MAS 433: Cryptography

Lecture 11

Hash Function

Wu Hongjun

Lecture Outline

- Classical ciphers
- Symmetric key encryption
- Hash function and Message Authentication Code
  - Birthday attack
  - **Hash function**
  - Message Authentication Code
- Public key encryption
- Digital signature
- Key establishment and management
- Introduction to other cryptographic topics

Recommended Reading

- CTP Section 4.1, 4.2, 4.3
- HAC Section 9.1, 9.2, 9.3, 9.4
- Wikipedia
  - Cryptographic hash function
    http://en.wikipedia.org/wiki/Cryptographic_hash_function
  - Merkle-Damgard construction
    http://en.wikipedia.org/wiki/Merkle%E2%80%93Damg%C3%A5rd_construction
  - SHA-1
    http://en.wikipedia.org/wiki/SHA-1
  - SHA-2
    http://en.wikipedia.org/wiki/SHA-2
  - SHA-3 competition
    http://en.wikipedia.org/wiki/SHA-3
- Full SHA-1, SHA-2 specifications
  http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

Hash Function

- Hash Function
  - Compress a message with arbitrary length into a fixed-length output
- Cryptographic hash function
  - To ensure that hash function's every output (message digest) represents a message uniquely
    - A message digest represents only one message
- Importance of cryptographic hash function
  - Important for data integrity
    - Example: Checksum for downloading software
  - Important for digital signature (for authentication)
    - The research on cryptographic hash function is mainly due to the invention of digital signature
  - Key generation, security token …………

Hash Function

- How to ensure that each message digest represents a message uniquely ?
  - The message space size is much larger than the size of the message digest space

    => it is impossible for a message digest to represent only one message
  - Solution: we try to ensure that it is computationally impossible to find two messages with the same message digest

    => then it becomes computationally possible for a message digest to represent only one message

Hash Function

- A strong cryptographic hash function h with n-bit message digest size has the following three properties
  - Preimage Resistance
    - For any given y, it is difficult to find m satisfying $h(m) = y$
    - i.e., it requires about 2^n computations to find a preimage
  - Second-Preimage Resistance
    - For any given m, it is difficult to find a different m' so that $h(m) = h(m')$
    - i.e., it requires about 2^n computations to find a second-preimage
  - Collision Resistance
    - It is difficult to find two different m and m' so that $h(m) = h(m')$
    - i.e., it requires about $2^{n/2}$ computations to find a collision

Birthday attack!

Hash Function Overall Structure

- Iterated structure
  - Divide a message into many message blocks

    $$m = m_1 \parallel m_2 \parallel m_3 \ldots.$$

  - Hash each message block iteratively:

    $H_0 = \text{IV}$ (here **IV is a fixed constant**)

    $H_i = f(H_{i-1}, m_i)$ (f is called compression function)

    (the size of H_i must be at least as large as the size of the message digest)

But, the above construction is insecure!

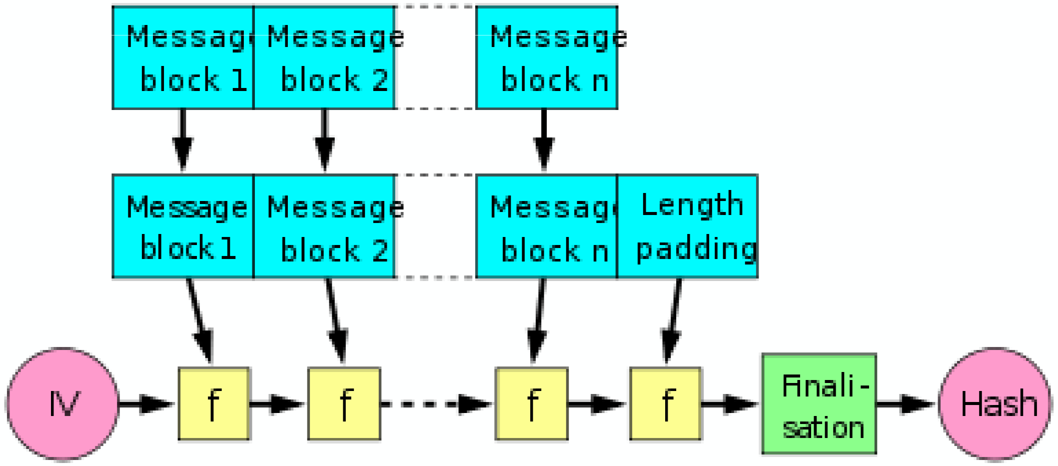
- For example, the message being represented by the last message block is ambiguous!

