

# Introduction to Modern Cryptography

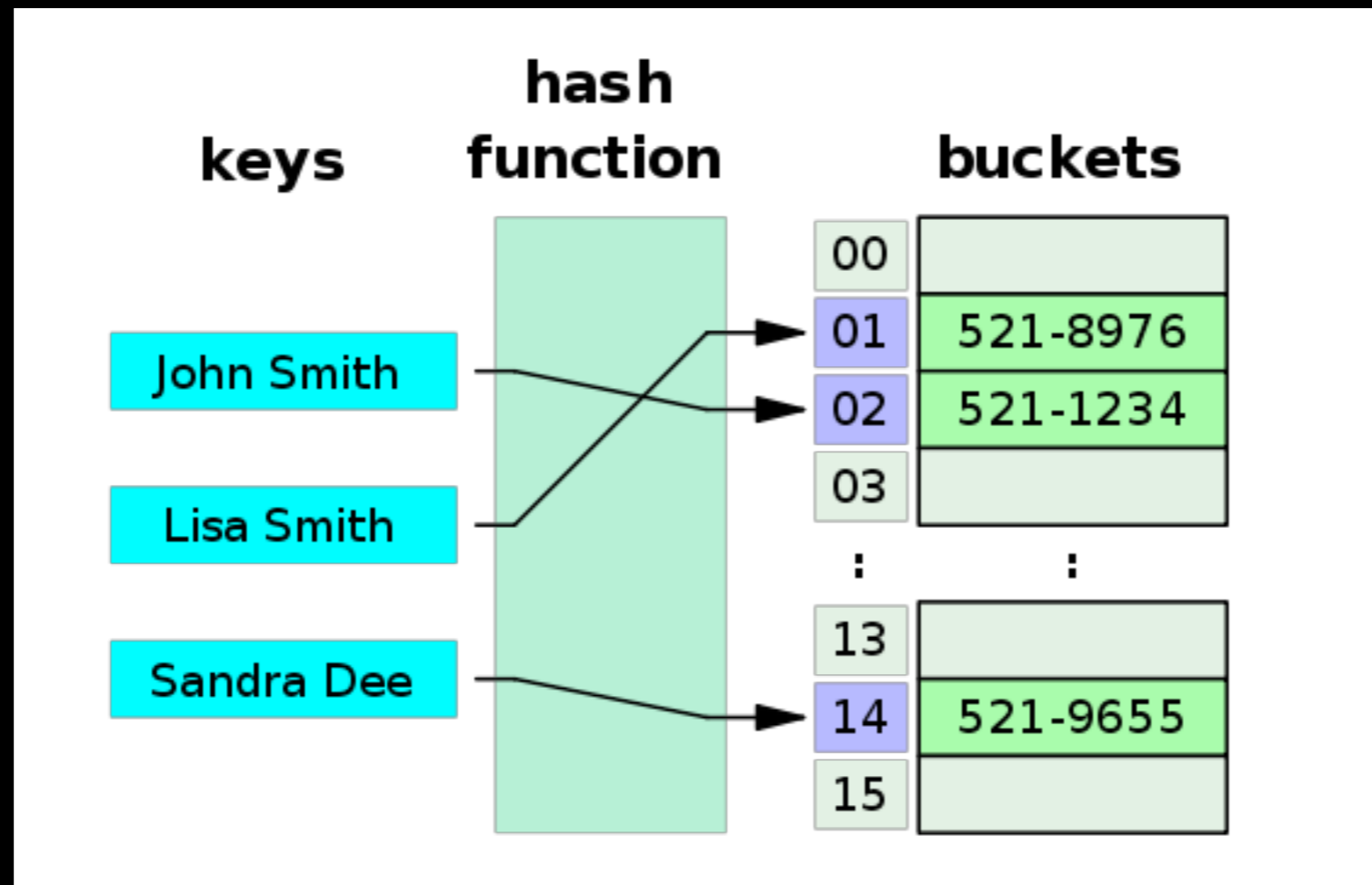


6th lecture:

Collision-Resistant Hash Functions

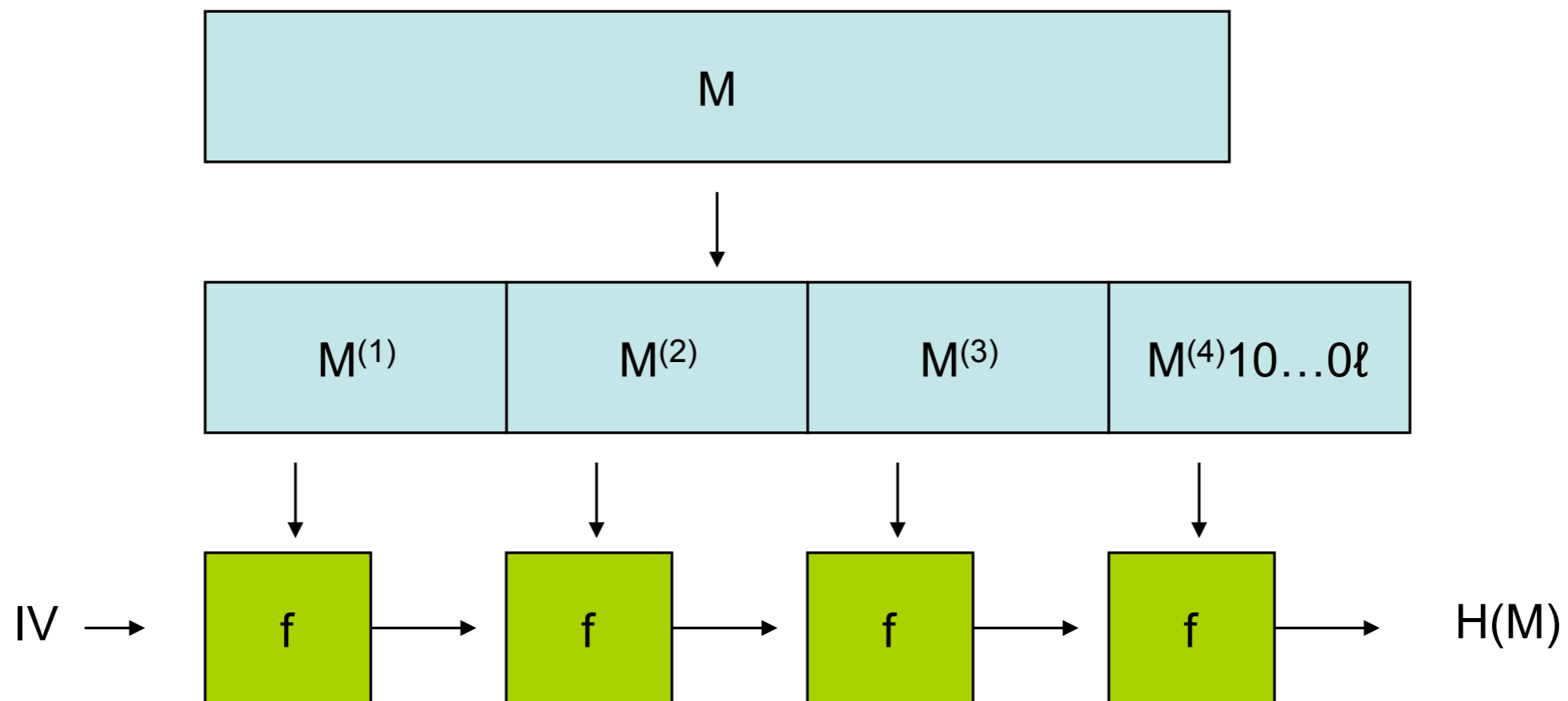
quite a few of these slides are copied from or heavily inspired by the  
University College London MSc InfoSec 2010 course given by Jens Groth  
Thank you very much!

