SHA-3 轮函数中 ρ、π 及 χ 变换的逆变换

王 淦[1,2],张文英[1,2]
(1. 山东师范大学 信息科学与工程学院,山东 济南 250014;
2. 山东省分布式计算机软件新技术重点实验室,山东 济南 250014)

摘 要:Keccak 自 2012 年被宣布为新一代 Hash 函数标准 SHA-3 后受到密码学界的高度关注,成为当前 Hash 函数研究的热点。文中给出了 SHA-3 轮函数中 ρ 、π 和 χ 三个变换的逆变换。ρ 变换只在同一道内沿 z 轴正向循环移位,故依据其移位距离表沿 z 轴负方向移位同样距离即得到其逆变换 ρ^{-1};π 变换依赖于 GF(5) 上一个 2 阶变换矩阵,利用高斯消元法对此方阵求逆可得到其逆矩阵,也即得到了 π 变换的逆变换;χ 变换是 SHA-3 轮函数中唯一的非线性变换,首先列出 χ 变换的真值表,然后通过真值表推导得出了其逆变换 χ^{-1} 的布尔函数表达式。基于 ρ^{-1}、π^{-1} 和 χ^{-1},可利用中间相遇攻击的思想构造差分路径对 SHA-3 进行攻击,通过消息修改技术使差分路径以概率 1 通过 χ^{-1},能够大大提高攻击成功的概率。

关键词:Hash 函数;SHA-3;轮函数;逆变换
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2014)12-0151-04
doi:10.3969/j.issn.1673-629X.2014.12.035

Inverse Mappings of ρ、π and χ Mappings in SHA-3 Permutation

WANG Gan[1,2], ZHANG Wen-ying[1,2]
(1. School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China;
2. Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250014, China)

Abstract: Keccak has become a hotspot after it has been selected as the new Hash standard SHA-3 in 2012. In this paper, give the inverse mappings of ρ, π and χ mappings in SHA-3 permutation. ρ mapping intends to provide intra lane diffusion along z axis. By shifting toward the reverse direction in terms of the same rotation constants table of ρ, can get its inverse mapping ρ^{-1}. The inverse mapping of π is obtained by using Gauss elimination method on the transformational matrix of π in GF(5). χ mapping is the only non-linear mapping of SHA-3 permutation, give its inverse mapping in the form of Boolean function expression through the truth table of χ. By means of the inverse mappings of ρ, π and χ, a differential attack on SHA-3 can be implemented using the meet-in-the-middle thought. In addition, by using the message modification technique, the differential path can be through χ^{-1} with probability 1, thus greatly improving the success probability of the attack.

Key words: Hash function; SHA-3; permutation; inverse mappings

0 引 言

自 2004 年以来,一系列 Hash 函数如 MD4、MD5、RIPEMD、HAVAL 和 SHA-1 等受到了我国学者王小云提出的模差分和消息修改方法的攻击,暴露出了这些 Hash 函数存在的许多严重问题,它们的安全性受到质疑[1-4]。因此,美国国家标准与技术研究所(National Institute of Standards and Technology, NIST)发起了征集新一代 Hash 函数标准 SHA-3 的计划[5]。该计划于 2007 年启动,经过长达五年的竞赛,NIST 于 2012 年 10 月 2 日宣布由 Guido Bertoni、Joan Daemen、Michael Peeters 和 Gilles Van Assche 设计的 Keccak[6] 为 SHA-3 标准[7]。Keccak 具有许多良好的性质,其在不同平台上的兼容性非常好,而且不论软件硬件实现代价都比较低[8-11]。加之其不同于以往 Hash 函数的设

收稿日期:2014-03-20 **修回日期**:2014-06-25 **网络出版时间**:2014-10-27
基金项目:国家自然科学基金资助项目(61272434);山东省自然科学基金资助项目(ZR2012FM004);信息安全国家重点实验室开放课题基金资助项目(4050101)
作者简介:王 淦(1988-),男,山东淄川人,硕士生,CCF 会员,研究方向为密码学与信息安全;张文英,博士后,教授,博士生导师,研究方向为密码学。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20141027.1429.003.html