Hash Function Overall Structure

- Merkle-Damgard structure
  - Strengthen the iterated structure with **padding**
    - pad bit ‘1’ to the end of the message
    - pad some zeros
    - pad the message length (in bits)
    - After padding, the overall length should be multiple of the block size
  - **Finalization** stage: process the output from the last message block, then to generate the message digest
  - The most widely used hash function overall structure

Hash Function Overall Structure

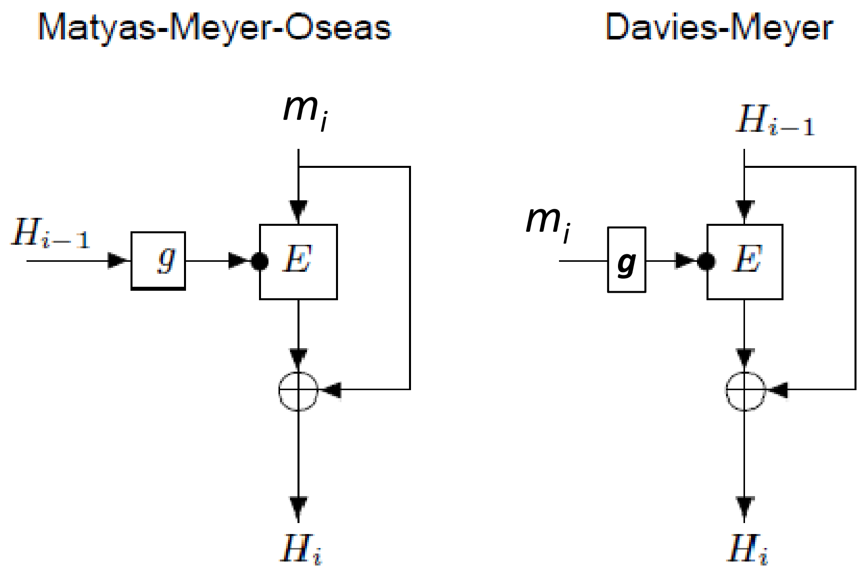
- Merkle-Damgard structure



Message digest

Compression Function Structure

- Many different compression function structures
- Compression function based on single block cipher:



  – Davies-Meyer structure is so far the most widely used:
    MD4, MD5, SHA-1, SHA-2

