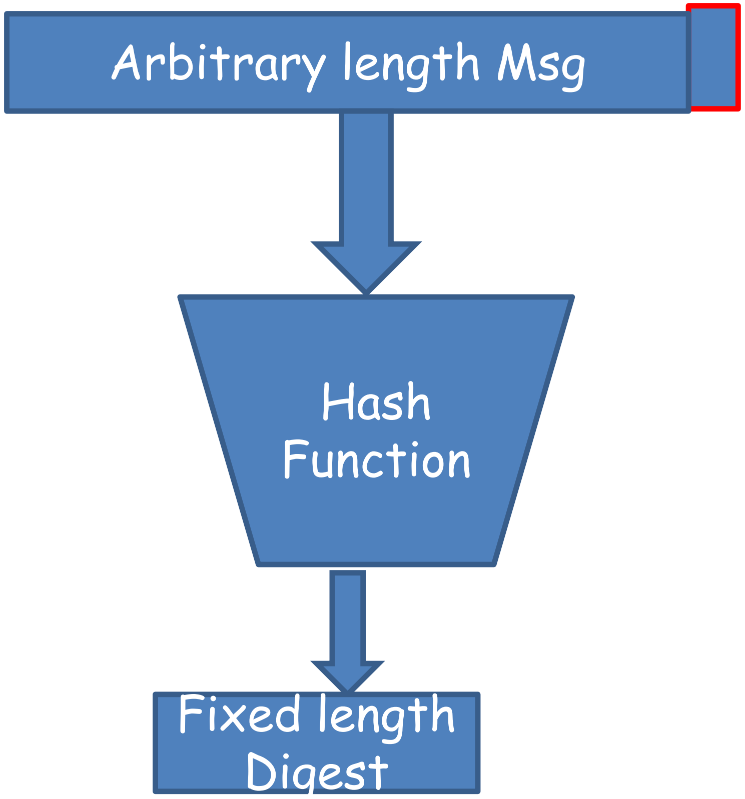
CS557: Cryptography

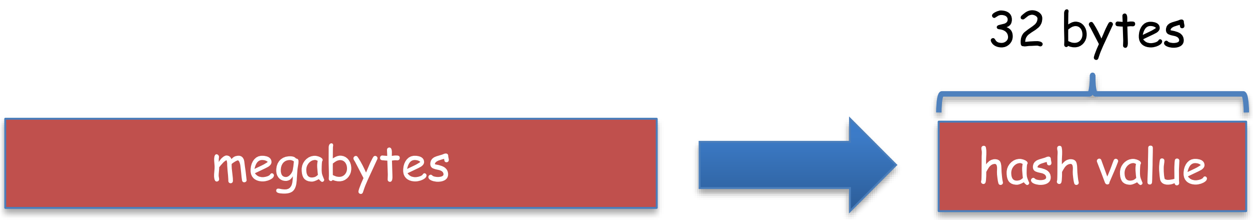
Cryptographic Hash Function III

S. Tripathy
IIT Patna

Cryptographic Hash Function

- Cryptographic hash functions:
  - An efficiently computable function
  - $H: M \rightarrow T$
  - where $|M| \gg |T|$





$T = \{0,1\}256$

Hash Functions

Effort Required for length = n-bit

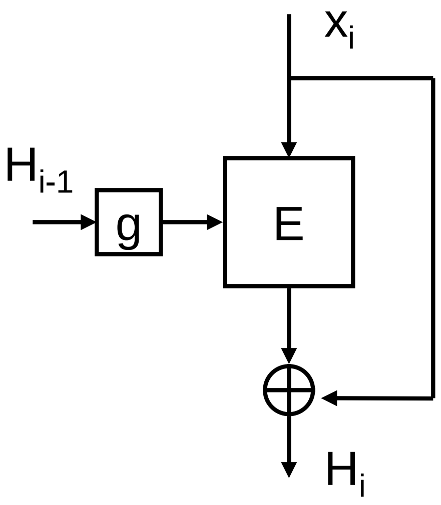
One Way / Pre-image	2^n
Weak Collision/ 2nd Pre-image Resistance	2^n
(Strong) Collision Resistance	$2^{n/2}$