# Hash Tables



- used in data structures to store associative arrays
- try to minimize collisions!

# Merkle-Damgård Construction



# Ralph C. Merkle



- co-inventor of public-key crypto
- Merkle puzzles, Merkle trees
- new ideas are hard to publish
- now interested in nanotechnology and cryonics

# Ivan Bjerre Damgård



- most publishing cryptographer in the world
- my PhD advisor
- amazing person
- plays the fiddle

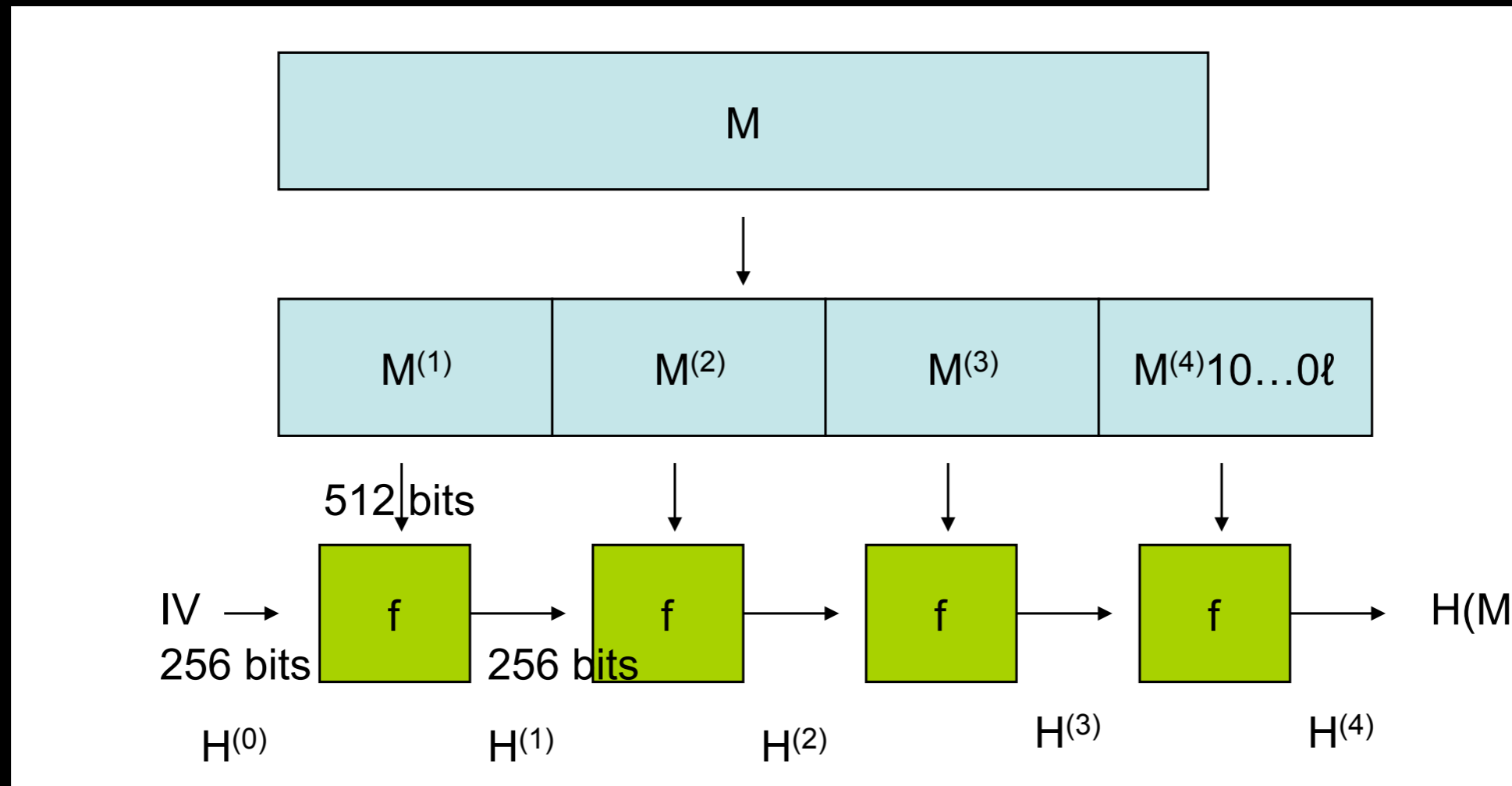
# Birthday Attacks on Hash Functions

- In a class of  $N$  students with random birthdays  $b_1, \dots, b_N \leftarrow \{1, 2, \dots, 365\}$ . How large does  $N$  need to be such that  $\Pr[\text{exists } i \neq j : b_i = b_j] > 1/2$  ?
- Answer:  $N \geq \sqrt{365} \approx 23$
- Task: Find a generic collision-attack on the hash function  $H: \{0, 1\}^* \rightarrow \{0, 1\}^n$

