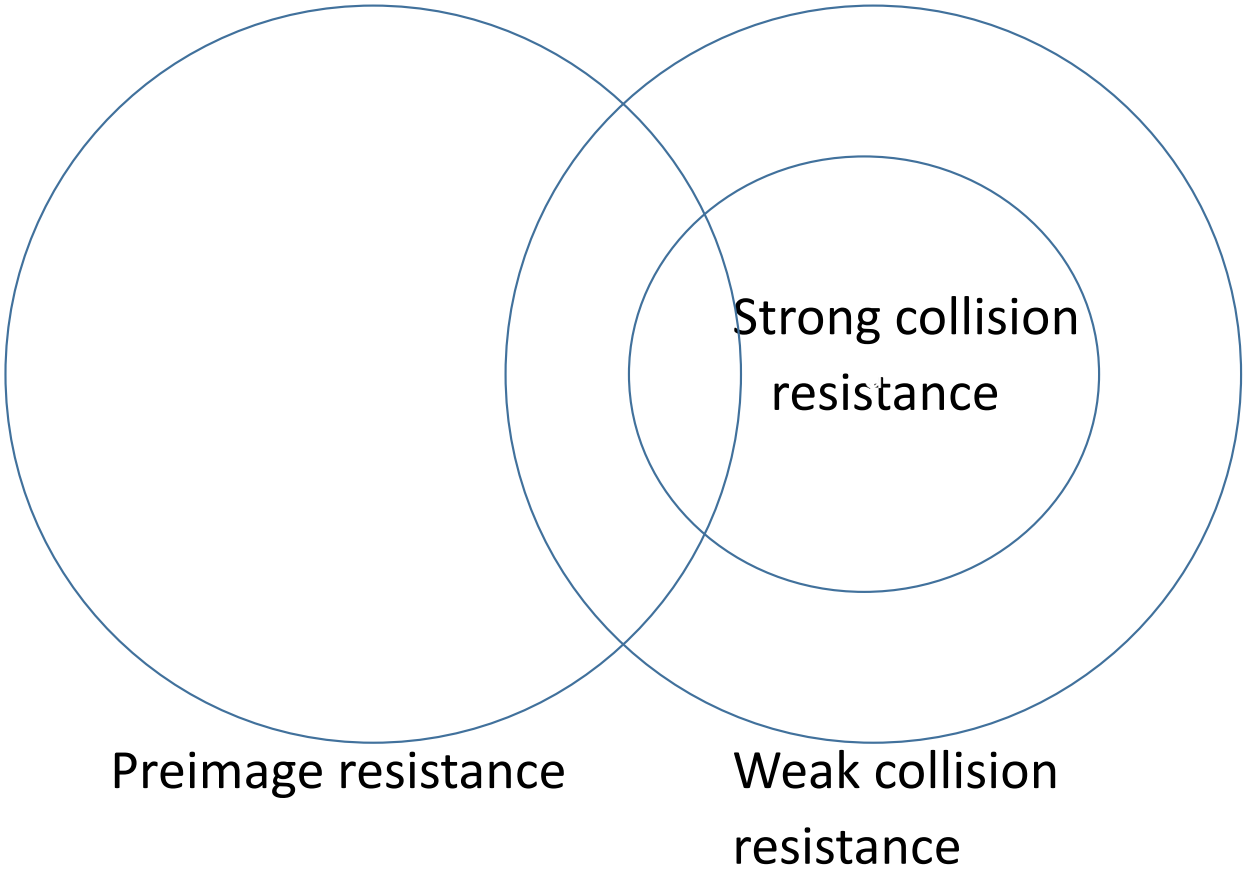
   For any output h', it is computationally infeasible to find y such that h(y)=h'

2. Weak collision resistance

   For any x, it is computationally infeasible to find $y \neq x$ with h(y)=h(x)

3. Strong collision resistance

   It is computationally infeasible to find any pair (x,y) such that h(x)=h(y)


Strong collision resistance
Preimage resistance
Weak collision resistance

Brute Force Attack on Hash Functions

Security depends on the length of h (n)

Attack on preimage resistance or weak collision resistance takes 2^{n-1}

Brute Force Attack on Hash Functions

Security depends on the length of h (n)