- Finding collisions is easier than solving pre- image or second preimage

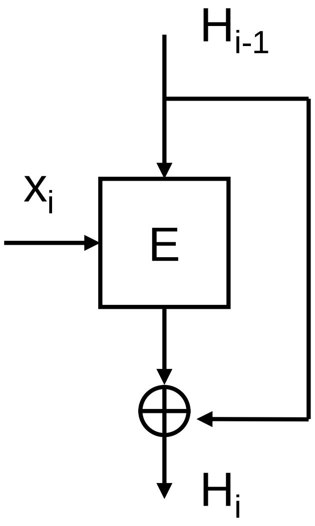
Block Ciphers as one-way Function (OWF)

- block ciphers can be used as hash functions
  - using H_0= initial value
  - compute: $H_i = E_{M_i} [H_{i-1}]$
  - and use final block as the hash value
  - similar to CBC but without a key
- resulting hash may be too small (64-bit) if DES like block ciphers used
  - Due to direct birthday attack
- other variants also susceptible to attack

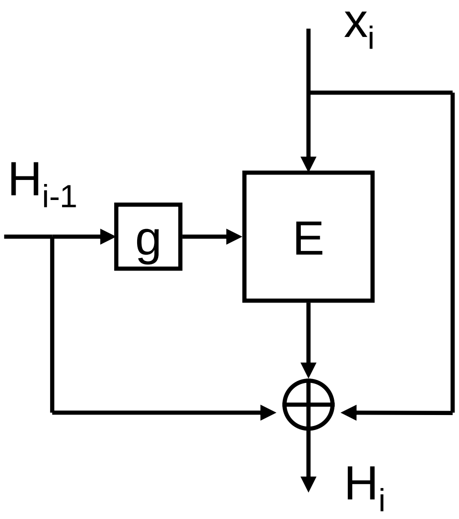
Single length MDCs



Matyas-Meyer-Oseas



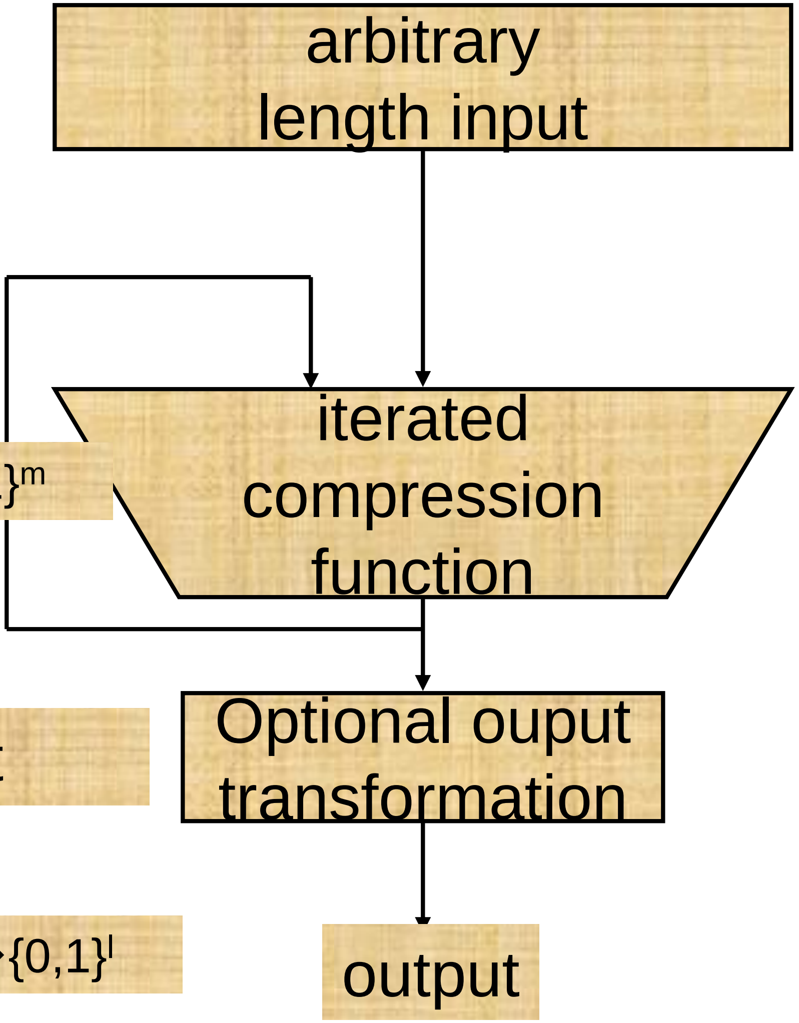
Davis-Meyer



Miyaguchi-Preneel

Iterated hash functions

Issues ?