# Finding Meaningful Collisions

- It is {hard, difficult, challenging, impossible} to {imagine, believe} that we will {find, locate, hire} another {employee, person} having similar {abilities, skills, character} as Alice. She has done a {great, super} job
- $4 \times 2 \times 3 \times 2 \times 3 \times 2 = 288$  possibilities
- prepare  $2^{n/2}$  of those and  $2^{n/2}$  of bad ones

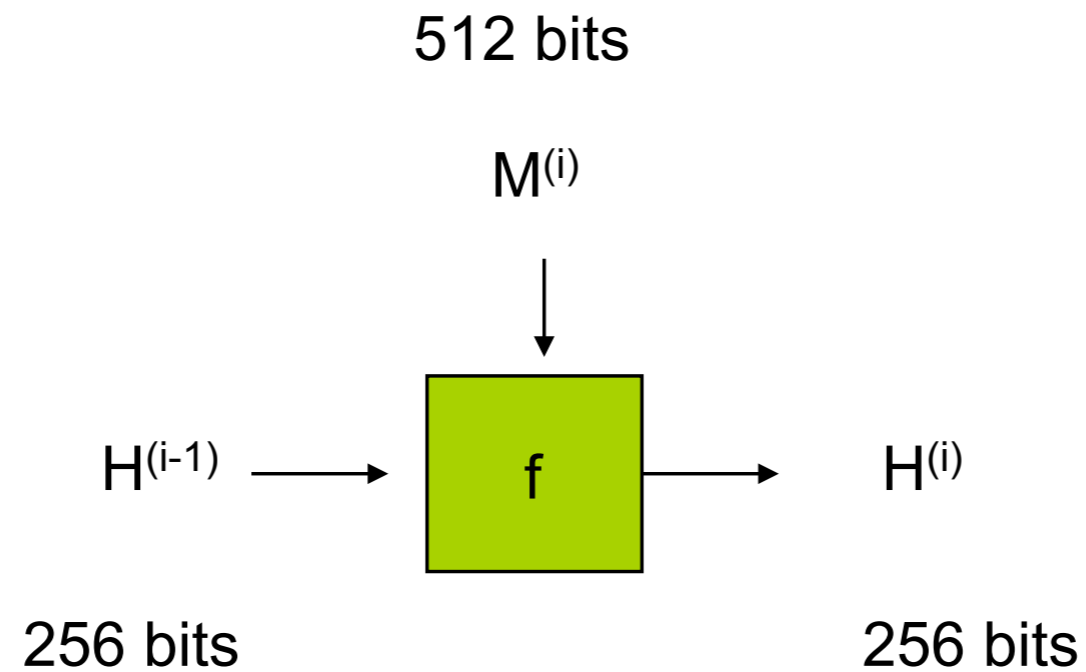
# SHA-256



- detailed specification can be found [here](#)
- $H(0) =$  6a09e667 bb67ae85 3c6ef372 a54ff53a  
510e527f 9b05688c 1f83d9ab 5be0cd19
- first 32 bits of fractional parts of square roots of 2,3,5,7,11,13,17