Hash Functions

- MD4 (1990)
  - 128-bit message digest
- MD5 (1991)
  - 128-bit message digest

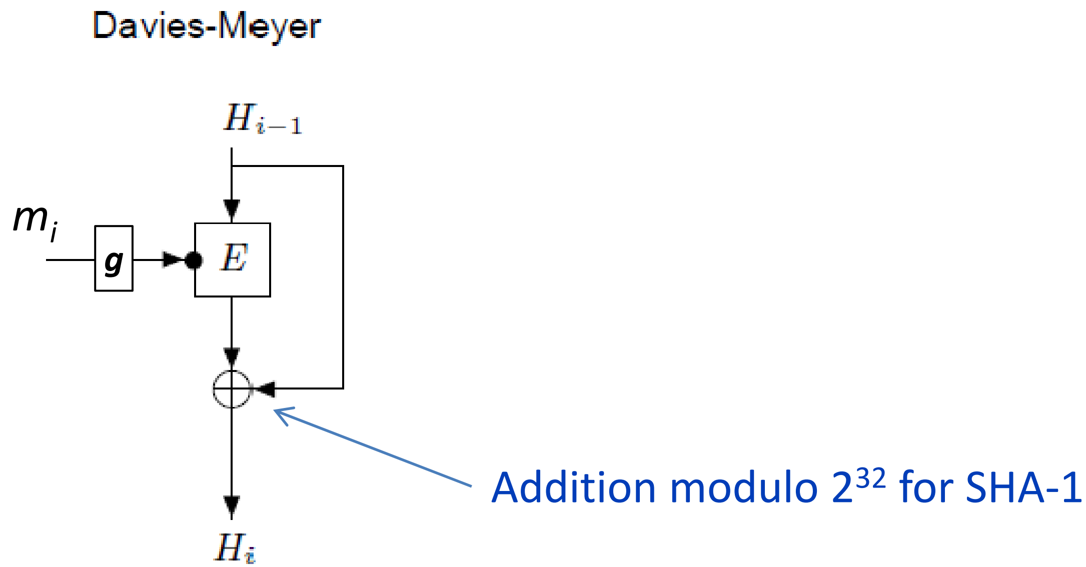
Designed by Ron Rivest,
Extremely weak,
MD5 broken by Wang Xiaoyun
etc in 2005

Hash Functions

- Hash function standard of NIST
  SHA – Secure Hash Algorithm (by NSA)
  - SHA-0, published in 1993
    - 160-bit message digest size
    - Insecure – withdrawn shortly, replaced by SHA-1
  - SHA-1, published in 1995
    - 160-bit message digest size
    - Insecure (2^{69}, Wang Xiaoyun, etc, 2005)
      - but so far not broken on computer
  - SHA-2, published in 2001
    - SHA-256, SHA-224
      - SHA-224 is based on SHA-256: different IV, truncating 32 bits
    - SHA-512, SHA-384
      - SHA-384 is based on SHA-512: different IV, truncating 64 bits

SHA-1

- 160-bit message digest
- 512-bit message block size
- Merkle-Damgard construction
- Davies-Meyer compression function structure



SHA-1

- Message expansion
  - Expand a 512-bit message block
  - Message block: m_0, m_1, …. m_{15} (each m_i is 32-bit)
  - Expanded message: w_0, w_1, …. w_{79}

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ ROTL^1(W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) & 16 \le t \le 79 \end{cases}$$

SHA-1

- 80 Steps to compress the expanded message
  - A 32-bit constant k_i for each step
- $(a_0, b_0, c_0, d_0, e_0) = H_{i\text{-}1}$ (H_0 is a fixed constant)

