北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《现代密码学》第六讲

HASH函数和MAC（一）

上讲内容回顾

北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- OTP与伪随机数生成器
- 流密码技术的发展
- 基于LFSR的PRG
- RC4算法
- Estream 算法举例
- PRG安全与流密码安全应用

本讲主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

本讲主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

Hash函数定义及安全目标

- Hash函数 **H**：$\{0,1\}^* \rightarrow \{0,1\}^n$又称为改动检测码 **MDC** (manipulation detection code)，杂凑函数、哈希函数等等。
- 原像空间$\{0,1\}^*$称为消息空间，又可用M表示，消息是任意有限长度；
- 像空间$\{0,1\}^n$称为hash值空间，hash值（散列值、消息摘要）长度固定为n.
- 信息安全属性：完整性

Hash函数定义及安全目标

单向函数定义：

函数 $f:\{0,1\}^* \rightarrow \{0,1\}^*$若满足下列两个条件，则称之为强单向函数：

1）计算f(x)是容易的，即f(x)是多项式时间可计算的；

2）计算f函数的逆$f^{-1}(x)$是困难的，即对每一多项式时间概率算法M，每一多项式p(n)和充分大的$n(n>n_0)$有

$$\Pr\{M(f(U_n)) \in f^{-1}(f(U_n))\} < 1/p(n)$$

Hash函数定义及安全目标

- 单向性（抗原像）：对于任意给定的消息，计算其哈希值容易．但是，对于给定的哈希值h，要找到M使得H(M)＝h在计算上是不可行的.
- 弱抗碰撞（抗二次原像）：对于给定的消息M_1，要发现另一个消息M_2，满足H(M_1)＝H(M_2)在计算上是不可行的.
- 强抗碰撞：找任意一对不同的消息M_1, M_2 ，使H(M_1)＝H(M_2)在计算上是不可行的.

Hash函数定义及安全目标

- 生日悖论

如果一个房间里有23个或23个以上的人，那么至少有两个人的生日相同的概率要大于50%

- 生日悖论

Th：令$r_1, \ldots, r_n \in \{1,\ldots,N\}$是相互独立的同分布整数，当$n = 1.2 \times N^{1/2}$时，

$$\Pr[\exists i \neq j: \ r_i = r_j] \geq \frac{1}{2}$$

Hash函数定义及安全目标

- 生日攻击

令$H:\{0,1\}^* \rightarrow \{0,1\}^n$ 是一个hash函数.

1. 从$\{0,1\}^*$中任选$2^{n/2}$个元素： $m_1, \ldots, m_{2^{n/2}}$
2. 对 $i = 1,\ldots,2^{n/2}$分别计算$t_i = H(m_i) \in \{0,1\}^n$
3. 寻找碰撞$t_i = t_j$. 若碰撞不存在，则返回第1步重新执行.

根据生日悖论，期望的迭代次数≈2

时间复杂度:$O(2^{n/2})$　　空间复杂度：$O(2^{n/2})$

本讲主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

Hash函数的发展现状

Hash的概念起源于1956年，Dumey用它来解决符号表问题。使得数据表的插入、删除、查询操作可以在平均常数时间完成。

1978年，Merkle和Damagad分别独立设计了MD迭代结构。
1983年，Davies提出一种使用DES构造压缩函数的方法。

1984年，Winternitz首次研究了Davies–Meyer构造的安全性。

Hash函数的发展现状

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

散列算法MD族是在90年代初由mit laboratory for computer science和RSA data security inc的Ron·Rivest设计的，MD代表消息摘要（message-digest）.
md2、md4和md5都产生一个128位的信息摘要.

- **MD2**
  1989年开发出md2算法. 在这个算法中，首先对信息进行数据补位，使信息的字节长度是16的倍数. 然后，以一个16位的检验和追加到信息末尾。
- **MD4**
  1990年开发出md4算法.
- **MD5**
  1991年，Rivest开发出技术上更为趋近成熟的md5算法.
- **RIPEMD-128/160/320**
  RIPEMD由欧洲财团开发和设计.

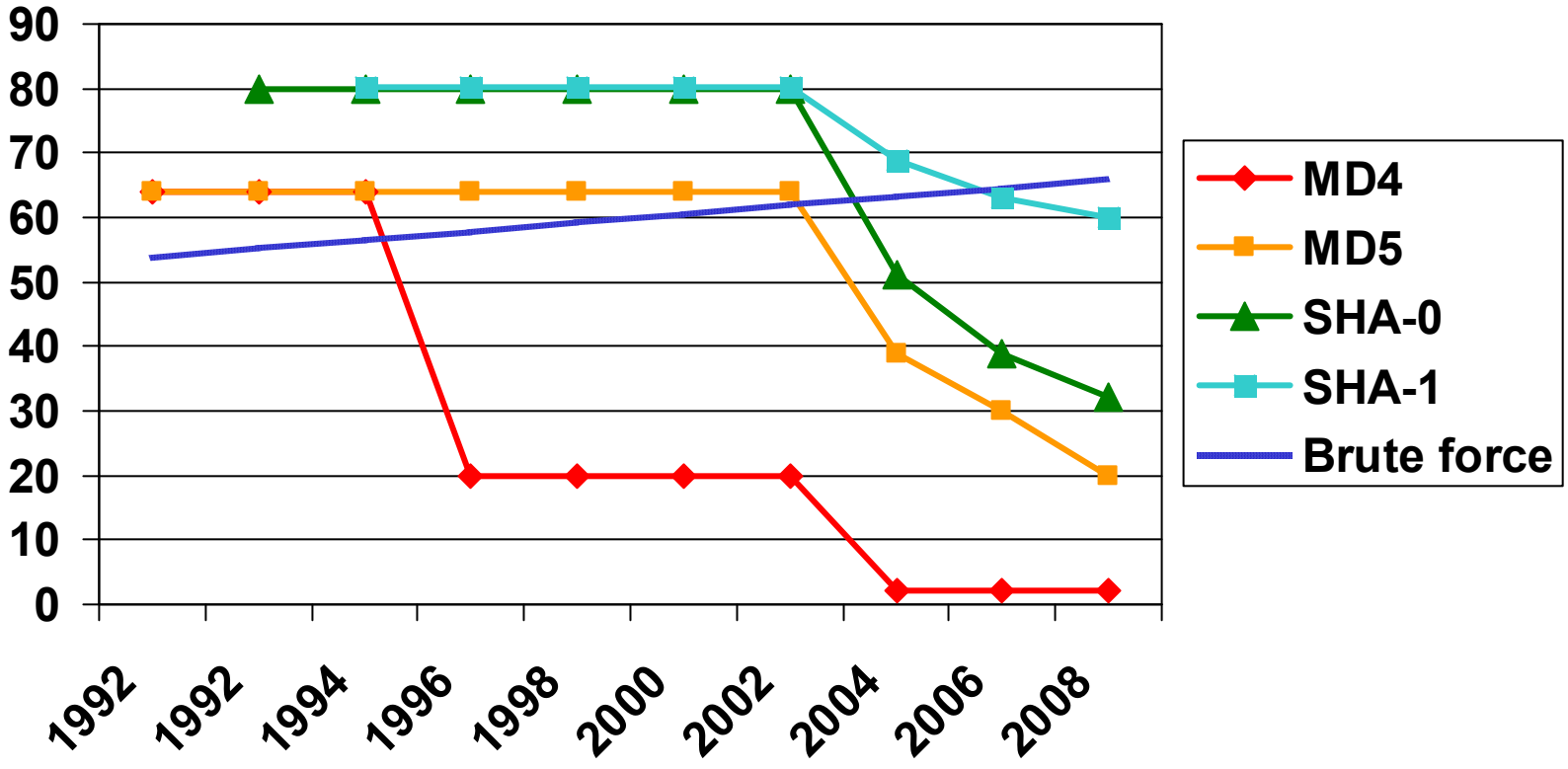
Hash函数的发展现状

SHA系列算法是NIST 根据Rivest 设计的MD4和MD5开发的算法. 国家安全当局发布SHA作为美国政府标准. SHA表示安全散列算法.

- SHA-0
  SHA-0正式地称作SHA，这个版本在发行后不久被指出存在弱点.
- SHA-1
  SHA-1是NIST于1994年发布的，它与MD4和MD5散列算法非常相似，被认为是MD4和 MD5的后继者.
- SHA-2
  SHA-2实际上分为SHA-224、SHA-256、SHA-384和SHA-512算法.