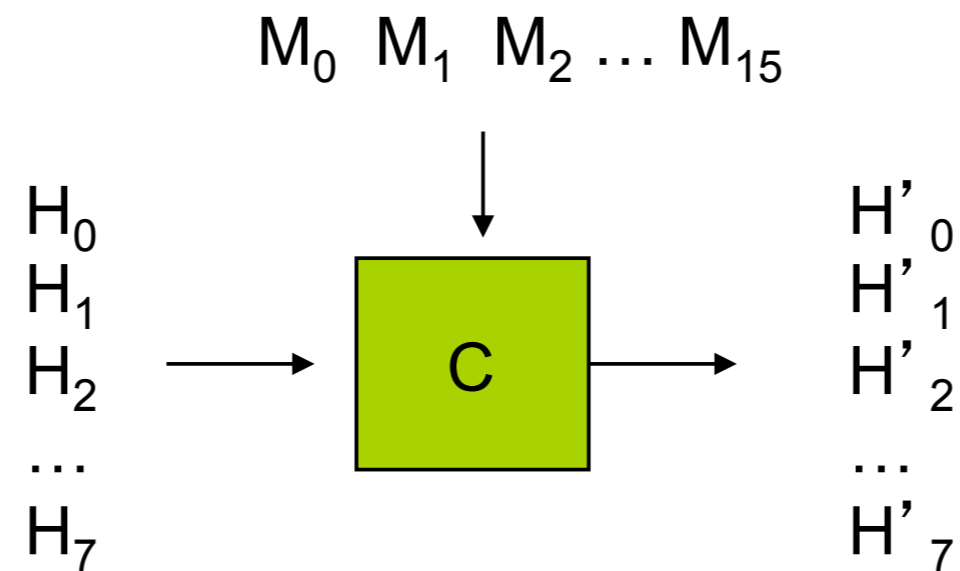


# SHA-256 compression function



# SHA-256 compression function

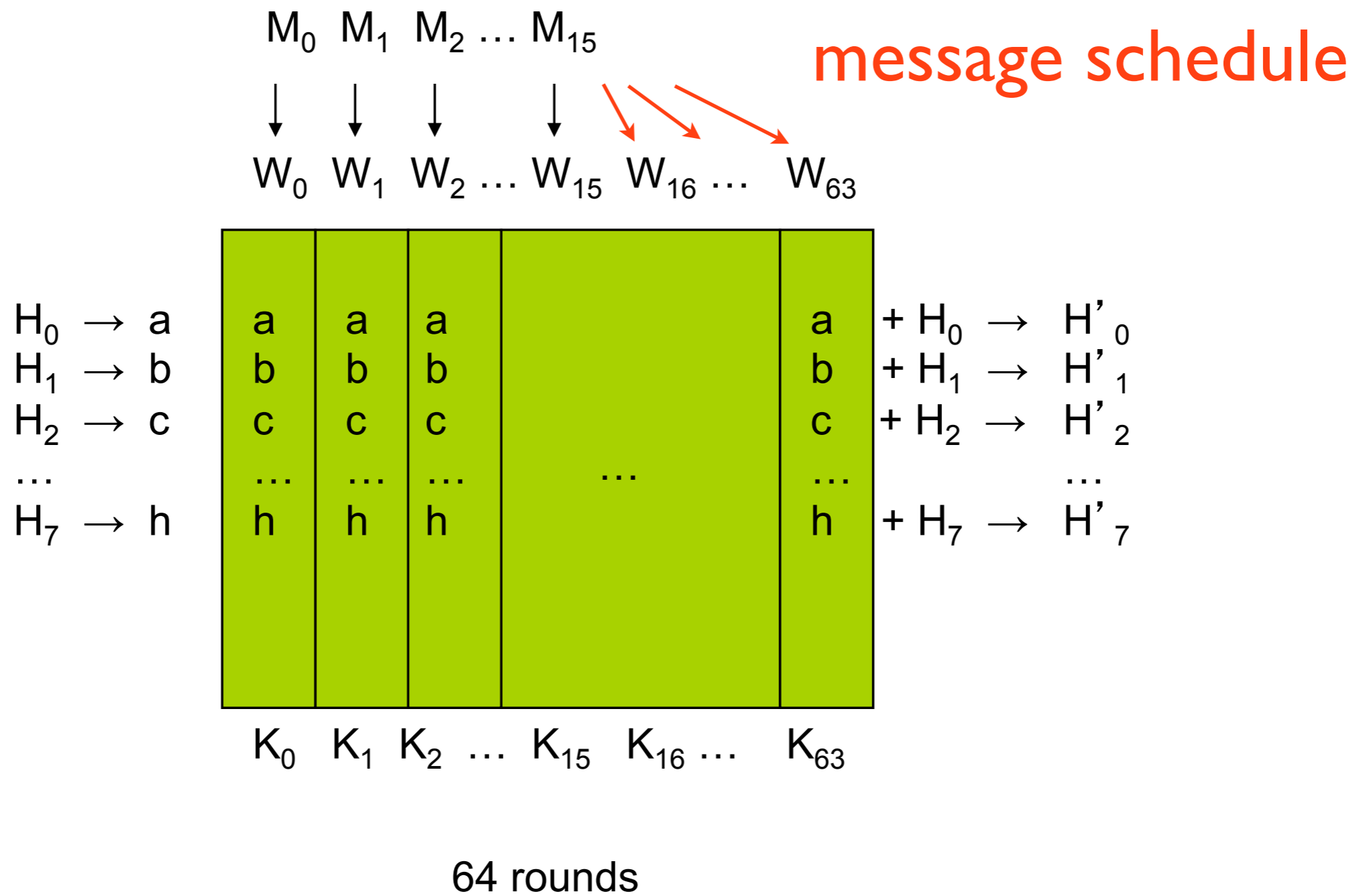
512 bits = 16 x 32 bit words



256 bits =  
8 x 32 bit words

256 bits =  
8 x 32 bit words

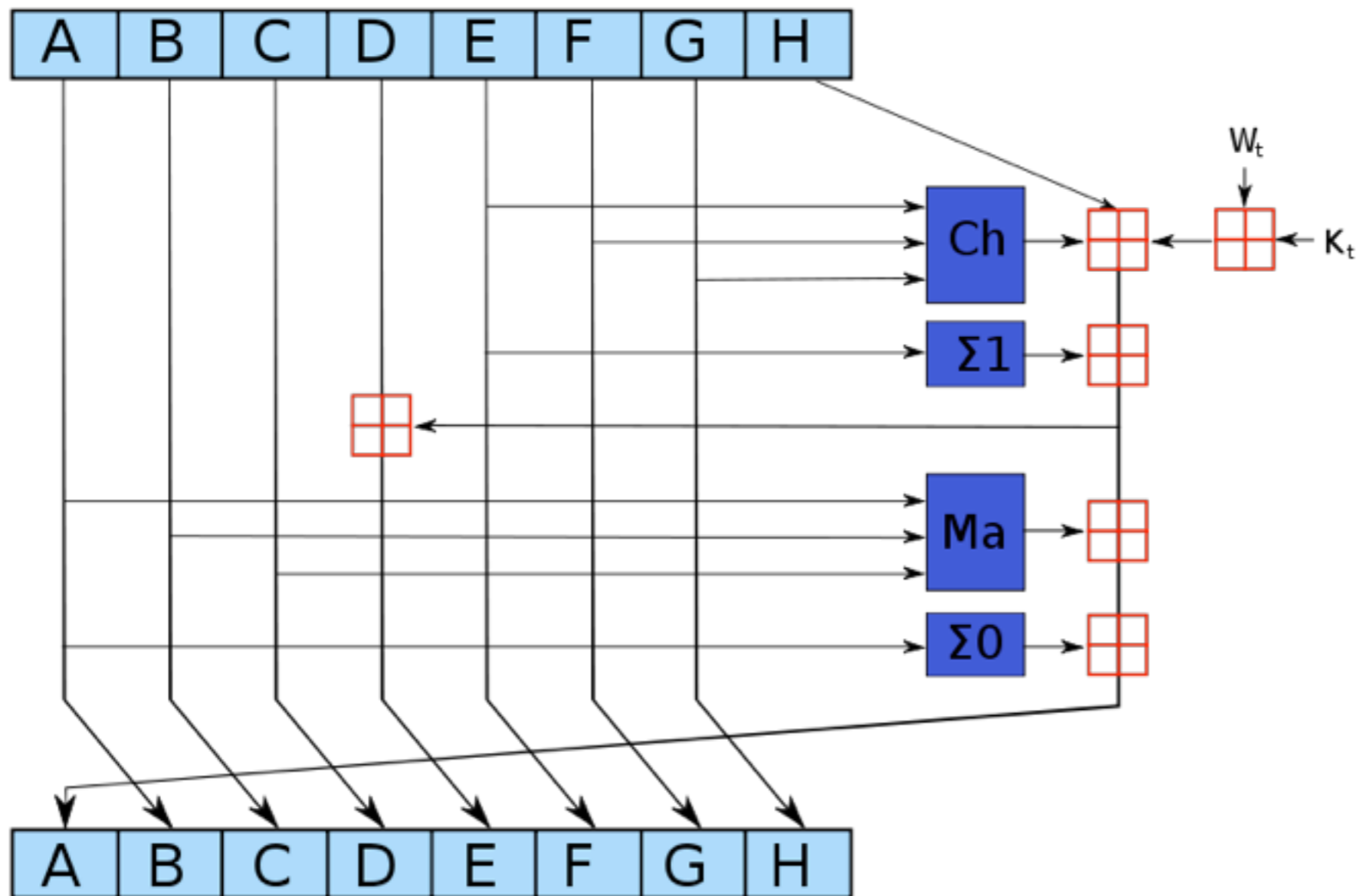
# SHA-256 compression function



# Message schedule

- $W_0 = M_0$
- ...
- $W_{15} = M_{15}$
- $W_{16} = W_0 + \sigma_0(W_1) + W_9 + \sigma_1(W_{14})$
- ...
- $W_{63} = W_{47} + \sigma_0(W_{48}) + W_{56} + \sigma_1(W_{61})$
  