$$T = ROTL^5(a) + f_t(b,c,d) + e + K_t + W_t$$

$$e = d$$

$$d = c$$

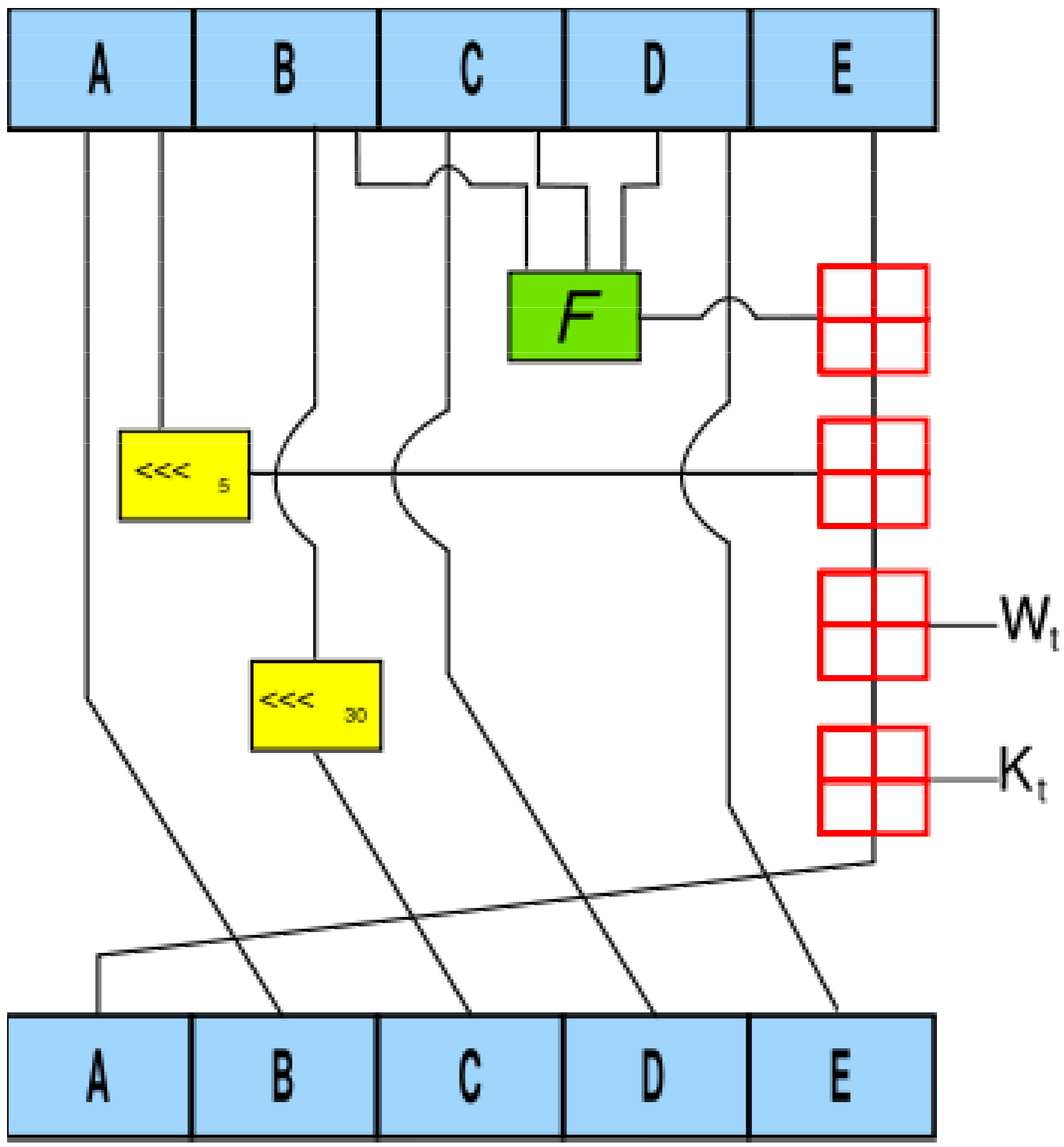
$$c = ROTL^{30}(b)$$

$$b = a$$

$$a = T$$

Each word is 32-bit

$$f_t(x,y,z) = \begin{cases} Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z) & 0 \le t \le 19 \\ Parity(x,y,z) = x \oplus y \oplus z & 20 \le t \le 39 \\ Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) & 40 \le t \le 59 \\ Parity(x,y,z) = x \oplus y \oplus z & 60 \le t \le 79. \end{cases}$$


A
B
C
D
E
F
<<< 5
<<< 30
W_t
K_t
A
B
C
D
E

SHA-256

- 256-bit message digest
- 512-bit message block size
- Merkle-Damgard construction
- Davies-Meyer compression function structure

SHA-256

- Message expansion
  - Expand a 512-bit message block
  - Message block: m_0, m_1, …. m_{15} (each m_i is 32-bit)
  - Expanded message: w_0, w_1, …. w_{63}