Hash函数的发展现状

强力攻击: 1 million PCs or US$ 100 000 hardware



碰撞攻击复杂度

Hash函数的发展现状

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- NESSIE工程推荐使用的hash算法有SHA-256/384/512和Whirlpool;
- 日本密码研究与评估委员会推荐使用的算法有RIPEMD-160、SHA-256/384/512。
- ECRYPT也在hash算法研究方面举办了一系列活动。
- 此外，NIST于2008年启动新的hash标准的征集活动。
  - 除迭代结构以外的结构
  - 适用于任何平台的压缩函数
- 2008年10月提交文档，收到64个算法，公开56个，51个进入第一轮评估
- 2009年10月，第二轮评估开始，剩余14个算法

Hash函数的发展现状

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 2011年，剩余五个算法

Hash Name	Principal Submitter	Best Attack on Main NIST Requirements	Best Attack on other Hash Requirements
BLAKE	Jean-Philippe Aumasson		
Grøstl	Lars R. Knudsen		
JH	Hongjun Wu	preimage	
Keccak	The Keccak Team		
Skein	Bruce Schneier		

- 2012年10月Keccak 成为SHA-3 standard

Hash Name	Principal Submitter	Best Attack on Main NIST Requirements	Best Attack on other Hash Requirements
Keccak	The Keccak Team		

GM/T 0004-2012《SM3密码杂凑算法》

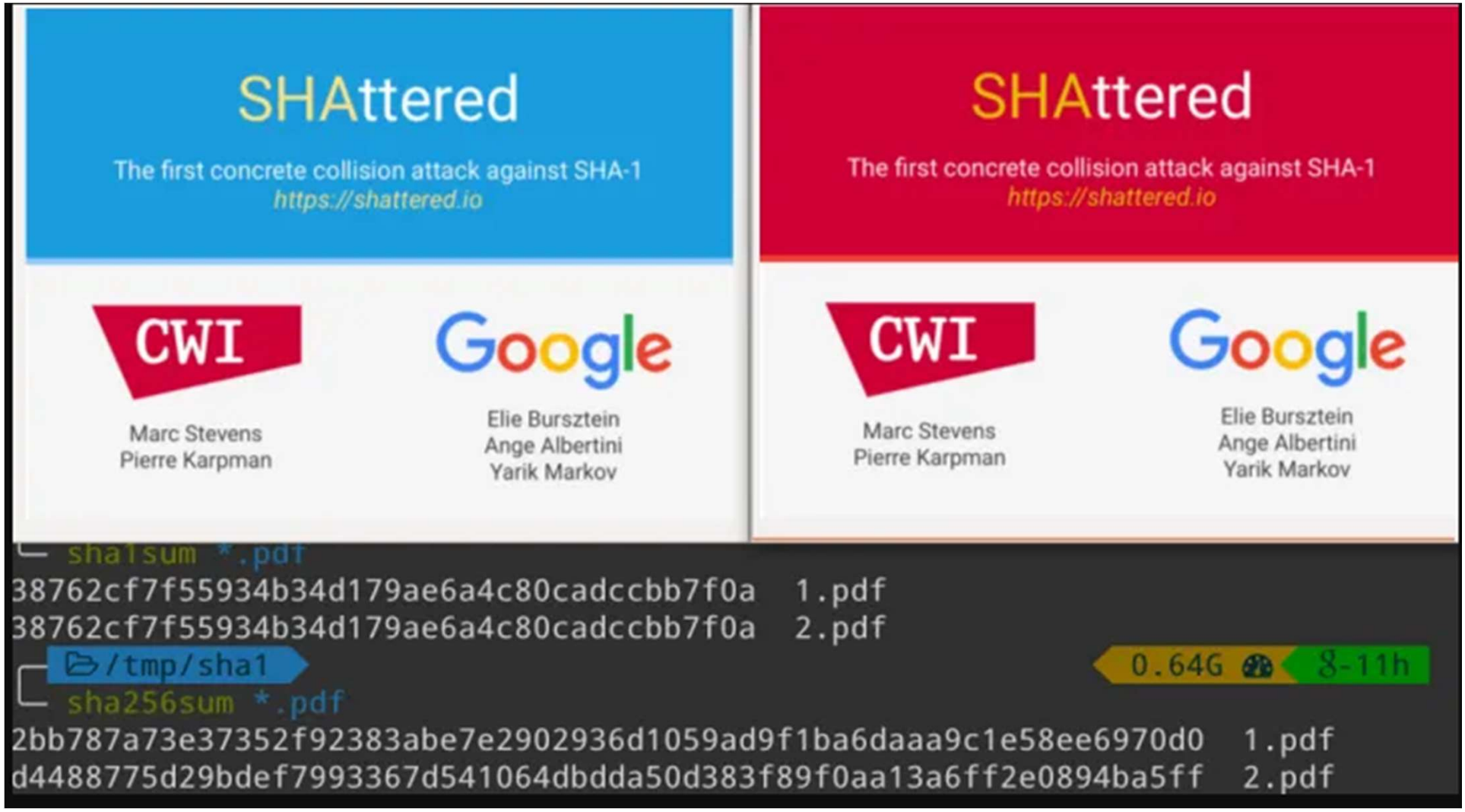
BUPT ISC 信息安全中心

Hash函数的发展现状

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 2017年2月，Marc Stevens[1]，Elie Bursztein[2]，Pierre Karpman[1]，Ange Albertini[2]，Yarik Markov[2]，([1]CWI Amsterdam 和 [2]Google Research)
- 两个内容不同的 pdf 文件，但拥有相同的 SHA-1 哈希值.
- $2^{63.1}$ SHA-1 压缩 和约6500 CPU years 和 100 GPU years.
- https://shattered.io

Hash函数的发展现状



Comparison of SHA functions

view • talk • edit

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security against collision attacks (bits)	Security against length extension attacks (bits)	Performance on Skylake (median cpb)[1]		First published
									Long messages	8 bytes	
MD5 (as reference)		128	128 (4 × 32)	512	4 (16 operations in each round)	And, Xor, Or, Rot, Add (mod 2^{32})	≤ 18 (collisions found)[2]	0	4.99	55.00	1992
SHA-0		160	160 (5 × 32)	512	80	And, Xor, Or, Rot, Add (mod 2^{32})	< 34 (collisions found)	0	≈ SHA-1	≈ SHA-1	1993
SHA-1							< 63 (collisions found)[3]		3.47	52.00	1995
SHA-2	*SHA-224*	224	256 (8 × 32)	512	64	And, Xor, Or, Rot, Shr, Add (mod 2^{32})	112	32	7.62	84.50	2004
	SHA-256	256					128	0	7.63	85.25	2001
	SHA-384	384	512 (8 × 64)	1024	80	And, Xor, Or, Rot, Shr, Add (mod 2^{64})	192	128	5.12	135.75	2001
	SHA-512	512					256	0[4]	5.06	135.50	2001
	SHA-512/224	224					112	288	≈ SHA-384	≈ SHA-384	2012
	SHA-512/256	256					128	256			
SHA-3	*SHA3-224*	224	1600 (5 × 5 × 64)	1152	24[5]	And, Xor, Rot, Not	112	448	8.12	154.25	2015
	SHA3-256	256		1088			128	512	8.59	155.50	
	SHA3-384	384		832			192	768	11.06	164.00	
	SHA3-512	512		576			256	1024	15.88	164.00	
	SHAKE128	*d* (arbitrary)		1344			min(*d*/2, 128)	256	7.08	155.25	
	SHAKE256	*d* (arbitrary)		1088			min(*d*/2, 256)	512	8.59	155.50	

Hash函数的发展现状

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

- 2023年3月

Ambush attacks on 160bit objectIDs & addresses

by Mysten Labs cryptography team *March 27, 2023*

The cost of 160bit hash collision attacks is in the feasibility range of just a few millions $, making it possible even for non-statewide adversaries.