- $\sigma_0(W) = \text{ROTR}^7(W) \oplus \text{ROTR}^{18}(W) \oplus \text{SHR}^3(W)$
- $\sigma_1(W) = \text{ROTR}^{17}(W) \oplus \text{ROTR}^{19}(W) \oplus \text{SHR}^{10}(W)$

# Single SHA-256 round



- $K_0 = 428a2f98$
- $K_1 = 71374491$
- ...
- $K_{63} = c67178f2$
- cube roots of first 64 primes

One iteration in a SHA-2 family compression function. The blue components perform the following operations:

$$\text{Ch}(E, F, G) = (E \wedge F) \oplus (\neg E \wedge G)$$

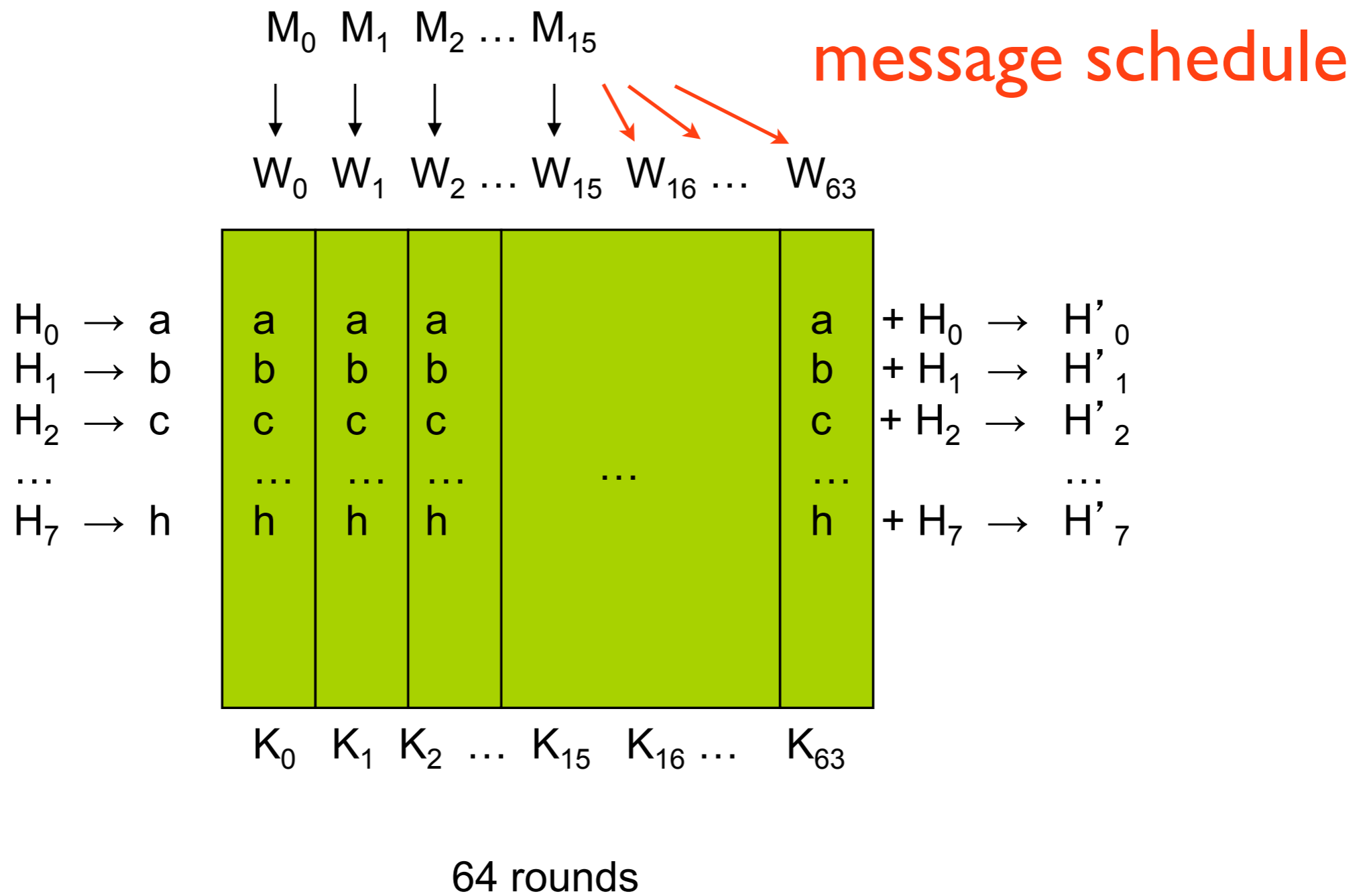
$$\text{Ma}(A, B, C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$

