UNIVERSITY OF DELAWARE

CYBERSECURITY

Applied Cryptography
CPEG 472/672
Lecture 6B

Instructor: Nektarios Tsoutsos

The SHA family of hash functions

- SHA=secure hash algorithm
  - NIST standard, worldwide standard
  - Use by non-military agencies in US
  - Replaced MD5 ('92-'05)
- SHA1 (160 bits)
  - M-D hash function with D-M compression
  - Based on special block cipher
  - 512-bit block size, compress: H=E(M,H)+H
    - Addition of 32-bit values instead of XORs
  - Replaced NSA's SHA-0 that had a flaw

SHA1 internals

```
SHA1-compress(H, M):
  (a0,b0,c0,d0,e0) = H
  (a,b,c,d,e)=SHA1-BS(a0,b0,c0,d0,e0,M)
  return (a+a0, b+b0, c+c0, d+d0, e+e0)
```

- Operates on arrays of 32-bit integers
    - Initial value of H (i.e., H0) is constant
    - Output 5 x 32-bit values = 160 bits

SHA1 internals

```
SHA1-BS(a,b,c,d,e,M):
  W = expand(M)
  for i = 0 to 79:
    new=(a<<<5)+f(i,b,c,d)+e+K[i]+W[i]
    (a,b,c,d,e)=(new,a,b>>>2,c,d)
  return (a,b,c,d,e)
```

- 80 rounds
- K[i] values are predefined constants

SHA1 internals

- expand() creates an array 320 bytes
    - 80 32-bit words
    - Input: 512 message block (16x32-bits)
    - W[0]-W[15]=input message
    - W[16]-W[79]=XOR of previous W and ROTL
- f() is a sequence of bitwise operations
    - Depends on the round
    - XORs
    - ANDs

SHA-1 is now broken

- 2005: weaknesses found on SHA-1
  - Can find a collision in 2^63 operations
  - Theoretical value is 2^80
- Shattered attack
  - https://shattered.io
  - Collision on two PDF documents
  - Cannot guarantee integrity any more
- Should use SHA-2, BLAKE2 or SHA-3

SHA-2

- Designed by the NSA, a NIST standard
  - Family of four hash functions
  - Hash output lengths: 224, 256, 384, 512
- SHA-256
  - Longer hashes => better security levels
  - 256-bit chaining values
  - Eight 32-bit values
  - 64 rounds
  - More complicated expand() and compress()

Other members of SHA-2 family

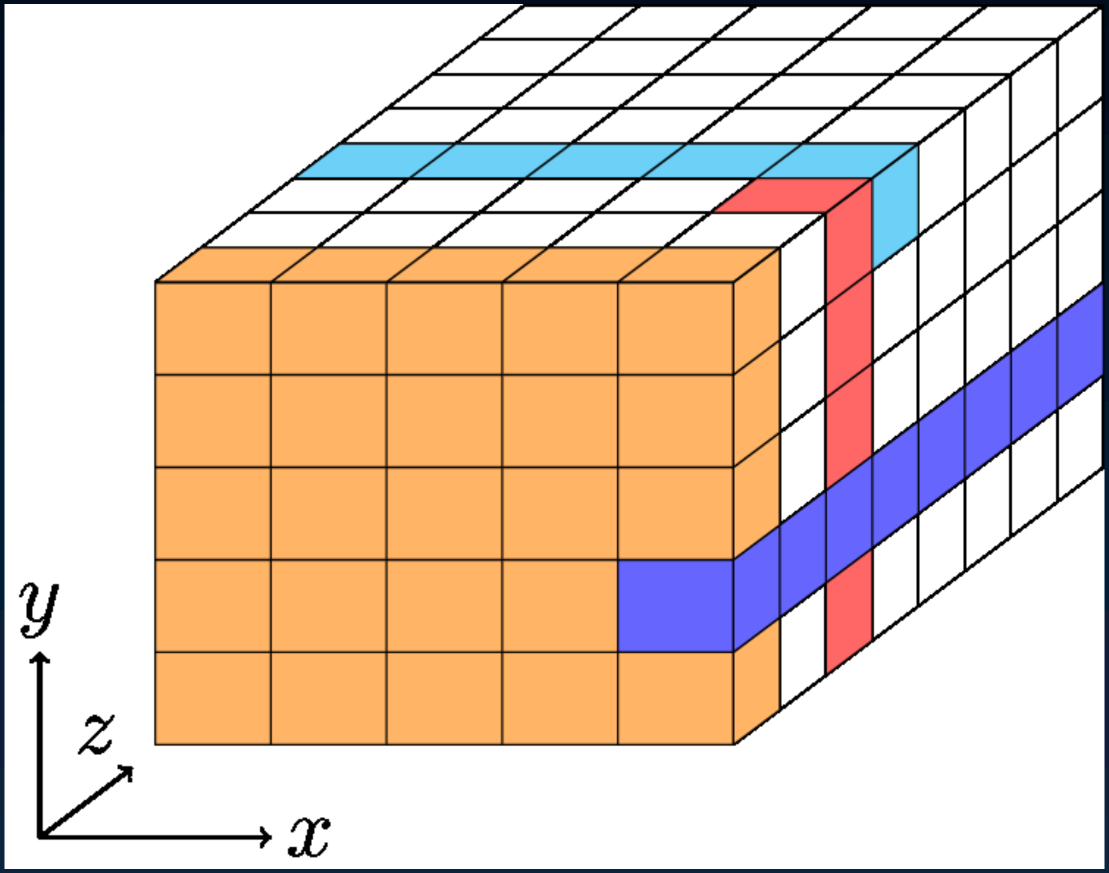
- SHA-224
    - Same as SHA-256
    - Take first 224 bits of the final chaining value
- SHA-512
    - Similar to SHA-256
        - Different rotation offsets
    - Use 64 bit values instead of 32-bits
    - Ingests 1024-bit message blocks
- SHA-384
    - Truncate SHA-512 to 384 bits