计理念，Keccak 成为了当前 Hash 函数研究的热点[12-13]。

SHA-3 轮函数中的 ρ 变换根据 25 道中每一道 x 和 y 的坐标确定其沿 z 轴正方向的移位距离，由于 ρ 变换只在同一道内循环移位，故依据其移位表将其沿 z 轴负方向移位同样距离即得到其逆变换 ρ^{-1}，ρ 变换的移位表即其逆变换 ρ^{-1} 的移位表。π 变换依赖于一个二阶变换矩阵，对 π 变换求逆归结为在 GF(5) 上对二阶方阵求逆的问题，利用高斯消元法可进行求解。χ 变换是 SHA-3 轮函数中唯一的非线性变换，它保证了整个轮函数的非线性。列出了 χ 变换的真值表，进而利用布尔函数通过真值表推导得到了其逆变换 χ^{-1} 的布尔函数表达式。

基于 ρ、π 和 χ 的逆变换可利用差分分析的方法[14]构造差分路径对 SHA-3 进行中间相遇攻击[15]。利用 χ^{-1} 的布尔函数表达式和消息修改技术对消息设定条件从而保证差分路径以概率 1 通过 χ^{-1}，较之利用 χ 的差分分布表重复搜索尝试的方法可大大提高攻击的成功率。

1 Keccak 算法简介

Keccak 算法基于海绵结构[16]，其结构如图 1 所示。Keccak 轮函数表示为 Keccak-f[b]，b 称为轮函数的宽度，也称为状态的个数，$b=25\times2^l$，$l\in\{0,1,2,3,4,5,6\}$。b 可表示为 $b=r+c$，其中 r 称为比特率，c 称为容量。消息经过填充后分割为 r 比特的块进行处理，输出长度为 n 的摘要，并满足 $c=2n$。根据 SHA-3 标准，$n\in\{224,256,384,512\}$，即 SHA-3 同时支持四种不同长度的摘要，分别表示为 Keccak-224，Keccak-256，Keccak-384 和 Keccak-512。

Keccak 算法共有 $12+2l$ 轮，每轮包含 5 个变换，轮函数表示为 $R=\iota\circ\chi\circ\pi\circ\rho\circ\theta$，其运算均在 GF(2) 上进行。SHA-3 使用的是 Keccak-f[1 600]，共 24 轮，其 1 600 比特状态的每一比特可看作三维数组 $a[x][y][z]$ 中的一个元素，其中 $0\leqslant x\leqslant4$，$0\leqslant y\leqslant4$，$0\leqslant z\leqslant63$。

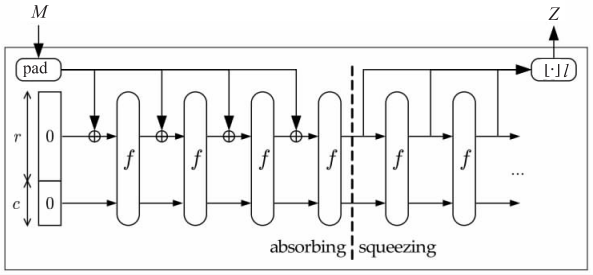

图 1 Keccak 海绵结构

Keccak 轮函数的 5 个变换如下：

$$\theta:a[x][y][z]\leftarrow a[x][y][z]+\sum_{y=0}^{4}a[x-1][y][z]+\sum_{y=0}^{4}a[x+1][y][z-1]$$，θ 将每一比特的值更新为其本身和其左边和右后方两列共 11 比特的异或值。

$$\rho:a[x][y][z]\leftarrow a[x][y][z-\frac{(t+1)(t+2)}{2}]$$，ρ 使某一道沿 z 轴正方向循环移位，移位的距离根据不同的坐标 (x,y) 而不同。