$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$

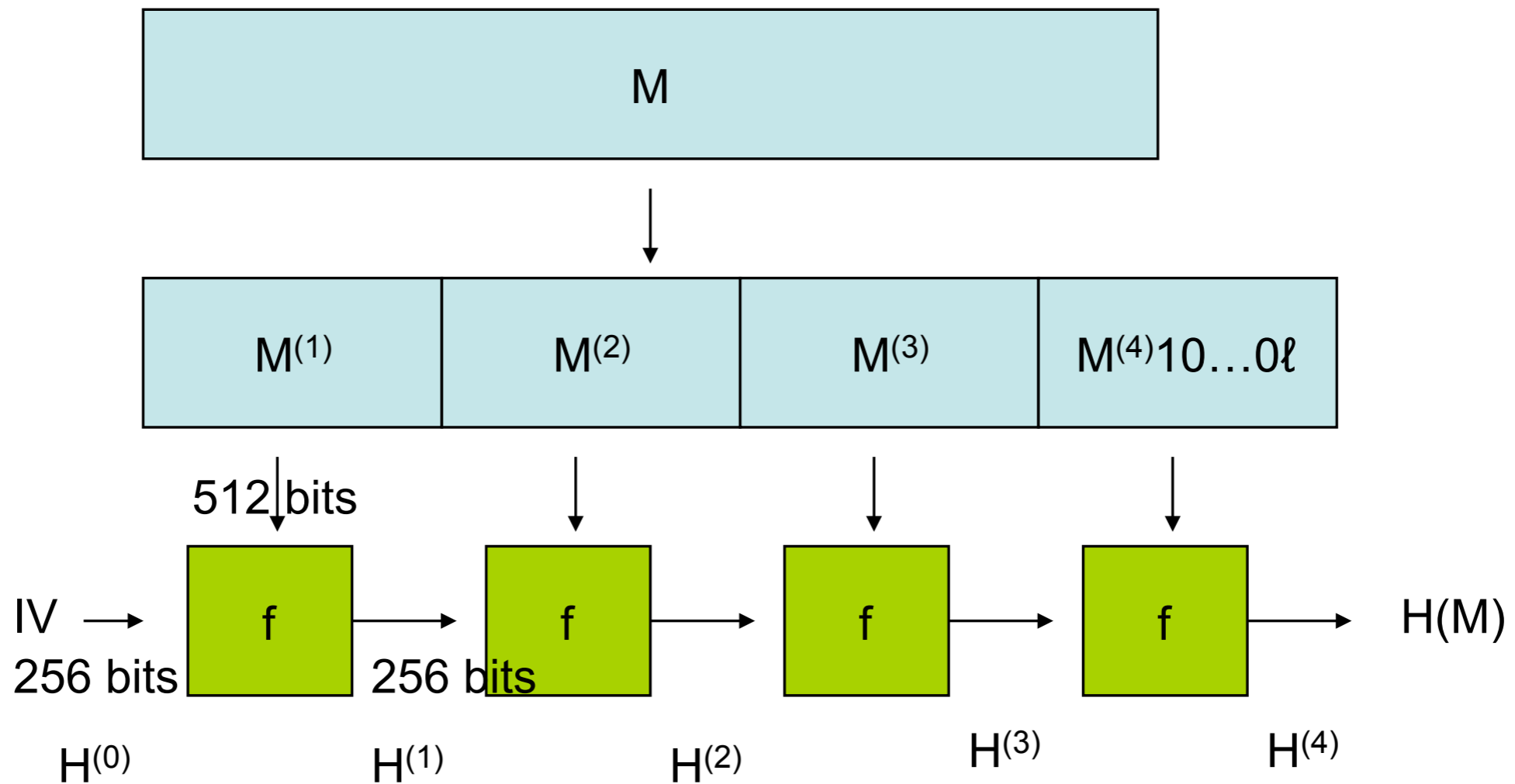
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$

The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256. The red  $\boxplus$  is an addition modulo  $2^{32}$ .

# SHA-256 compression function



# SHA-256



- SHA-256:  $\{0,1\}^* \rightarrow \{0,1\}^{256}$  for input messages of length  $|M| < 2^{64}$ , i.e.  $M$  of size at most 2 billion GigaBytes
- **believed to be hard** to find a collision

# Number Of Hashes to Find Collision

	Output bits	Birthday	Shortcut
MD4	128	$2^{64}$	$2^2$
RIPEMD	128	$2^{64}$	$2^{18}$
MD5	160	$2^{80}$	$2^{21}$
RIPEMD-160	160	$2^{80}$	
SHA-0	160	$2^{80}$	$2^{34}$
SHA-1	160	$2^{80}$	$2^{51}$
SHA-224	224	$2^{112}$	
SHA-256	256	$2^{128}$	