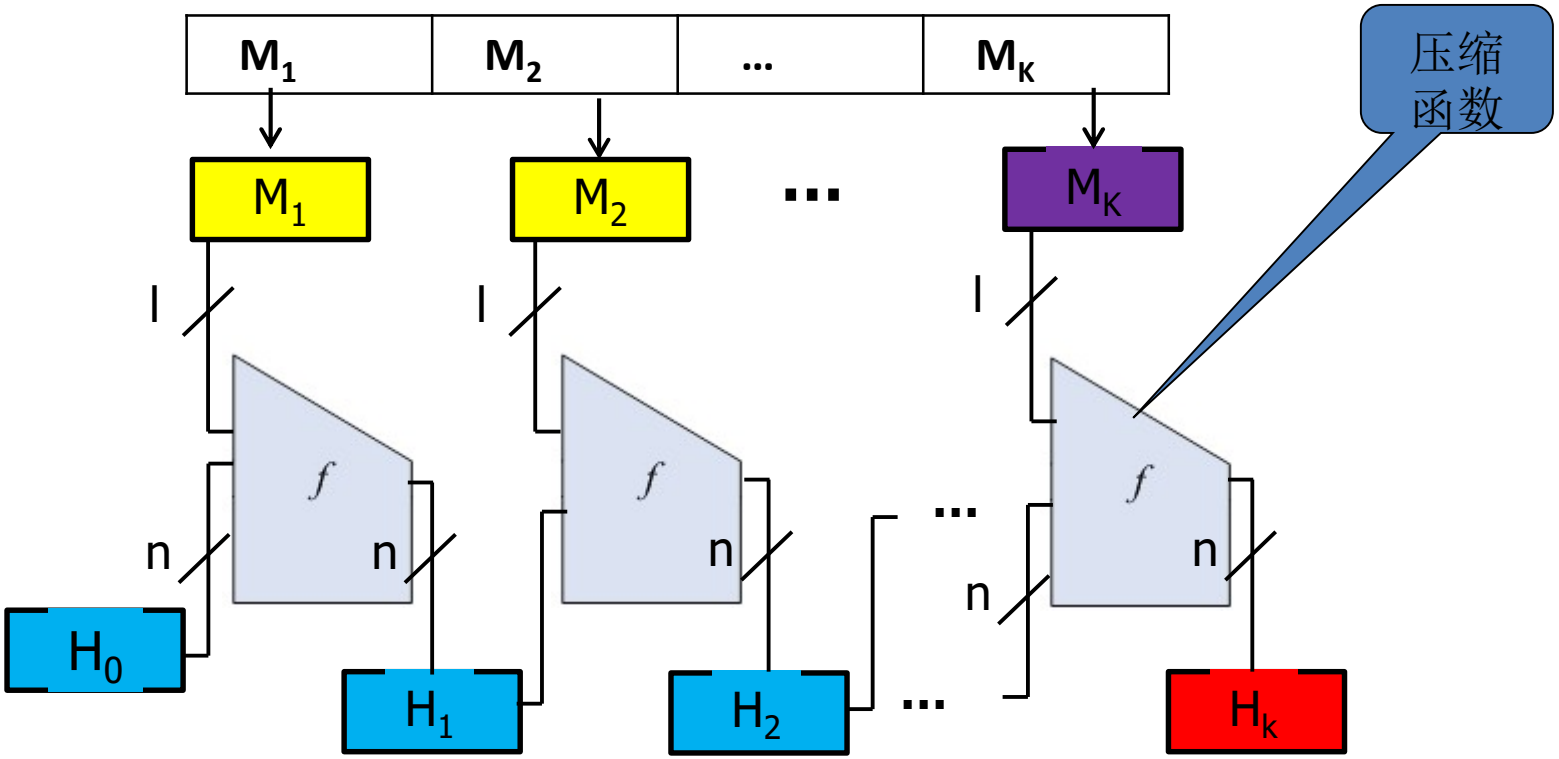
Proposal: switch to 256bit objectIDs (and inherently addresses too).

BUPT ISC 信息安全中心

本讲主要内容

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造
- 消息鉴别码的定义及安全目标
- 消息鉴别码的发展现状
- 消息鉴别码的构造
- 认证加密模式

Hash函数的构造-1



Hash函数的构造-1

- 固定初始值
- 长消息分块迭代处理
- 长度填充（MD-加固）

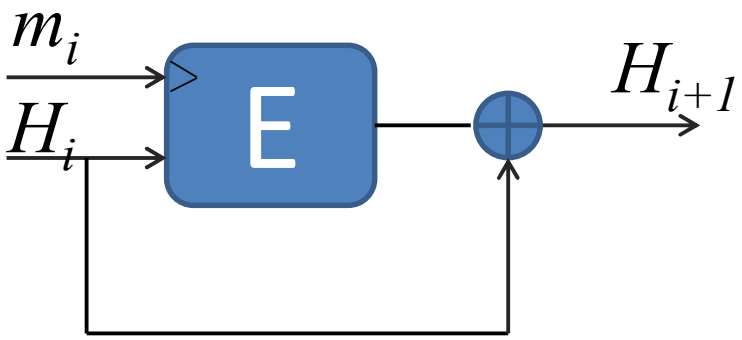
  m||PB, PB=100...00LM，LM为消息长度

Th：如果压缩函数是抗碰撞的，则MD结构构造的hash函数是抗碰撞的

压缩函数既可以由hashing方法构造，也可以由分组密码构造.

Hash函数的构造-1

- Davies-Meyer压缩函数



Th：如果E是一个理想的密码，则DM压缩函数寻找碰撞的复杂度为生日攻击复杂度

Hash函数的构造-1

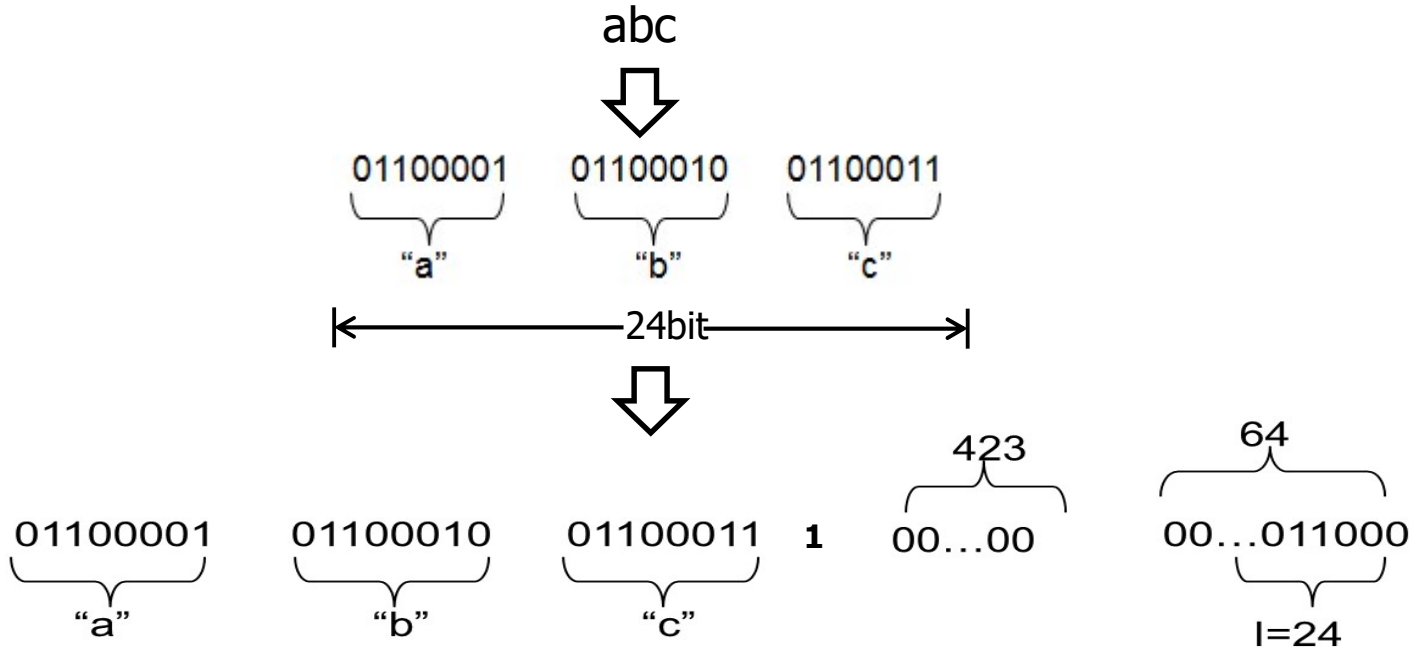
北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

1. SHA-256消息填充

首先将比特“1”添加到消息的末尾，再添加k个零，这里k是方程$l+1+k \equiv 448 \mod 512$的最小的非负解. 然后再添加一个64比特长的块，其值等于消息M的长度l 的二进制表示. 使得填充后的消息的长度为512比特的倍数.