arbitrary length input

iterated compression function

Optional ouput transformation

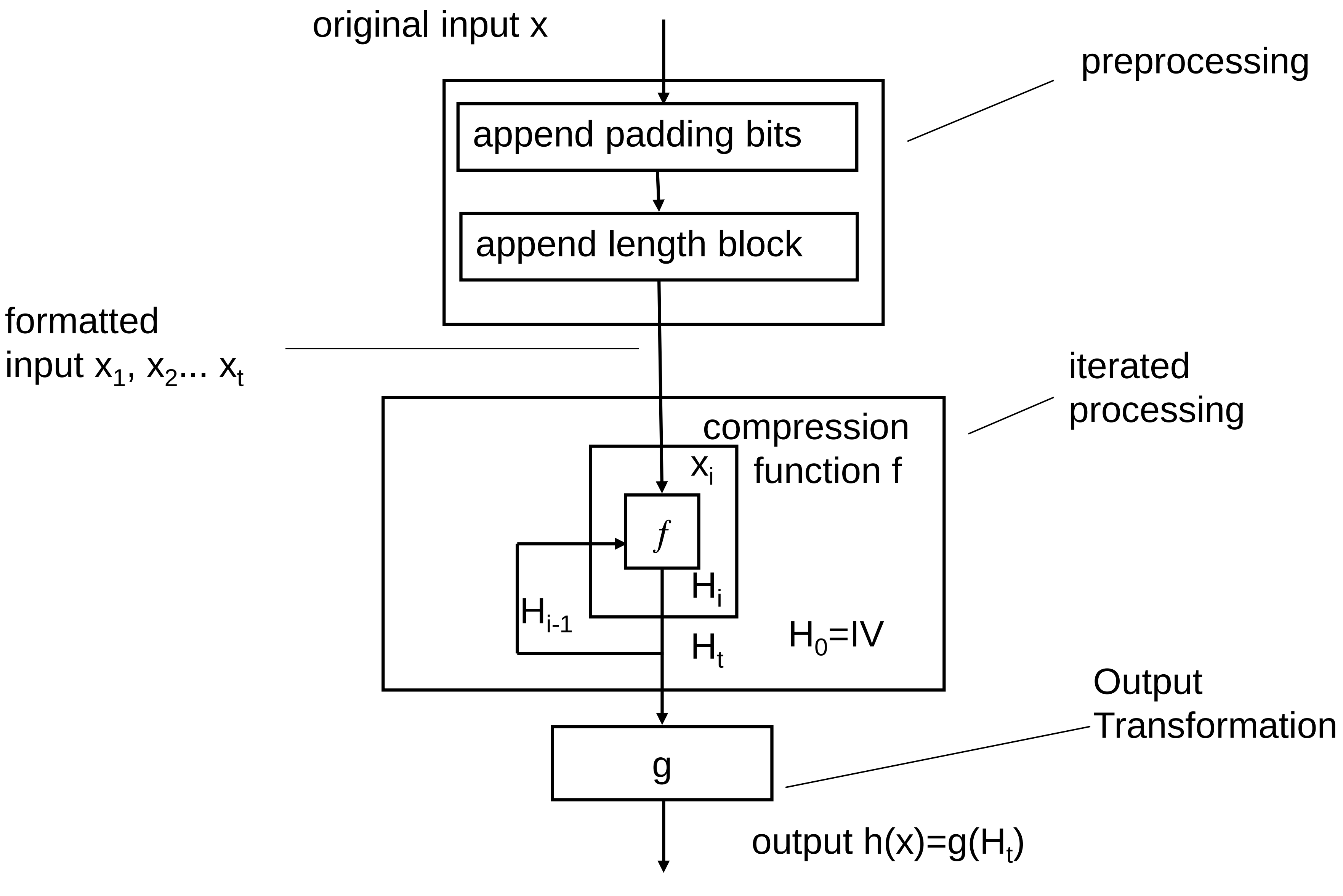
output

Compress: $\{0,1\}^{m+t} \rightarrow \{0,1\}^{m}$

fixed length output

Output trans: $\{0,1\}^{m} \rightarrow \{0,1\}^{l}$

Detailed view of Hash Function



original input x

preprocessing

append padding bits

append length block

formatted
input $x_1, x_2 \ldots x_t$

iterated
processing

compression
function f

x_i

f

H_i

H_{i-1}

H_t