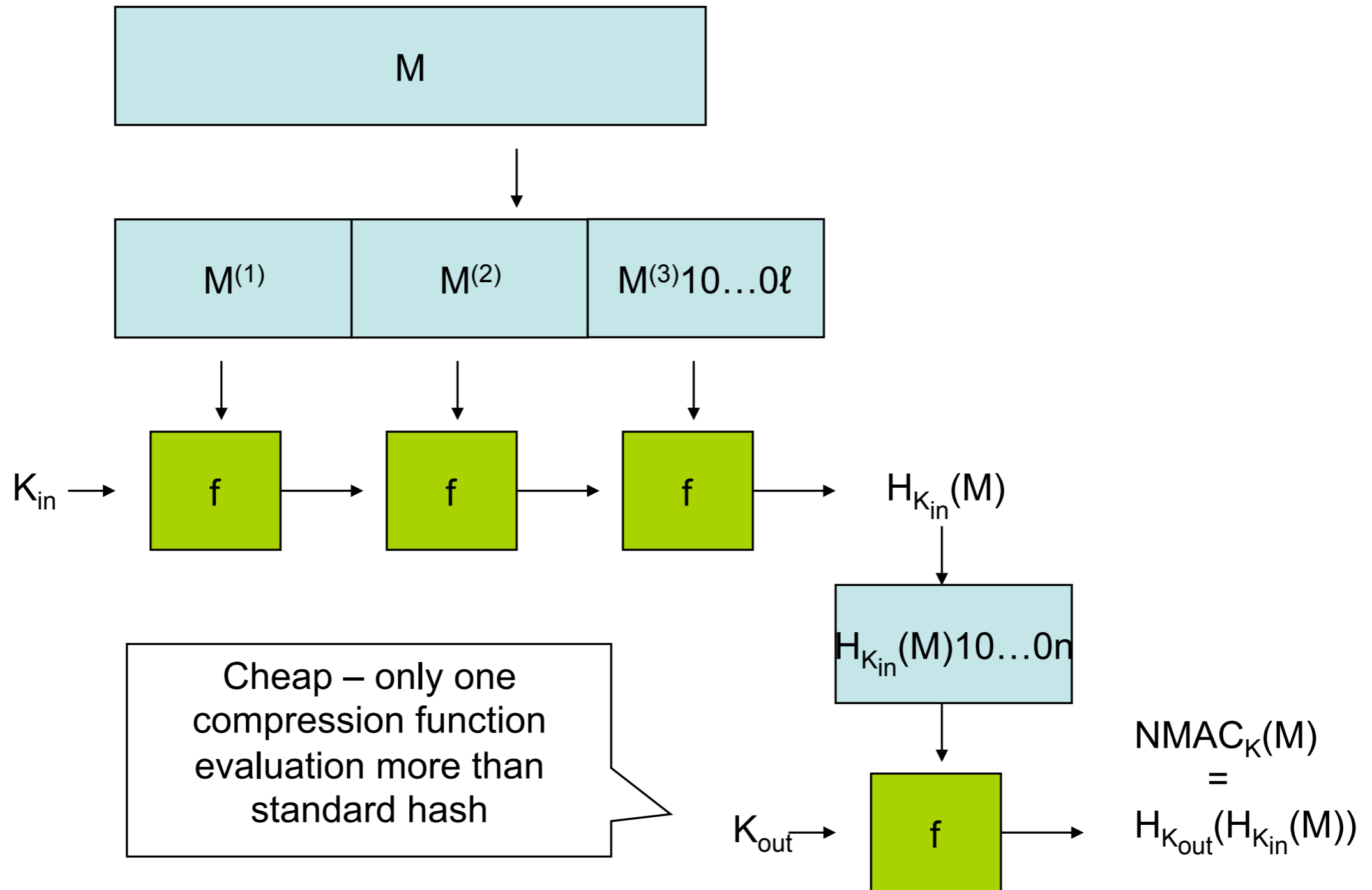
# Number Of Hashes to Find Collision

	Output bits	Birthday	Shortcut
MD4	128	$2^{64}$	$2^2$
RIPEMD	128	$2^{64}$	$2^{18}$
MD5	160	$2^{80}$	$2^{21}$
RIPEMD-160	160	$2^{80}$	
SHA-0			$2^{34}$
SHA-1			$2^{51}$
SHA-224	224	$2^{112}$	
SHA-256	256	$2^{128}$	

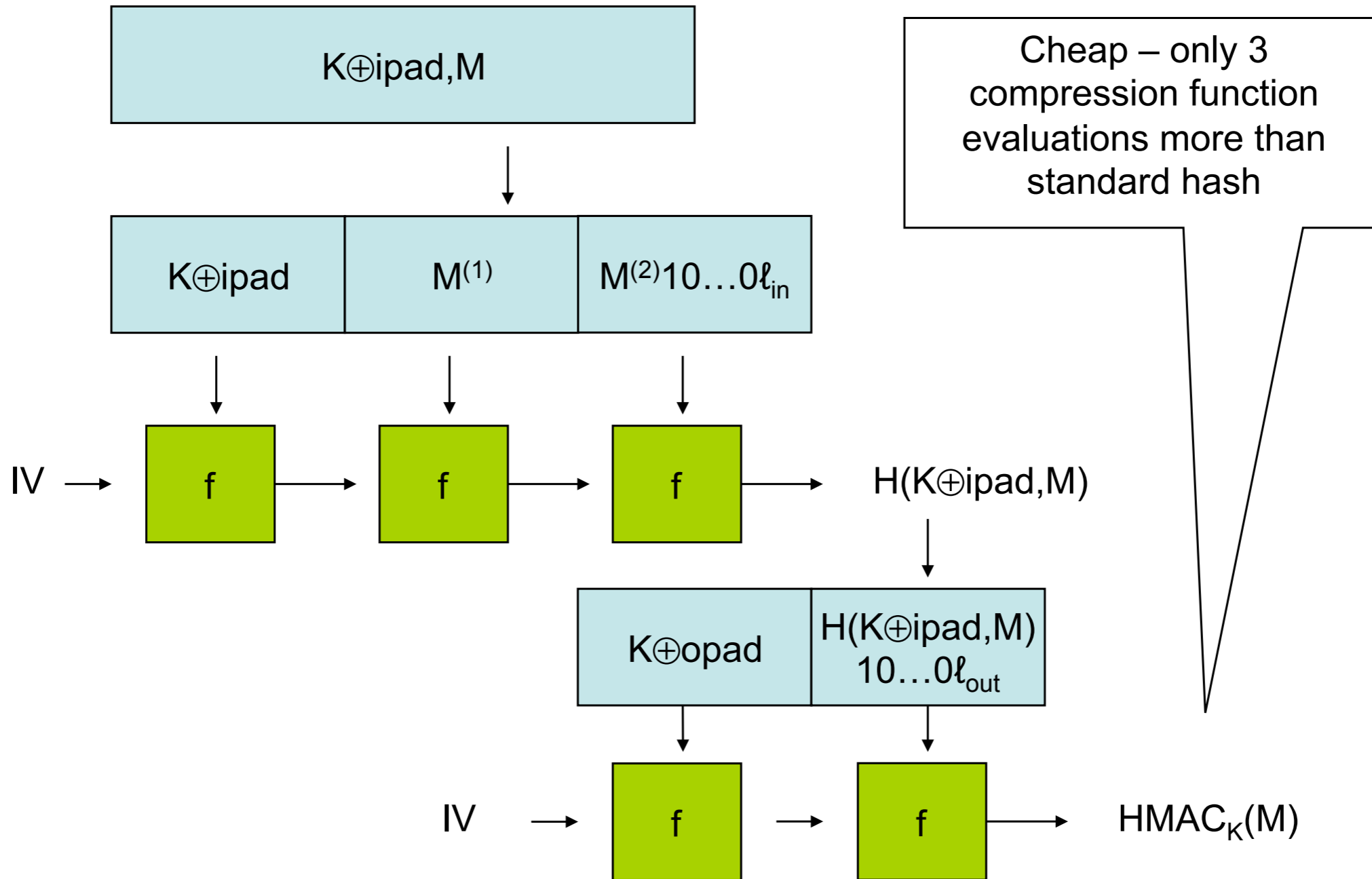
creating a rogue  
Certification Authority  
certificate