Hash函数的构造-1

SHA-256消息填充



512=24+5+1+n n=423

Hash函数的构造-1

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

2 SHA-256迭代

消息分组和初始值进入MD结构进行迭代压缩

SHA-256的初始变量

$H_0^{(0)}$=6a09e667　　$H_0^{(4)}$=510e527f

$H_0^{(1)}$=bb67ae85　　$H_0^{(5)}$=9b05688c

$H_0^{(2)}$=3c6ef372　　$H_0^{(6)}$=1f83d9ab

$H_0^{(3)}$=a54ff53a　　$H_0^{(7)}$=5be0cd19

这些初值由计算前8个素数的平方根的小数部分的前32位(二进制)生成

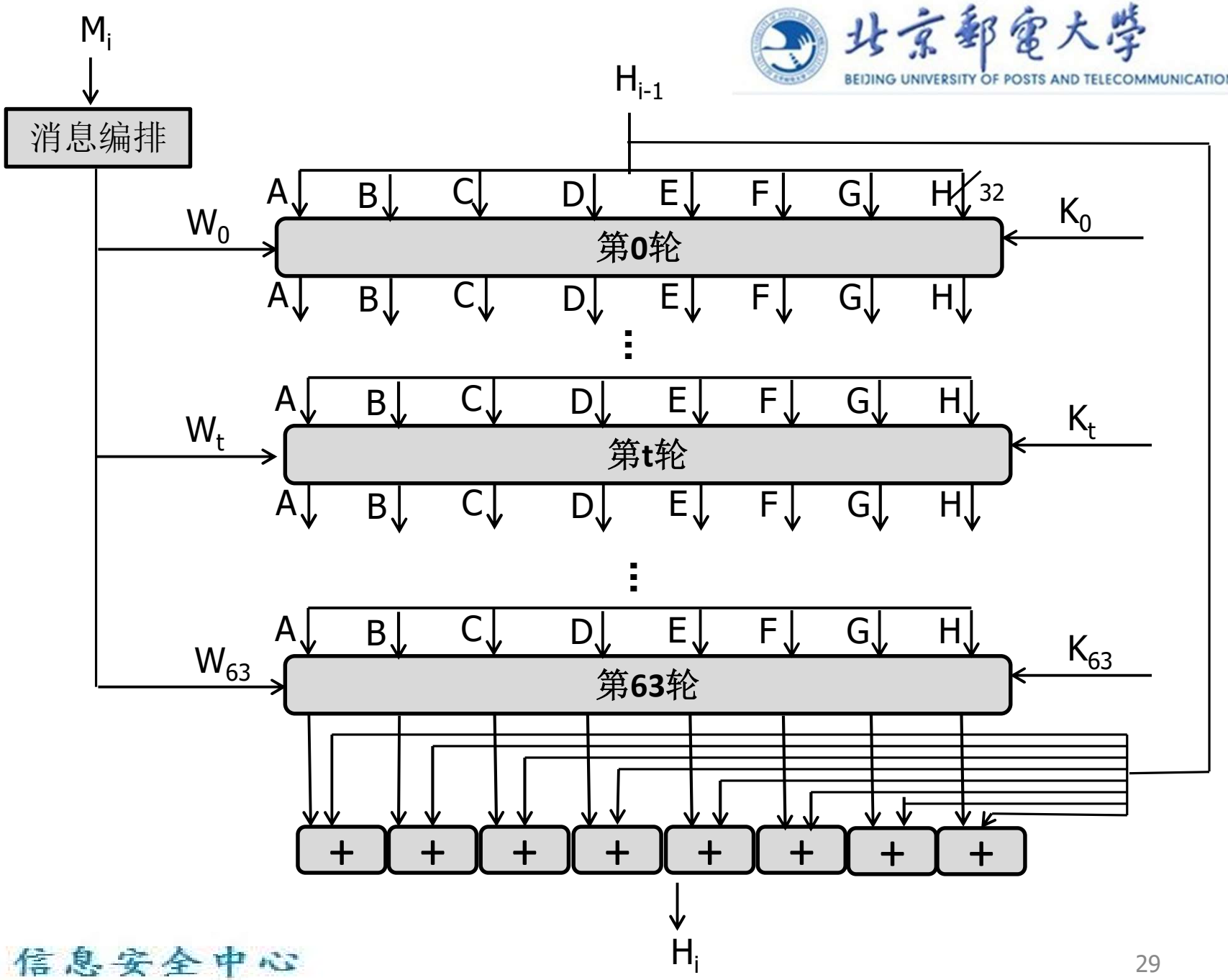
压缩函数的消息分组长度为512比特，压缩函数共64步变换.

Hash函数的构造-1

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

SHA-256 压缩函数

- 输入链接变量a、b、c、d、e、f、g和h:
- for t=0 to 63，执行步函数
- 与输入链接变量的副本模加，计算第i个Hash值$H^{(i)}$:


M_i
消息编排
H_{i-1}
A B C D E F G H
32
W_0
K_0
第0轮
A B C D E F G H
W_t
K_t
第t轮
A B C D E F G H
W_{63}
K_{63}
第63轮
+ + + + + + + +
H_i

Hash函数的构造-1

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

SHA-256 步函数

- 输入寄存器a、b、c、d、e、f、g和h的当前值
- 输入扩展消息字Wi
- 输入常数Ki
- 更新寄存器

$$T_1 = h + \sum_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t$$

$$T_2 = \sum_0^{\{256\}}(a) + Maj(a,b,c)$$

$$h = g$$

$$g = f$$

$$f = e$$

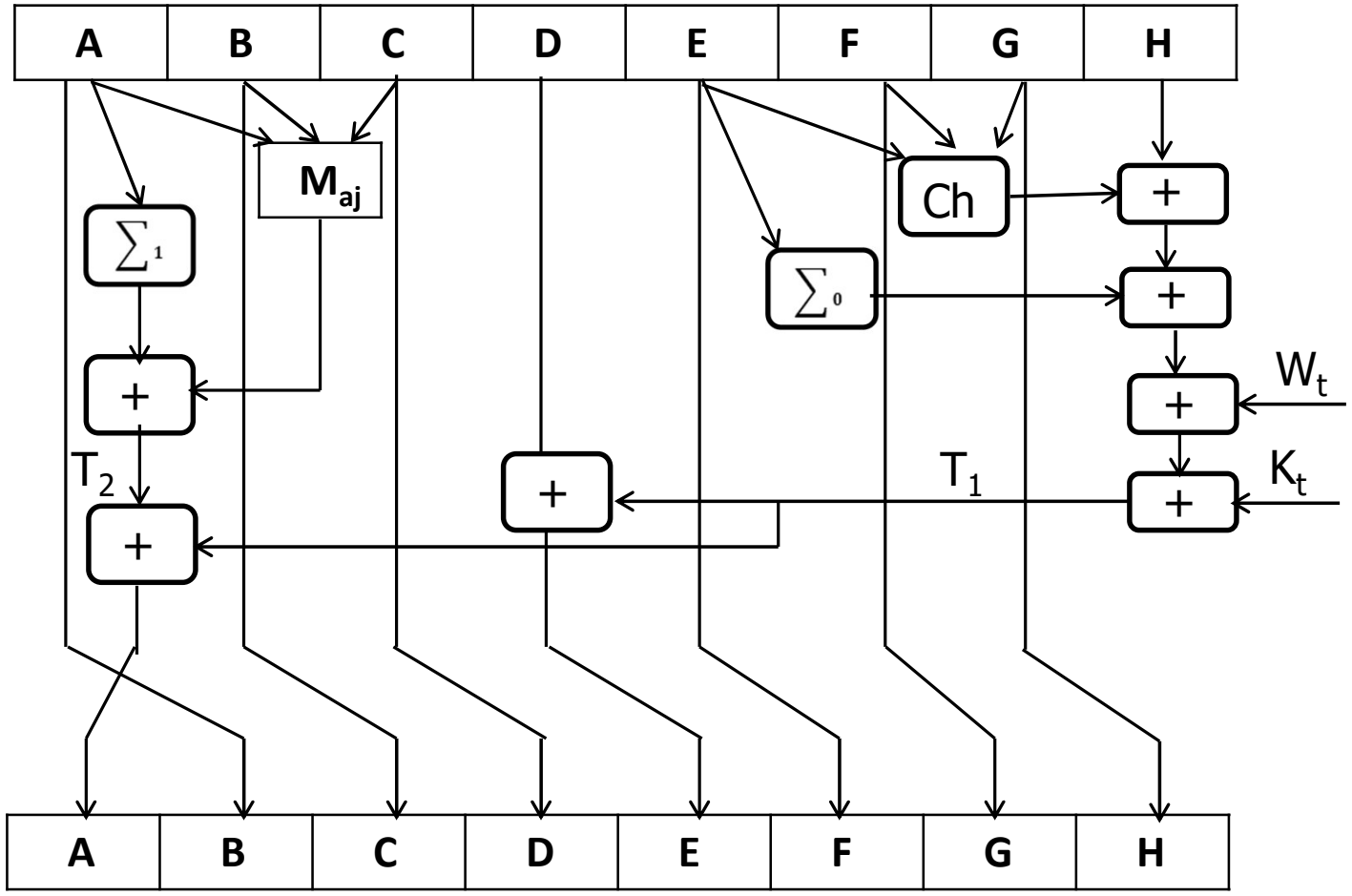
$$e = d + T_1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = T_1 + T_2$$