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases}$$

$$\sigma_0^{\{256\}}(x) \;=\; ROTR^7(x) \;\oplus\; ROTR^{18}(x) \;\oplus\; SHR^3(x)$$

$$\sigma_1^{\{256\}}(x) \;=\; ROTR^{17}(x) \;\oplus\; ROTR^{19}(x) \;\oplus\; SHR^{10}(x)$$

SHA-256

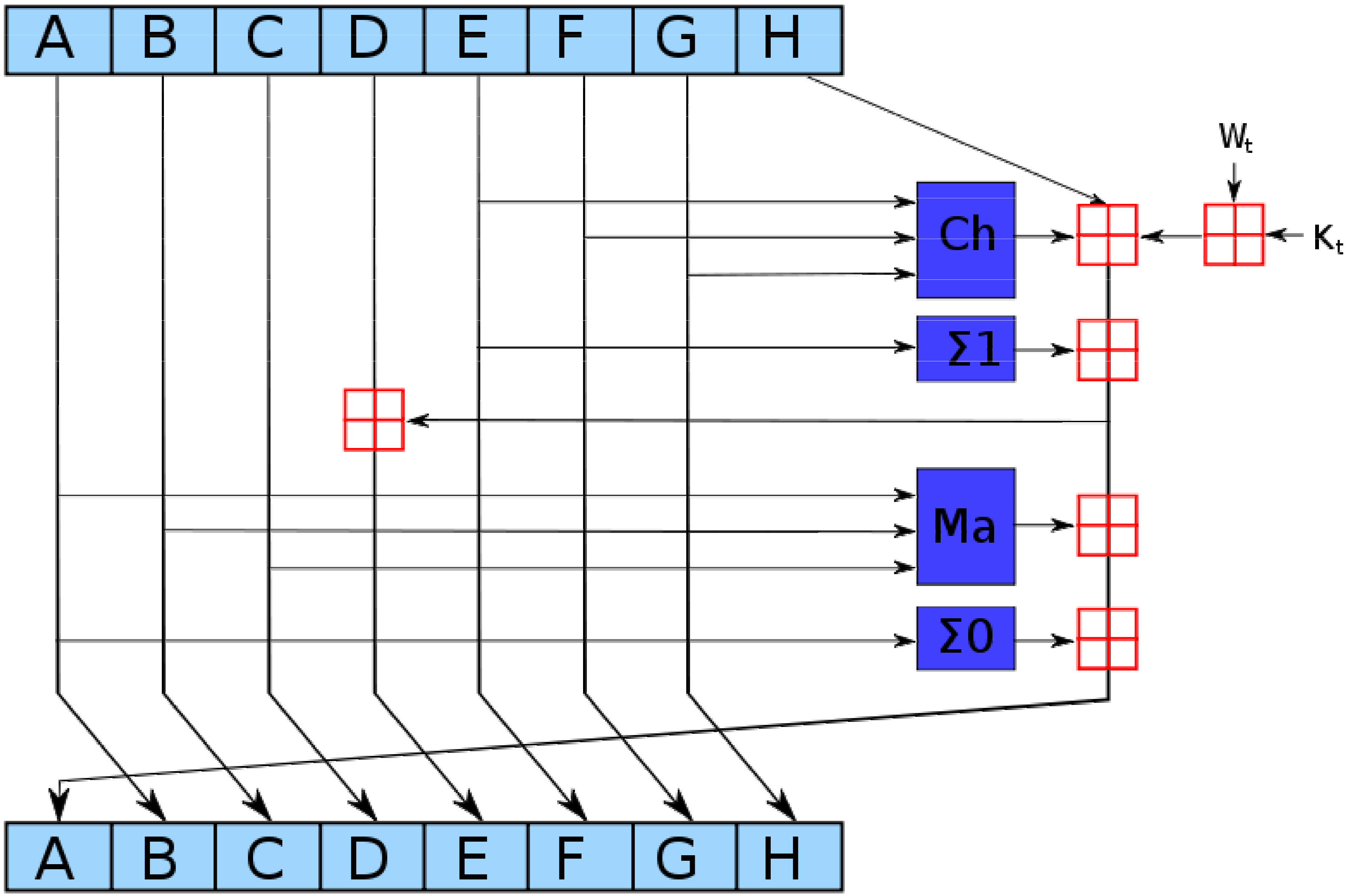
- 64 steps to compress the expanded message
  - A random constant k_i for each step
- $(a_0,b_0,c_0,d_0,e_0,f_0,g_0,h_0) = H_{i\text{-}1}$ (H_0 is a fixed constant)