H_0=IV

Output
Transformation

g

output $h(x)=g(H_t)$

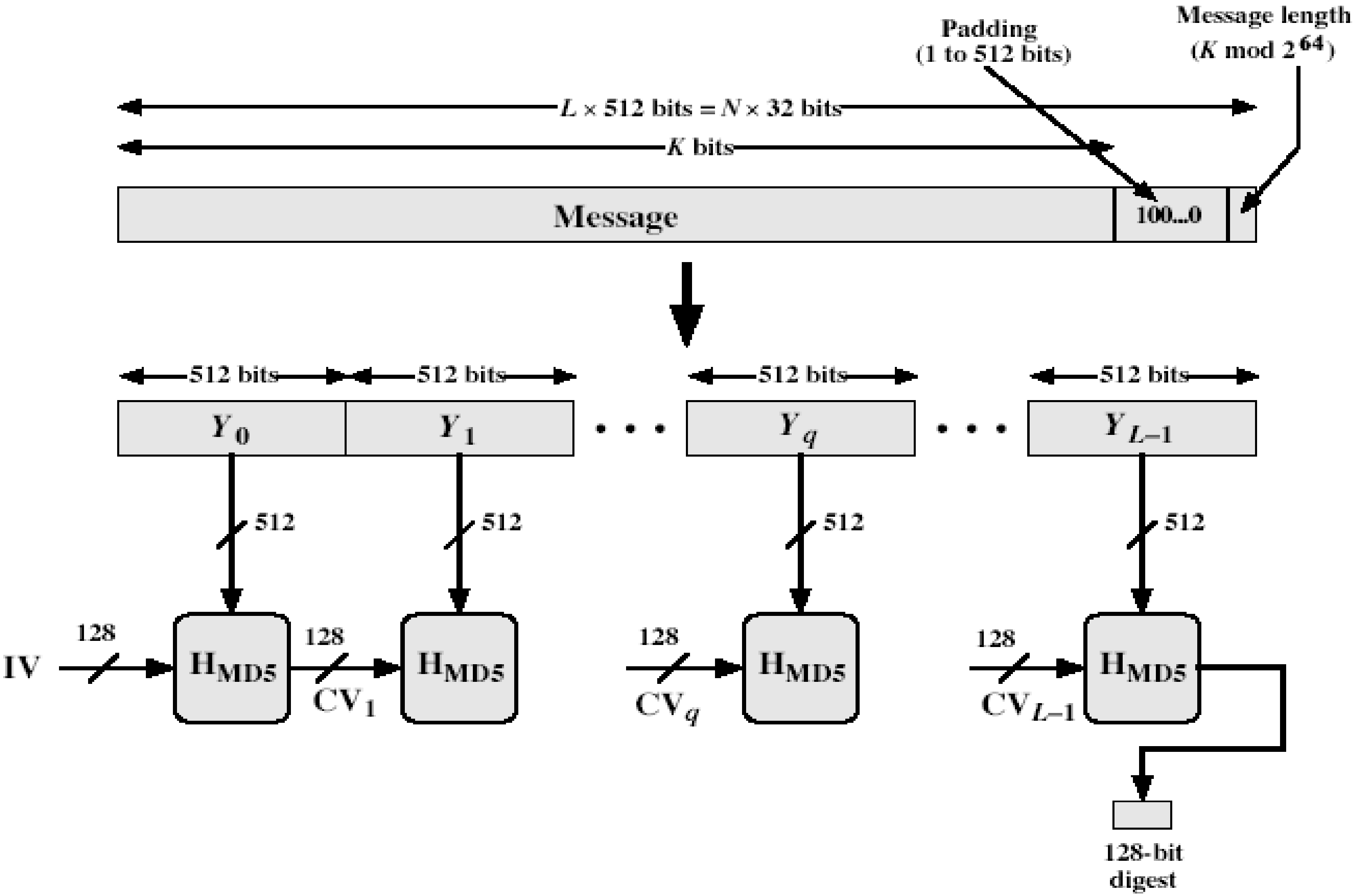
MD4

- precursor to MD5
- also produces a 128-bit hash of message
- has 3 rounds of 16 steps vs 4 in MD5
- design goals:
    - collision resistant (hard to find collisions)
    - direct security (no dependence on "hard" problems)
    - fast, simple, compact
    - favours little-endian systems (eg PCs)

MD5

- designed by Ronald Rivest
- latest in a series of MD2, MD4,
- we have MD6 also
- produces a 128-bit hash value
- widely used hash algorithm
  - in recent times have both brute-force & cryptanalytic concerns
- specified as Internet standard RFC1321

MD5 Overview

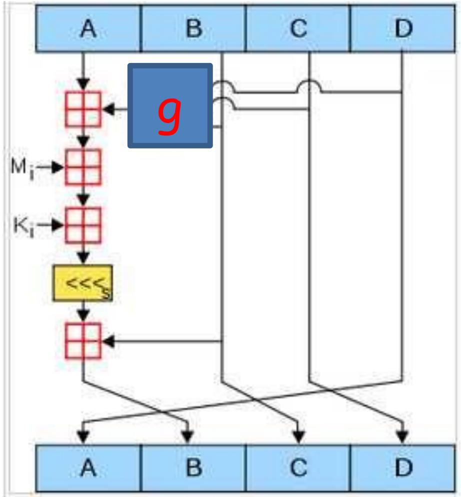


each round has 16 steps of the form:
$B = B+((A+g(B,C,D)+X[k]+T[i])<<<s)$
T[i] is a constant value (i^{th} 32-bit word in matrix T) derived from sin

X[k] is M[q x 16 + k], the k^{th} 32-bit word in the q^{th} 512-bit block of the message