Attack on preimage resistance or weak collision resistance takes 2^{n-1}

Attack on strong collision resistance takes $2^{n/2}$ due to Birthday Paradox

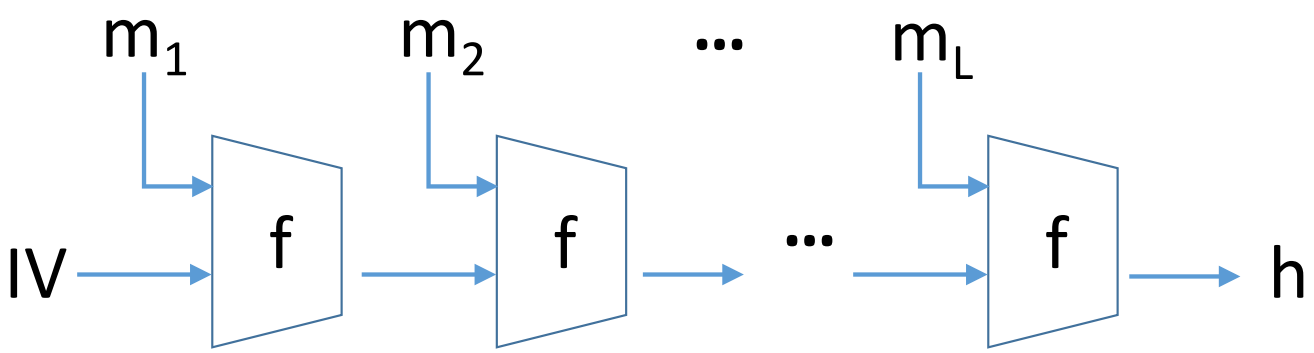
(Strong collision resistance is harder to achieve in the defender perspective)

Hash Iterative Structure

Iterative w/ compression functions (f)

To support variable-length input (m_i's)

If f collision resistant, then so is the hash

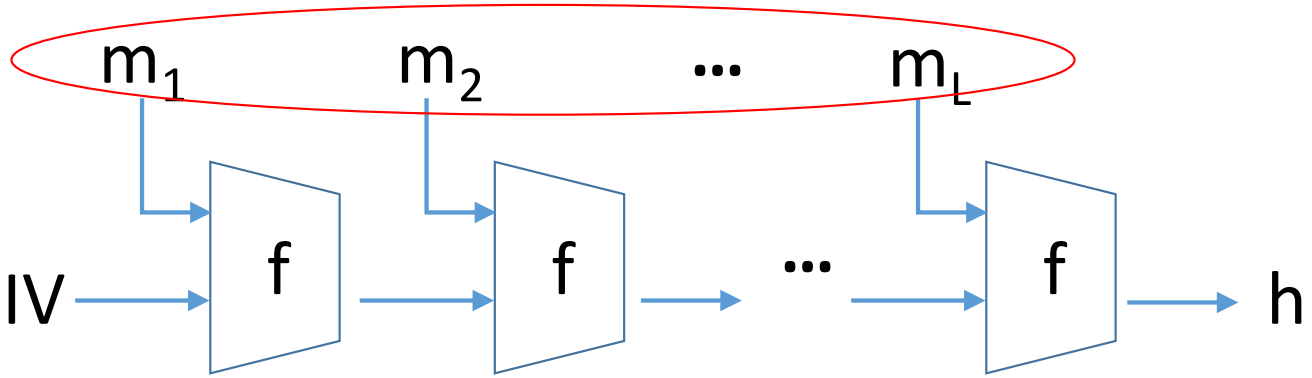


Hash Iterative Structure

Iterative w/ compression functions (f)

To support variable-length input (m_i's)