SHA-3

- NIST competition
  - Need to have a hash standard different from SHA-1 (broken) and SHA-2 (not yet broken)
- Requirements
  - Candidates should not be like SHA1, SHA2
  - At least as secure/fast as SHA-2
  - At least as capable as SHA-2
- 5 finalists
  - BLAKE, Grostl, JH, Keccak, Skein

Keccak (SHA-3)

- Sponge construction
  - 1600 bit internal state



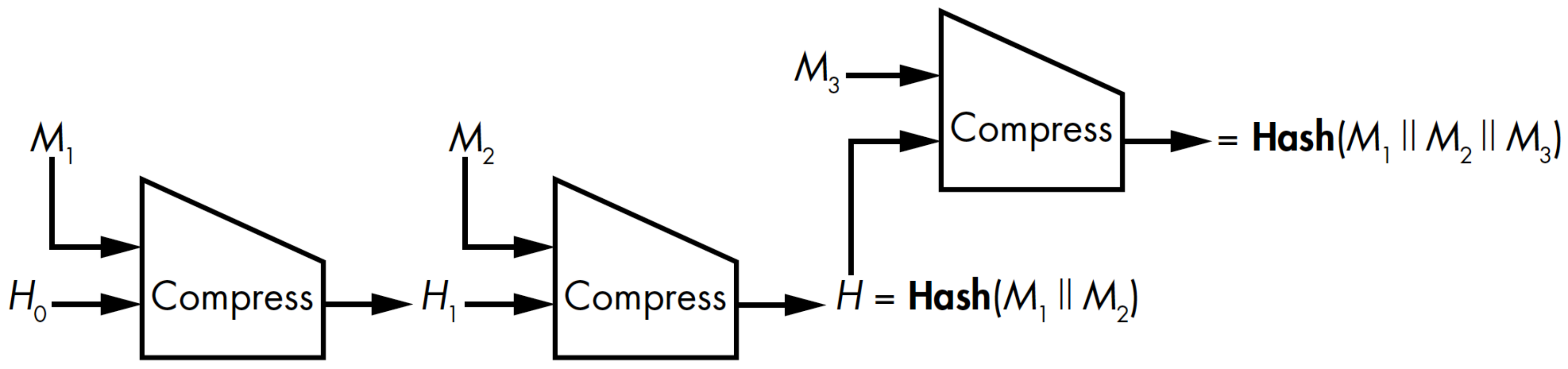
Keccak (SHA-3)

- SHA-3 can ingest blocks of different sizes
  - 1152, 1088, 832, 576 bits
- Hash value bit size is:
  - 224, 256, 384, 512
- Uses a single core algorithm
  - SHA-2 uses two: one for 256, one for 512
- Supports extendable output functions
  - Part of the standard

BLAKE2

- SHA-3 is not faster than SHA-2
  - Need for secure fast hash
- BLAKE2
  - At least as secure as SHA-3
  - Faster than previous standard (incl. MD5)
  - Can hash large amounts of data
  - Supports parallelism
  - M-D based, D-M compress (ChaCha-based)
- Variants
  - BLAKE2b, BLAKE2s, BLAKE2bp, BLAKE2sp

Length Extension Attack



M_1
H_0
Compress
H_1
M_2
Compress
H = **Hash**(M_1 || M_2)
M_3
Compress
= **Hash**(M_1 || M_2 || M_3)

- Can generate hash of longer message
  - This can be very bad in some cases
- Mitigation
  - How can we prevent that?

Fooling Proof of Storage Protocols

- Proof of Storage Protocols
  - Cloud server proves to client that user files are indeed stored on the server
  - Server may have incentive to delete them to save storage
- How to prove the files are still there?
  - Client picks random C
  - Server returns Hash(M||C)
- What is the problem?

Hands-on exercises

- Length extension attack on SHA1
- SHA-3 examples
- BLAKE2 examples

Reading for next lecture

- Aumasson: Chapter 7
    - We will have a short quiz
- Midterm: Thu April 9th, 2:00-3:15pm
    - All material during first 6 weeks
    - Chapters 1-6
    - Lectures 1A-6B