<<<s is circular left shift of the 32-bit argument by s bits

IV: h1 = 0x67452301, h2 = 0xefcdab89, h3 = 0x98badcfe, h4 = 0x10325476



$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

$CV_0 = IV$

$CV_{q+1} = SUM_{32}[CV_q, I(Y_q, H(Y_q, G(Y_q, F(Y_q, CV_q))))]$

$MD = CV_{L-1}$

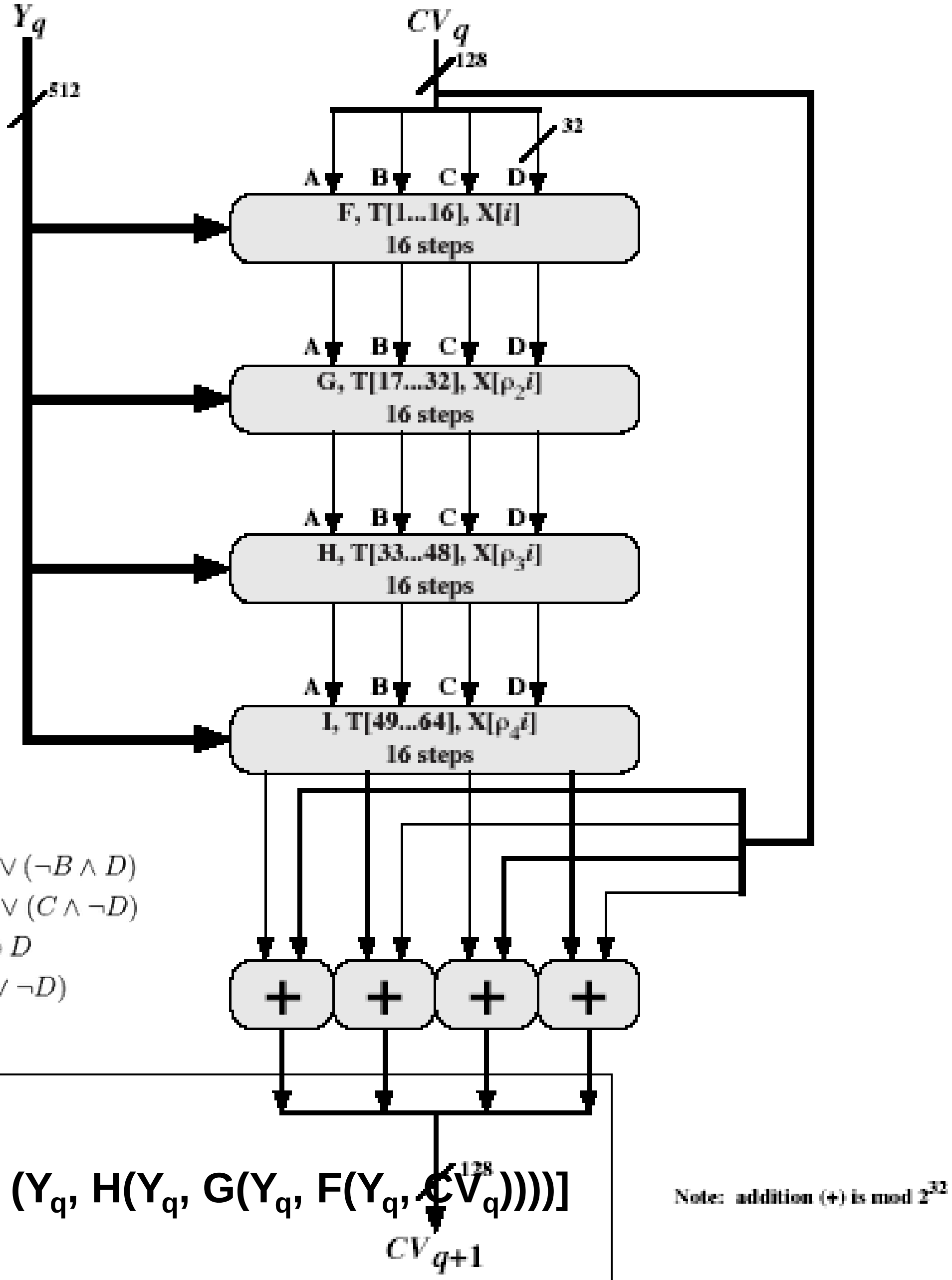

Y_q
512
CV_q
128
32
A
B
C
D
F, T[1...16], X[i]
16 steps
A
B
C
D
G, T[17...32], X[$\rho_2 i$]
16 steps
A
B
C
D
H, T[33...48], X[$\rho_3 i$]
16 steps
A
B
C
D
I, T[49...64], X[$\rho_4 i$]
16 steps
+
+
+
+
128
CV_{q+1}
Note: addition (+) is mod 2^{32}

Figure MD5 Processing of a Single 512-bit Block

Strength of MD5

- Rivest claims security is good as can be
  - MD5 hash is dependent on all message bits
- known attacks are:
  - Berson 92 attacked any 1 round using differential cryptanalysis (but can't extend)
  - Boer & Bosselaers 93 found a pseudo collision (again unable to extend)
  - Dobbertin 96 created collisions on MD compression function (but initial constants prevent exploit)
- conclusion is that MD5 looks vulnerable
- *Reading ass: Anton A. Kuznetsov. "An algorithm for MD5 single-block collision attack using highperformance computing cluster*

- Thanks