$$
\begin{aligned}
T_1 &= h + \textstyle\sum_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t \\
T_2 &= \textstyle\sum_0^{\{256\}}(a) + Maj(a,b,c) \\
h &= g \\
g &= f \\
f &= e \\
e &= d + T_1 \\
d &= c \\
c &= b \\
b &= a \\
a &= T_1 + T_2
\end{aligned}
$$

Each word is 32-bit

$$
\begin{aligned}
Ch(x,y,z) &= (x \wedge y) \oplus (\neg x \wedge z) \\
Maj(x,y,z) &= (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)
\end{aligned}
$$

$$
\begin{aligned}
\textstyle\sum_0^{\{256\}}(x) &= ROTR^{2}(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \\
\textstyle\sum_1^{\{256\}}(x) &= ROTR^{6}(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)
\end{aligned}
$$


A
B
C
D
E
F
G
H
W_t
K_t
Ch
Σ1
Ma
Σ0
A
B
C
D
E
F
G
H

SHA-512

- 512-bit message digest
- 1024-bit message block size
- Merkle-Damgard construction
- Davies-Meyer compression function structure

SHA-512

- Message expansion
  - Expand a 1024-bit message block
  - Message block: m_0, m_1, …. m_{15} (each m_i is 64-bit)
  - Expanded message: w_0, w_1, …. w_{79}

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{512\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{512\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 79 \end{cases}$$

$$\sigma_0^{\{512\}}(x) = ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x)$$
$$\sigma_1^{\{512\}}(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x)$$