256bit

Hash函数的构造-1

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

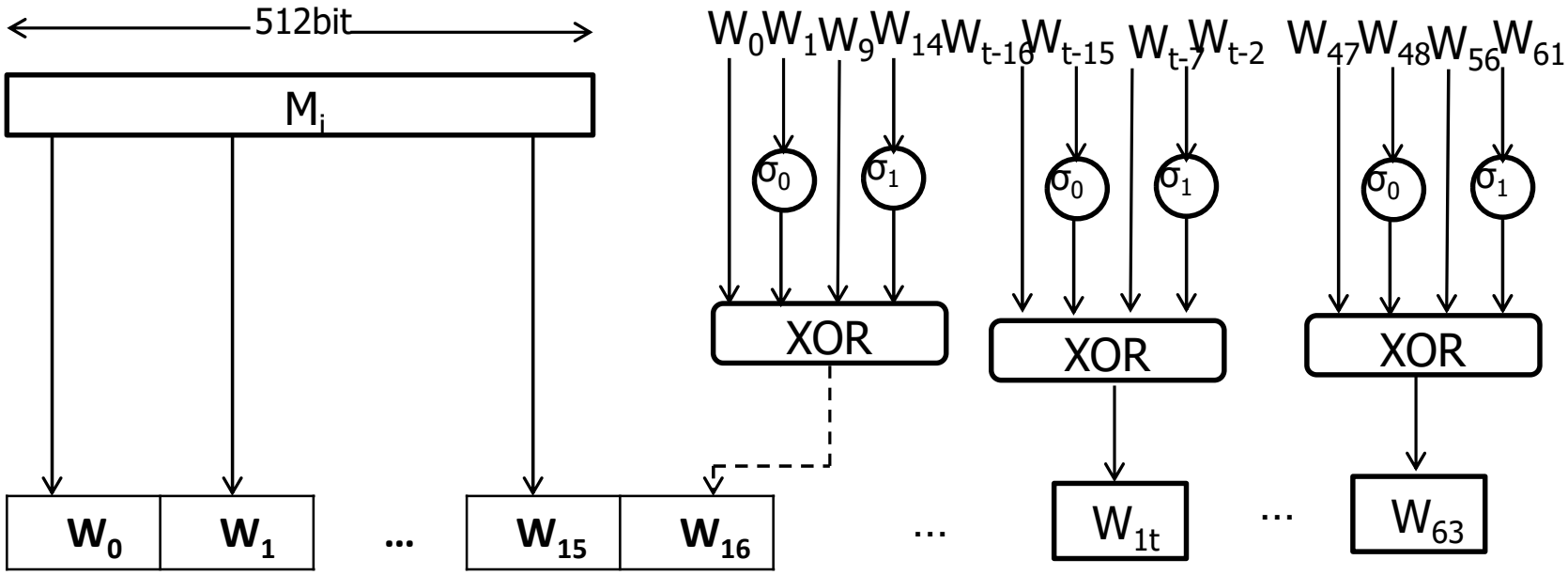
SHA-256的消息编排

当消息填充完成后，将消息块$M^{(1)}$，$M^{(2)}$，...，$M^{(N)}$按序排列，然后执行以下步骤：

- For i=1 to N

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

Hash函数的构造-1


512bit
M_i
W_0 W_1 ... W_{15} W_{16}
$W_0 W_1 W_9 W_{14} W_{t-16} W_{t-15} W_{t-7} W_{t-2}$
$W_{47} W_{48} W_{56} W_{61}$
σ_0 σ_1
XOR
W_{1t}
W_{63}

Hash函数的构造-1

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

SHA-256使用了6个逻辑函数，设x,y和z为3个32比特长的自变量，输出结果都是32比特长的字，逻辑函数定义如下：

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

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

$$\sum_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$

$$\sum_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$$

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

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

Hash函数的构造-1

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

SHA-256的常数

共使用了64个32位字长的常数，它们分别由最小的64个素数的三次方根的小数部分的前32位产生（二进制表示）

428a2f98 71374491 b5c0fbcf e9b5dba5
3956c25b 59f111f1 923f82a4 ab1c5ed5
d807aa98 12835b01 243185be 550c7dc3
72be5d74 80deb1fe 9bdc06a7 c19bf174
e49b69c1 efbe4786 0fc19dc6 240ca1cc
2de92c6f 4a7484aa 5cb0a9dc 76f988da
983e5152 a831c66d b00327c8 bf597fc7
c6e00bf3 d5a79147 06ca6351 14292967
27b70a85 2e1b2138 4d2c6dfc 53380d13
650a7354 766a0abb 81c2c92e 92722c85
a2bfe8a1 a81a664b c24b8b70 c76c51a3
d192e819 d6990624 f40e3585 106aa070
19a4c116 1e376c08 2748774c 34b0bcb5
391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
748f82ee 78a5636f 84c87814 8cc70208
90befffa a4506ceb bef9a3f7 c67178f2

Hash函数的构造-1

3 最后一轮迭代输出的链接变量值，即为散列值，长度为256比特.

SHA-224算法可用来Hash任意l(0≤l≤2^{64})位长的消息M。算法的具体实现和SHA-256基本一样，不同的是以下两点：

1） 初始Hash值H(0)的设置不同；

2） 输出224比特长的消息摘要，即剪切H(N)的左边224比特位产生

Hash函数的构造-1

Published in	Year	Attack method	Attack	Variant	Rounds	Complexity
New Collision Attacks Against Up To 24-step SHA-2[31]	2008	Deterministic	Collision	SHA-256	24/64	$2^{28.5}$
				SHA-512	24/80	$2^{32.5}$
Preimages for step-reduced SHA-2[32]	2009	Meet-in-the-middle	Preimage	SHA-256	42/64	$2^{251.7}$
					43/64	$2^{254.9}$
				SHA-512	42/80	$2^{502.3}$
					46/80	$2^{511.5}$
Advanced meet-in-the-middle preimage attacks[33]	2010	Meet-in-the-middle	Preimage	SHA-256	42/64	$2^{248.4}$
				SHA-512	42/80	$2^{494.6}$
Higher-Order Differential Attack on Reduced SHA-256[2]	2011	Differential	Pseudo-collision	SHA-256	46/64	2^{178}
					33/64	2^{46}
Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family[1]	2011	Biclique	Preimage	SHA-256	45/64	$2^{255.5}$
				SHA-512	50/80	$2^{511.5}$
			Pseudo-preimage	SHA-256	52/64	2^{255}
				SHA-512	57/80	2^{511}
Improving Local Collisions: New Attacks on Reduced SHA-256[34]	2013	Differential	Collision	SHA-256	31/64	$2^{65.5}$
			Pseudo-collision	SHA-256	38/64	2^{37}
Branching Heuristics in Differential Collision Search with Applications to SHA-512[35]	2014	Heuristic differential	Pseudo-collision	SHA-512	38/80	$2^{40.5}$
Analysis of SHA-512/224 and SHA-512/256[36]	2016	Differential	Collision	SHA-256	28/64	practical
				SHA-512	27/80	practical
			Pseudo-collision	SHA-512	39/80	practical

[1] *Dmitry Khovratovich, Christian Rechberger & Alexandra Savelieva (2011). "Bicliques for Preimages: Attacks on Skein-512 and the SHA-2 family" . IACR Cryptology ePrint Archive. 2011:286.*

[2] *Mario Lamberger & Florian Mendel (2011). "Higher-Order Differential Attack on Reduced SHA-256" . IACR Cryptology ePrint Archive. 2011:37.*

[31] *Somitra Kumar Sanadhya & Palash Sarkar (2008). "New Collision Attacks Against Up To 24-step SHA-2" . IACR Cryptology ePrint Archive. 2008:270.*

[32] *Kazumaro Aoki; Jian Guo; Krystian Matusiewicz; Yu Sasaki & Lei Wang (2009). Preimages for step-reduced SHA-2. Advances in Cryptology – ASIACRYPT 2009. Lecture Notes in Computer Science.* ***5912****. Springer Berlin Heidelberg. pp. 578–597.*