# MACs from Hash Functions

# NMAC-SHA-256



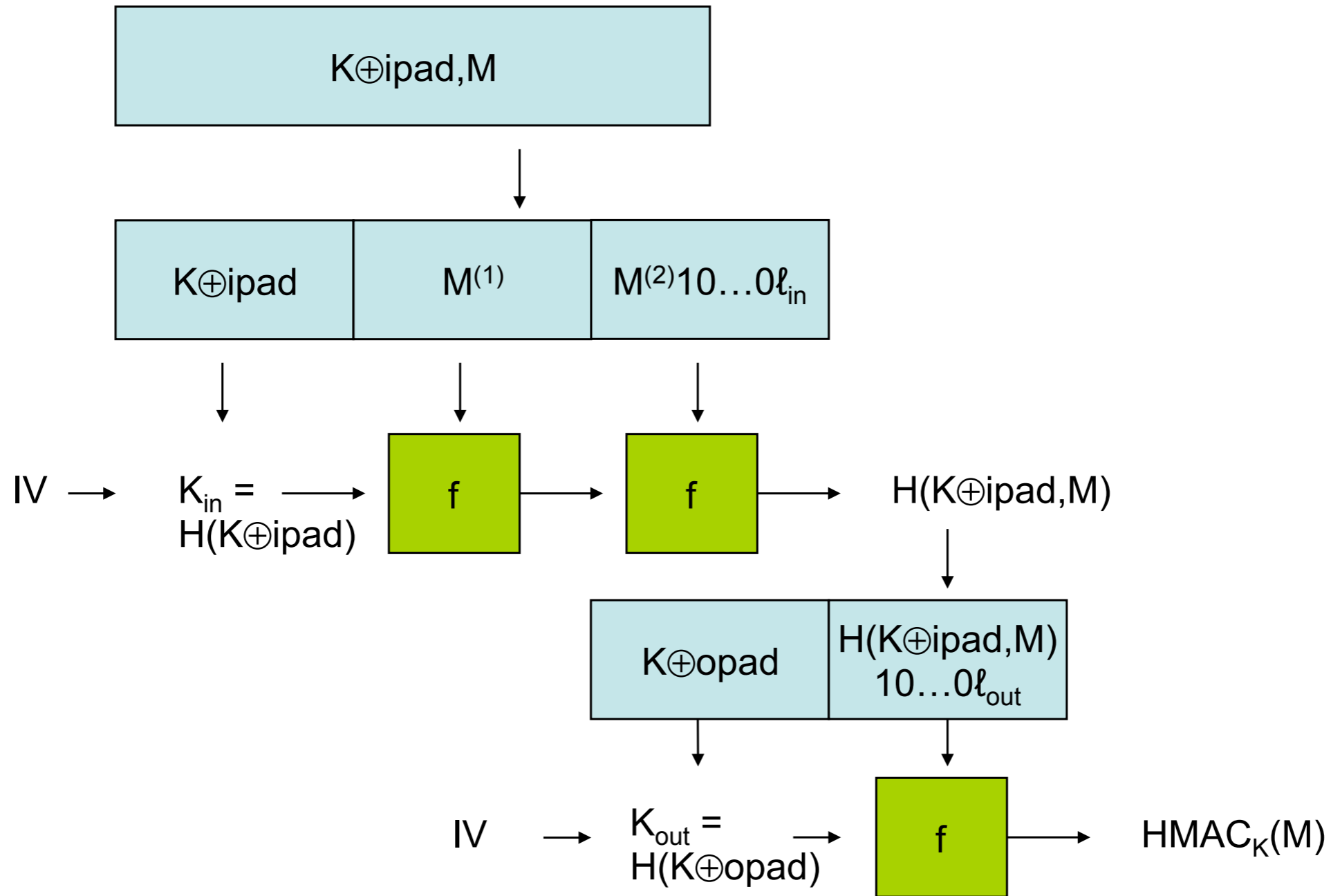
# HMAC-SHA-256



- $$\text{HMAC}_K(M) = H( K \oplus \text{opad}, H( K \oplus \text{ipad}, M ) )$$

$$\text{ipad} = 3636\dots 36, \quad \text{opad} = 5c5c\dots 5c$$

# HMAC vs NMAC



- HMAC can be seen as variant of NMAC
- as secure if  $H(x \oplus \text{ipad}), H(x \oplus \text{opad})$  is pseudorandom