SHA-512

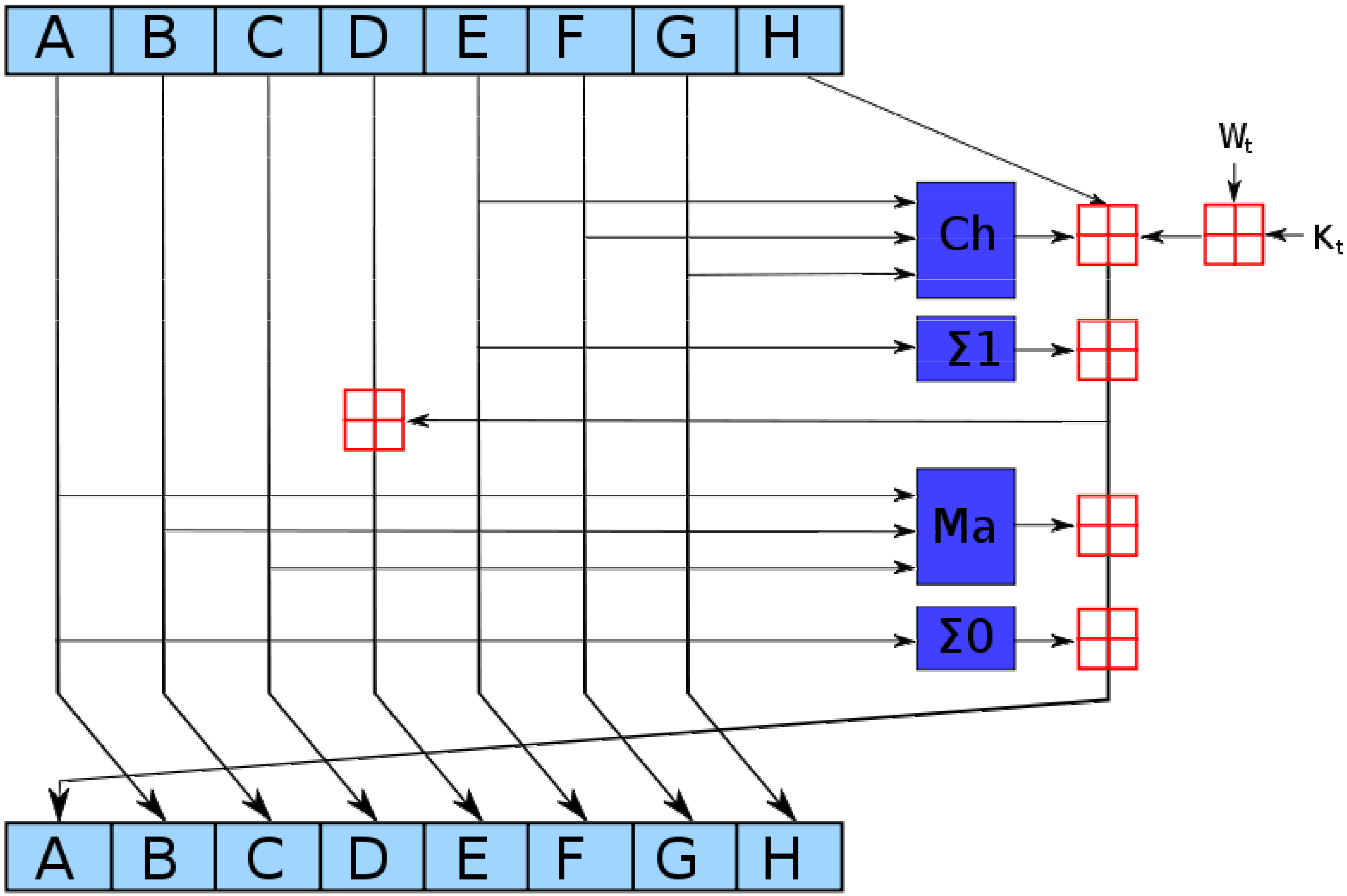
- 80 steps to compress the expanded message
  - A random 64-bit constant k_i for each step
- $(a_0,b_0,c_0,d_0,e_0,f_0,g_0,h_0) = H_{i-1}$ (H_0 is a fixed constant)

$$T_1 = h + \sum_1^{\{512\}}(e) + Ch(e,f,g) + K_t^{\{512\}} + W_t$$
$$T_2 = \sum_0^{\{512\}}(a) + Maj(a,b,c)$$
$$h = g$$
$$g = f$$
$$f = e$$
$$e = d + T_1$$
$$d = c$$
$$c = b$$
$$b = a$$
$$a = T_1 + T_2$$

Each word is 64-bit

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$$
$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$\sum_0^{\{512\}}(x) = ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x)$$
$$\sum_1^{\{512\}}(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x)$$


A B C D E F G H
W_t
Ch
K_t
Σ1
Ma
Σ0
A B C D E F G H

SHA-3 Competition (2008—2012)

- NIST hash function competition
  - In order to select one or two strong and efficient hash functions
  - Received 64 submissions in 2008
  - In 2009, 14 candidates were selected
  - In 2010, 5 candidates were selected
  - In 2012, 1 or 2 candidates would be selected
    - The final candidates will be called SHA-3

Summary

- Cryptographic hash function
  - Aim: Each message digest represents only one message (computationally)
  - Three security requirements
    - Preimage resistance
    - Second-preimage resistance
    - Collision resistance
- SHA-1
  - Insecure
  - How to break it in practice?
- SHA-2
  - SHA-224,SHA-256, SHA-384, SHA-512
- SHA-3
  - ongoing