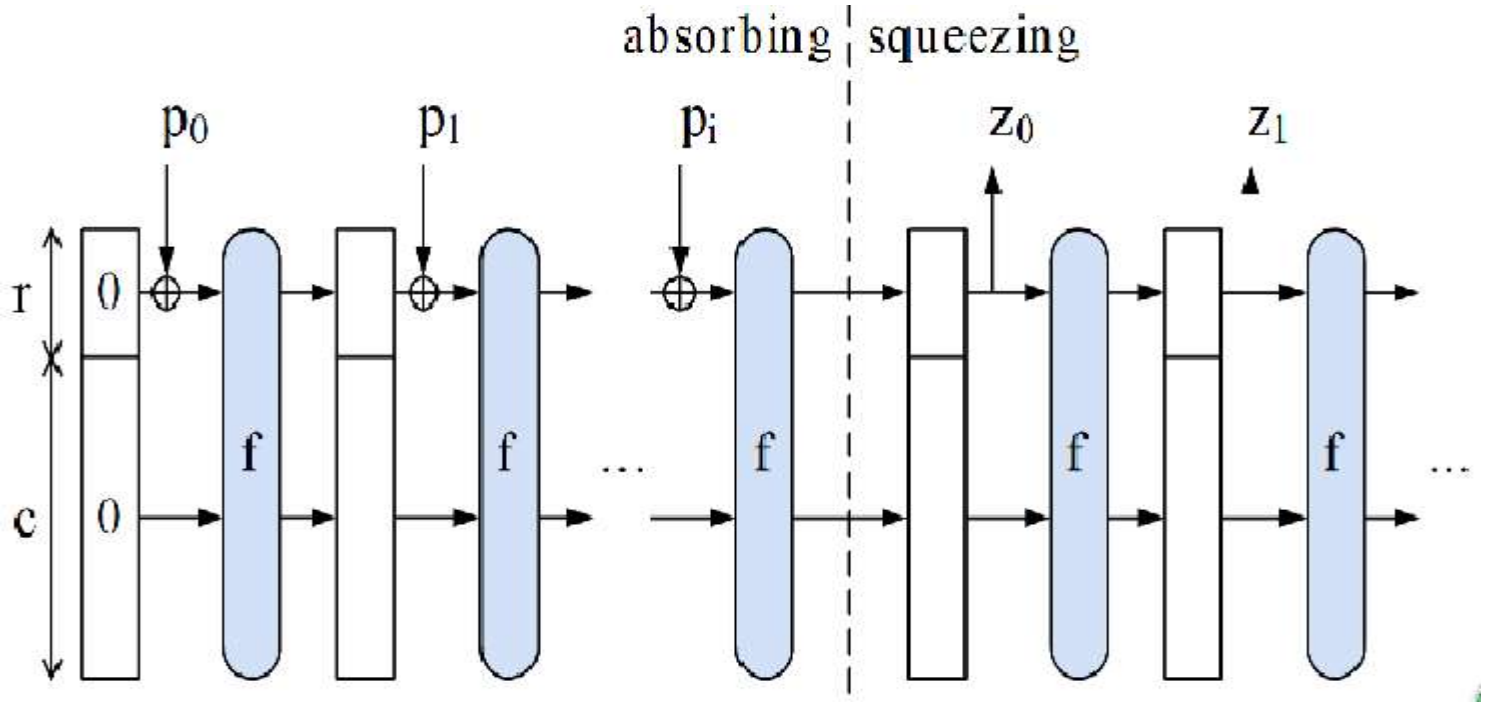
[33]*Jian Guo; San Ling; Christian Rechberger & Huaxiong Wang (2010). Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. Advances in Cryptology – ASIACRYPT 2010. Lecture Notes in Computer Science.* ***6477****. Springer Berlin Heidelberg. pp. 56–75.*

[34] *Florian Mendel; Tomislav Nad; Martin Schläffer (2013). Improving Local Collisions: New Attacks on Reduced SHA-256. Advances in Cryptology – EUROCRYPT 2013. Lecture Notes in Computer Science.* ***7881****. Springer Berlin Heidelberg. pp. 262–278.*

[35]*Maria Eichlseder and Florian Mendel and Martin Schläffer (2014). "Branching Heuristics in Differential Collision Search with Applications to SHA-512" . IACR Cryptology ePrint Archive. 2014:302.*

[36]*Christoph Dobraunig; Maria Eichlseder & Florian Mendel (2016). "Analysis of SHA-512/224 and SHA-512/256".*

Hash函数的构造-2



海绵结构

Hash函数的构造-2

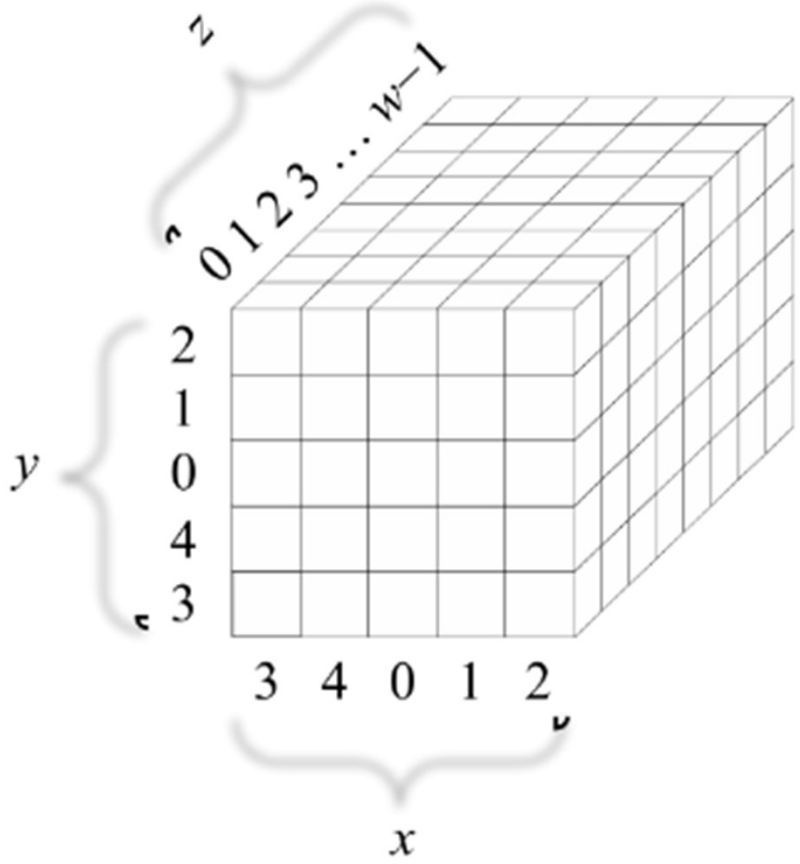
- Keccak[r,c](M, d) 定义如下
- 使用填充函数填充M，填充后的比特流记为P，其长度为r的整数倍（即$n = \text{len}(P)/r$ 为整数），将 P 分割为n 个长为 r比特的消息块$P_0, \ldots, P_{n-1}$
- 状态S初始化为全 0 .
- 吸收过程：对每个块P_i,
  - 在P_i 后填充c个0 ,扩展为长度为b的比特流,
  - 与此时状态S进行异或
  - 执行f置换操作生成新状态S
- 输出过程：将 Z 初始化为空串,
  - 若Z 的长度小于d:
    - ✓将状态S的前r 比特缀在Z的末尾
    - ✓若 Z 的长度仍然小于 d 比特，对S执行 f置换生成新的状态 S.
  - 将 Z 截断到 d 比特

Hash函数的构造-2

SHA-3 使用10*1 的填充模式: 一个 1比特, 足够多个 0 bits (最大 $r-1$个) 和最后一个 1 bit.