If f collision resistant, then so is the hash

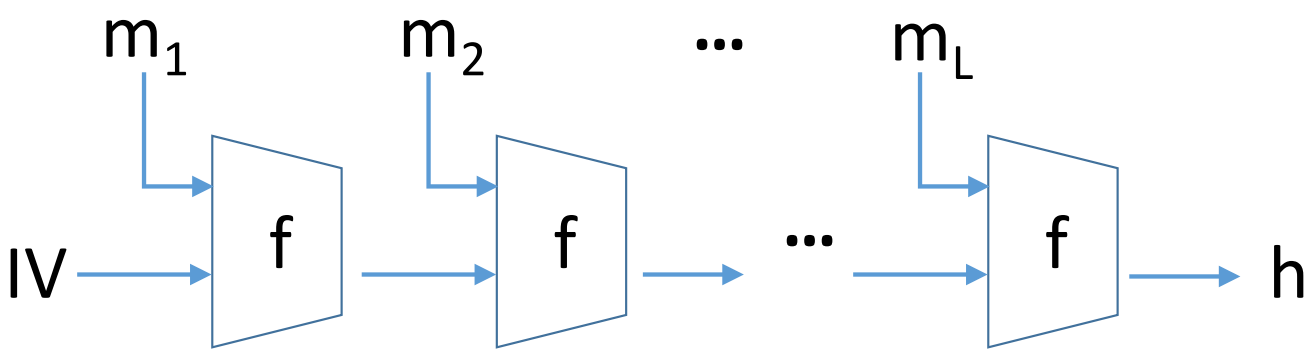


Hash Iterative Structure

Iterative w/ compression functions (f)

To support variable-length input (m_i's)

If f collision resistant, then so is the hash

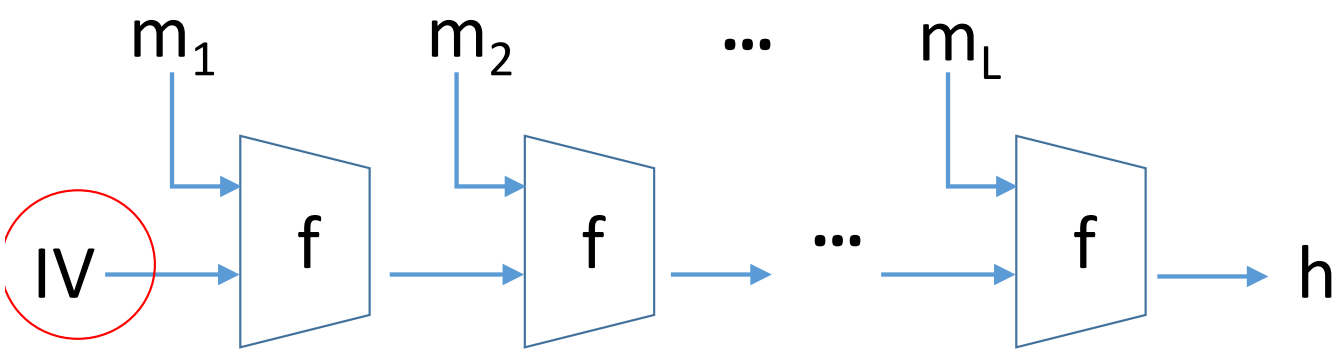


Hash Iterative Structure

Iterative w/ compression functions (f)

To support variable-length input (m_i's)

If f collision resistant, then so is the hash

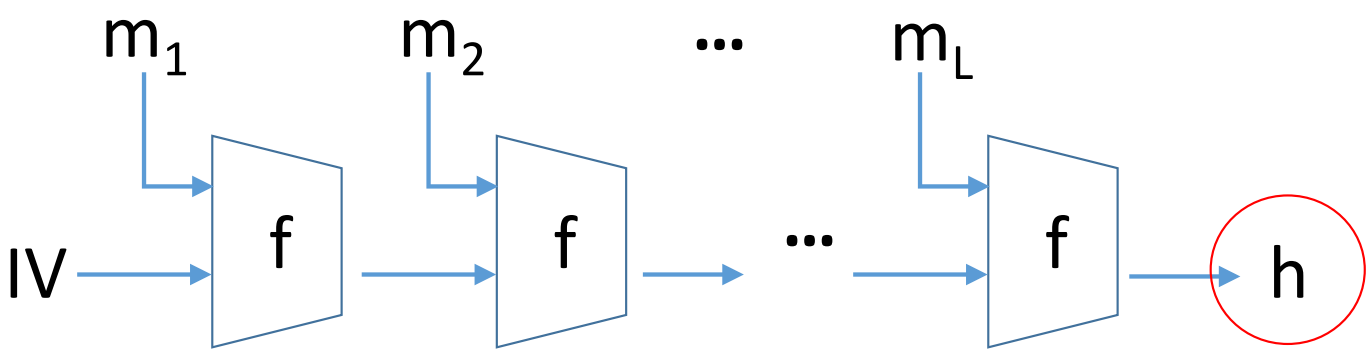


Hash Iterative Structure

Iterative w/ compression functions (f)

To support variable-length input (m_i's)

If f collision resistant, then so is the hash



Hash Using Block Ciphers

f can be a block cipher

Similar to CBC but with no key