- 比特率 r,
- 容量c.
- $b = r+c = 1600$ bits
- $n = 224$: Keccak[$r = 1152$, $c = 448$]$_{224}$
- $n = 256$: Keccak[$r = 1088$, $c = 512$]$_{256}$
- $n = 384$: Keccak[$r = 832$, $c = 768$]$_{384}$
- $n = 512$: Keccak[$r = 576$, $c = 1024$]$_{512}$
- Keccak轮函数f迭代轮数$n_r = 12 + 2 \times l$, l=6

Hash函数的构造-2



状态5 × 5 array of 64-bit words

Hash函数的构造-2

- Convert string to State Array

For all triples (x, y, z) such that $0 \le x < 4$, $0 \le y < 4$, and $0 \le z < w$,

$$\mathbf{A}[x, y, z] = S[w(5y + x) + z].$$

For example, if $b = 1600$, so that $w = 64$, then

$$\begin{array}{llll}
\mathbf{A}[0,0,0]=S[0] & \mathbf{A}[1,0,0]=S[64] & \mathbf{A}[2,0,0]=S[128] & \mathbf{A}[3,0,0]=S[192] \\
\mathbf{A}[0,0,1]=S[1] & \mathbf{A}[1,0,1]=S[65] & \mathbf{A}[2,0,1]=S[129] & \mathbf{A}[3,0,1]=S[193] \\
\mathbf{A}[0,0,2]=S[2] & \mathbf{A}[1,0,2]=S[66] & \mathbf{A}[2,0,2]=S[130] & \mathbf{A}[3,0,2]=S[194] \\
\vdots & \vdots & \vdots & \vdots \\
\mathbf{A}[0,0,62]=S[62] & \mathbf{A}[1,0,62]=S[126] & \mathbf{A}[2,0,62]=S[190] & \mathbf{A}[3,0,62]=S[254] \\
\mathbf{A}[0,0,63]=S[63] & \mathbf{A}[1,0,63]=S[127] & \mathbf{A}[2,0,63]=S[191] & \mathbf{A}[3,0,63]=S[255]
\end{array}$$

and

$$\begin{array}{llll}
\mathbf{A}[4,0,0]=S[256] & \mathbf{A}[0,1,0]=S[320] & \mathbf{A}[1,1,0]=S[384] & \mathbf{A}[2,1,0]=S[448] \\
\mathbf{A}[4,0,1]=S[257] & \mathbf{A}[0,1,1]=S[321] & \mathbf{A}[1,1,1]=S[385] & \mathbf{A}[2,1,1]=S[449] \\
\mathbf{A}[4,0,2]=S[258] & \mathbf{A}[0,1,2]=S[322] & \mathbf{A}[1,1,2]=S[386] & \mathbf{A}[2,1,2]=S[450] \\
\vdots & \vdots & \vdots & \vdots \\
\mathbf{A}[4,0,62]=S[318] & \mathbf{A}[0,1,62]=S[382] & \mathbf{A}[1,1,62]=S[446] & \mathbf{A}[2,1,62]=S[510] \\
\mathbf{A}[4,0,63]=S[319] & \mathbf{A}[0,1,63]=S[383] & \mathbf{A}[1,1,63]=S[447] & \mathbf{A}[2,1,63]=S[511]
\end{array}$$

etc.

Hash函数的构造-2

- Convert state array to string

For each pair of integers (i,j) such that $0 \le i < 4$ and $0 \le j < 4$, define the string $Lane(i,j)$ by

$$Lane(i,j) = \mathbf{A}[i,j,0] \,\|\, \mathbf{A}[i,j,1] \,\|\, \mathbf{A}[i,j,2] \,\|\, \ldots \,\|\, \mathbf{A}[i,j,w\text{-}2] \,\|\, \mathbf{A}[i,j,w\text{-}1].$$

For each integer j such that $0 \le j < 4$, define the string $Plane(j)$ by

$$Plane(j) = Lane(0,j) \,\|\, Lane(1,j) \,\|\, Lane(2,j) \,\|\, Lane(3,j) \,\|\, Lane(4,j).$$

Then

$$S = Plane(0) \,\|\, Plane(1) \,\|\, Plane(2) \,\|\, Plane(3) \,\|\, Plane(4).$$

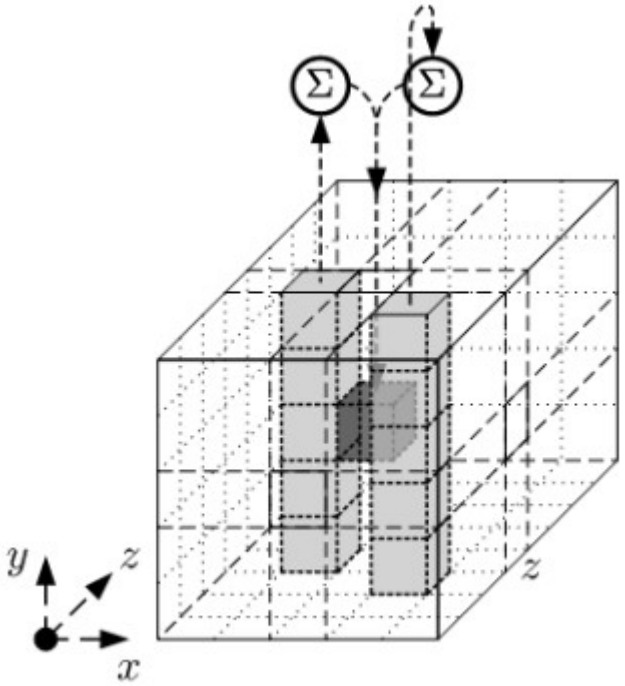
Hash函数的构造-2

- Convert state array to string

For example, if $b = 1600$, so that $w = 64$, then

$$
\begin{aligned}
S = \quad & \mathbf{A}[0,0,0] \,\|\, \mathbf{A}[0,0,1] \,\|\, \mathbf{A}[0,0,2] \,\|\, \ldots \,\|\, \mathbf{A}[0,0,62] \,\|\, \mathbf{A}[0,0,63] \\
& \|\, \mathbf{A}[1,0,0] \,\|\, \mathbf{A}[1,0,1] \,\|\, \mathbf{A}[1,0,2] \,\|\, \ldots \,\|\, \mathbf{A}[1,0,62] \,\|\, \mathbf{A}[1,0,63] \\
& \|\, \mathbf{A}[2,0,0] \,\|\, \mathbf{A}[2,0,1] \,\|\, \mathbf{A}[2,0,2] \,\|\, \ldots \,\|\, \mathbf{A}[2,0,62] \,\|\, \mathbf{A}[2,0,63] \\
& \|\, \mathbf{A}[3,0,0] \,\|\, \mathbf{A}[3,0,1] \,\|\, \mathbf{A}[3,0,2] \,\|\, \ldots \,\|\, \mathbf{A}[3,0,62] \,\|\, \mathbf{A}[3,0,63] \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
& \|\, \mathbf{A}[3,4,0] \,\|\, \mathbf{A}[3,4,1] \,\|\, \mathbf{A}[3,4,2] \,\|\, \ldots \,\|\, \mathbf{A}[3,4,62] \,\|\, \mathbf{A}[3,4,63] \\
& \|\, \mathbf{A}[4,4,0] \,\|\, \mathbf{A}[4,4,1] \,\|\, \mathbf{A}[4,4,2] \,\|\, \ldots \,\|\, \mathbf{A}[4,4,62] \,\|\, \mathbf{A}[4,4,63]
\end{aligned}
$$

Hash函数的构造-2



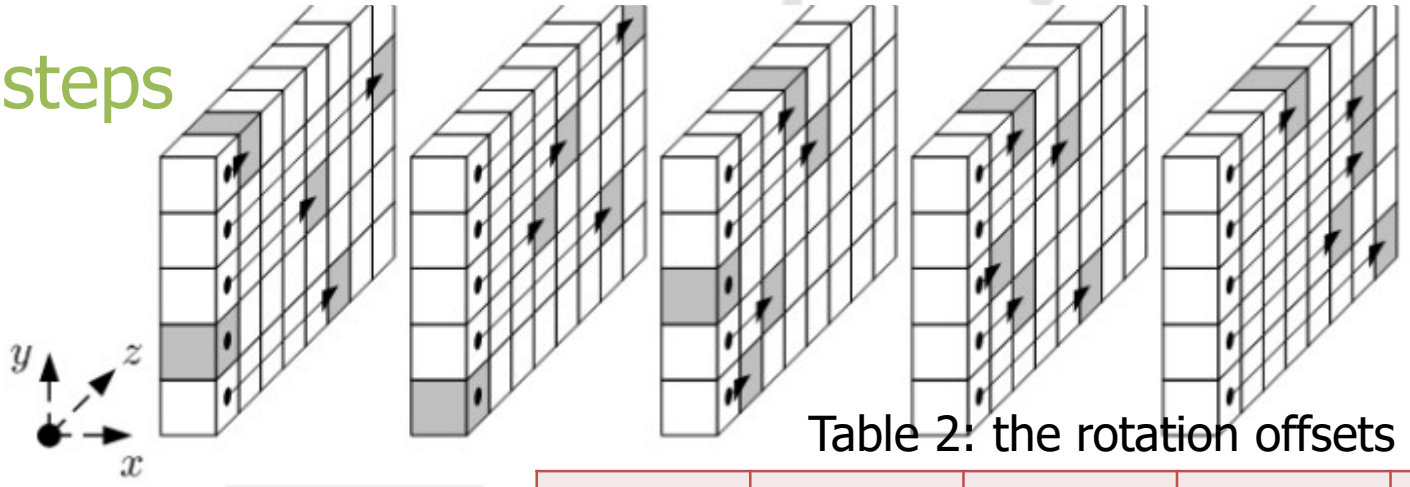
θ step

$$\theta: a'[x][y][z] \leftarrow a[x][y][z] \oplus \sum_{y'=0}^{4} a[x-1][y'][z] \oplus \sum_{y'=0}^{4} a[x+1][y'][z-1];$$

Hash函数的构造-2

Let $(x, y) = (1, 0)$.
For t from 0 to 23:
a. for all z such that $0 \le z < w$, let $\mathbf{A}'[x, y, z] = \mathbf{A}[x, y, (z-(t+1)(t+2)/2) \bmod w]$;
b. let $(x, y) = (y, (2x+3y) \bmod 5)$.
Return $\mathbf{A}'$.

ρ steps

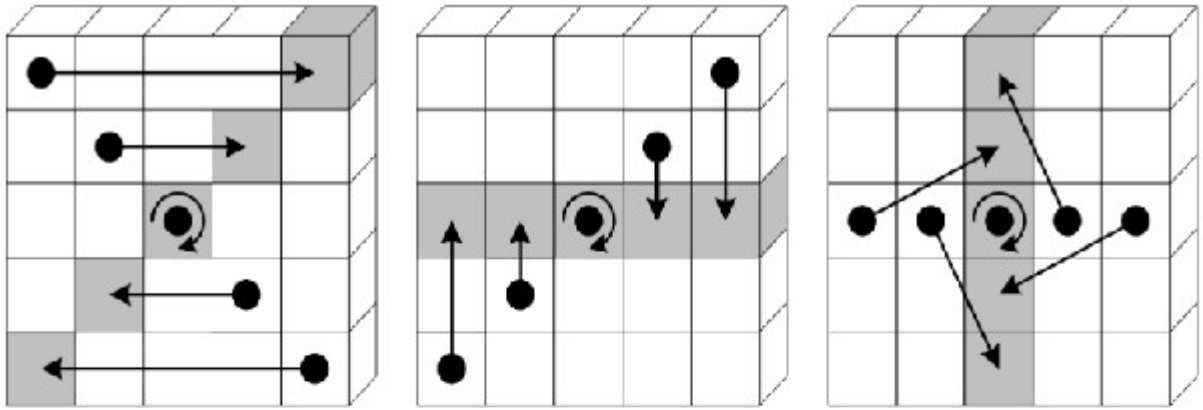


$\mathbf{A}'[0, 0, z] = \mathbf{A}[0, 0, z]$.

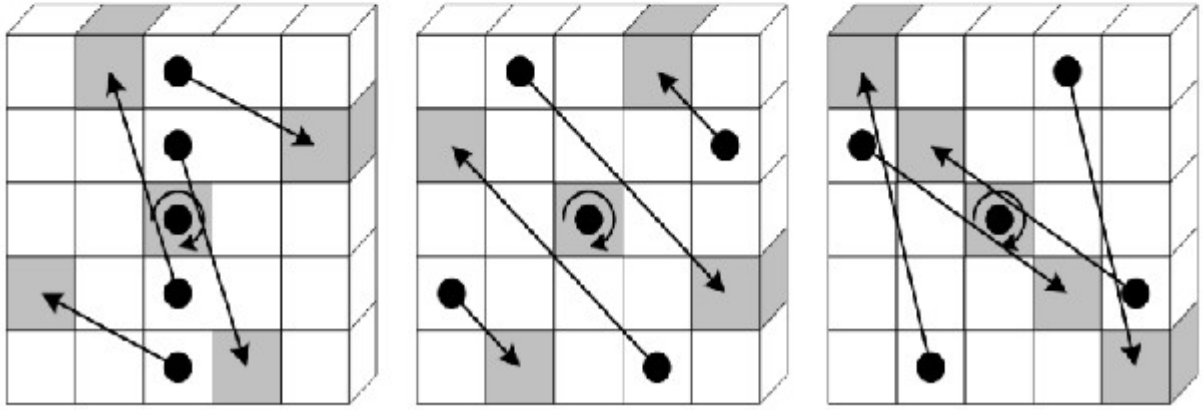
Table 2: the rotation offsets

	x = 3	x = 4	x = 0	x = 1	x = 2
y = 2	25	39	3	10	43
y = 1	55	20	36	44	6
y = 0	28	27	0	1	62
y = 4	56	14	18	2	61
y = 3	21	8	41	45	15

Hash函数的构造-2



π steps

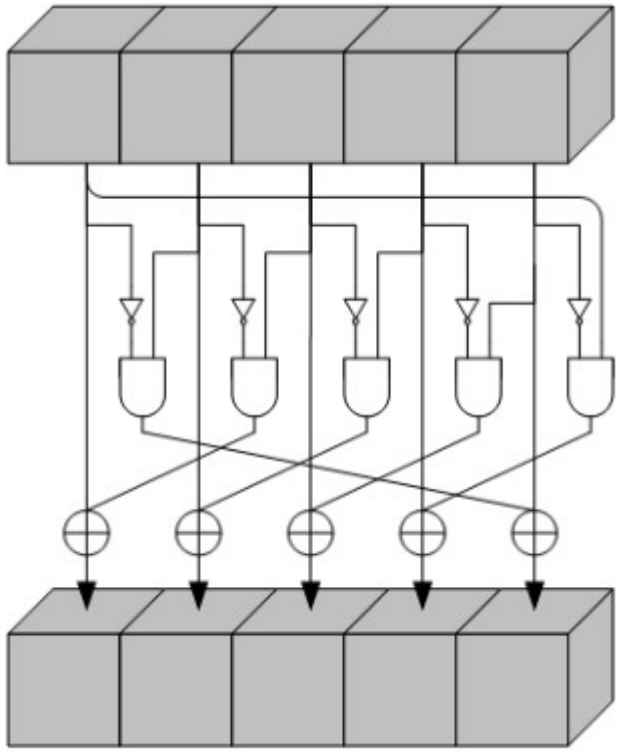


1. For all triples (x, y, z) such that $0 \le x < 4$, $0 \le y < 4$, and $0 \le z < w$, let
   $\mathbf{A}'[x, y, z] = \mathbf{A}[(x + 3y) \bmod 5, x, z]$.
2. Return $\mathbf{A}'$.

Hash函数的构造-2

$$\chi : a'[x][\bullet][\bullet] \leftarrow a[x][\bullet][\bullet] \oplus ((a[x+1][\bullet][\bullet] \oplus 1) \wedge a[x+2][\bullet][\bullet]);$$

χ step



The effect of χ is to XOR each bit with a non-linear function of two other bits in its row,

Hash函数的构造-2

北京郵電大學 BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

$$\iota : a'[0][0][\bullet] \leftarrow a[0][0][\bullet] \oplus RC[n_r]$$

- step

RC[0]	0x0000000000000001	RC[12]	0x000000008000808B
RC[1]	0x0000000000008082	RC[13]	0x800000000000008B
RC[2]	0x800000000000808A	RC[14]	0x8000000000008089
RC[3]	0x8000000080008000	RC[15]	0x8000000000008003
RC[4]	0x000000000000808B	RC[16]	0x8000000000008002
RC[5]	0x0000000080000001	RC[17]	0x8000000000000080
RC[6]	0x8000000080008081	RC[18]	0x000000000000800A
RC[7]	0x8000000000008009	RC[19]	0x800000008000000A
RC[8]	0x000000000000008A	RC[20]	0x8000000080008081
RC[9]	0x0000000000000088	RC[21]	0x8000000000008080
RC[10]	0x0000000080008009	RC[22]	0x0000000080000001
RC[11]	0x000000008000000A	RC[23]	0x8000000080008008

BUPT ISC 信息安全中心

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security bits (Info)	Example performance(MiB/s)	First Published
SHA-2	*SHA-224* *SHA-256*	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	139	2001
	SHA-384 *SHA-512* *SHA-512/224* *SHA-512/256*	384 512 224 256	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256 112 128	154	2001
SHA-3	*SHA3-224* *SHA3-256* *SHA3-384* *SHA3-512*	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	Unlimited	24	And, Xor, Rot, Not	112 128 192 256	-	2015

Comparison of SHA functions（2015）

本节要点小结

- Hash函数的定义及安全目标
- Hash函数的发展现状
- Hash函数的构造

THE END !