$$\pi:a[x][y][z]\leftarrow a[x'][y'][z'],\ \begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}0&1\\2&3\end{pmatrix}\begin{pmatrix}x'\\y'\end{pmatrix}$$，π 对 xy 平面上坐标位置为 (x',y') 的一道的位置进行变换，新位置由 (x,y) 指定。

$$\chi:a[x][y][z]\leftarrow a[x][y][z]+(\neg a[x+1][y][z]\wedge a[x+2][y][z])$$，χ 对沿 x 轴方向一行中的 5 个比特进行非线性运算。

$$\iota:a[0][0][z]\leftarrow a[0][0][z]+\mathrm{RC}[i]$$，ι 添加一个每轮均不相同的 64 比特的常量。

有关 Keccak 算法的详细描述可参考文献[6]。

2 ρ 的逆变换

2.1 ρ 变换的移位表

ρ 沿 z 轴正方向对一道内的 64 个比特进行模 64 循环移位操作，移位的距离由 $\frac{(t+1)(t+2)}{2}$ 指定。计算公式为 $\begin{pmatrix}0&1\\2&3\end{pmatrix}^t\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}x\\y\end{pmatrix}$，其中 $0\leqslant t<24$ 且运算均在 $\mathrm{GF}(5)^{2\times2}$ 上进行，当 $(x,y)=(0,0)$ 时不移位。对 t 的 24 种取值情况逐一计算对应的 (x,y) 即可得到 ρ 变换的移位表，如表 1 所示。

表 1 ρ 的移位表

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

2.2 ρ 变换的逆变换 ρ^{-1}

依照表 1，根据每一道的 x 和 y 坐标，沿 z 轴负方向移位相应距离即可得到 ρ 变换的逆变换 ρ^{-1}：$a[x][y][z]\leftarrow a[x][y][z+\frac{(t+1)(t+2)}{2}]$。

3 π 的逆变换

3.1 有限域相关知识

定义：给定域 F 和一个素数 p，阶为 p 的有限域 GF

(p)定义为整数$\{0,1,\cdots,p-1\}$的集合[17]。

由上述定义,5 元域即 GF(5)为集合$\{0,1,2,3,4\}$。根据有限域中的运算规则,将 GF(5)上的加法表、乘法表以及各元素的逆元表列表,如表 2 ~ 表 4 所示。

表 2　GF(5)的加法表

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

表 3　GF(5)的乘法表

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

表 4　GF(5)的逆元表

元素	加法逆元	乘法逆元
0	0	不存在
1	4	1
2	3	3
3	2	2
4	1	4

3.2　π 变换的逆变换 π^{-1}

π 变换基于 GF(5)上的二阶变换方阵 $\begin{pmatrix}0 & 1\\ 2 & 3\end{pmatrix}$，遵从前述 GF(5)上的运算规则,应用高斯消元法对此二阶方阵求逆如下:

$$\begin{pmatrix}0 & 1 & 1 & 0\\ 2 & 3 & 0 & 1\end{pmatrix}\rightarrow\begin{pmatrix}2 & 3 & 0 & 1\\ 0 & 1 & 1 & 0\end{pmatrix}\rightarrow$$

$$\begin{pmatrix}1 & 4 & 0 & 3\\ 0 & 1 & 1 & 0\end{pmatrix}\rightarrow\begin{pmatrix}1 & 0 & 1 & 3\\ 0 & 1 & 1 & 0\end{pmatrix}$$，得到其逆矩阵为 $\begin{pmatrix}1 & 3\\ 1 & 0\end{pmatrix}$，因此 π 变换的逆变换为 π^{-1}:$a[x][y][z]\leftarrow a[x'][y'][z']$,$\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}1 & 3\\ 1 & 0\end{pmatrix}\begin{pmatrix}x'\\ y'\end{pmatrix}$。

4　χ 的逆变换

χ 是 Keccak 轮函数中唯一的非线性变换。χ 对沿 x 轴一行中的 5 个比特进行运算,因此可将 χ 看作一个输入输出均为 5 比特的 S 盒。令 $X=(x_1,x_2,x_3,x_4,x_5)$ 表示一行,则 χ 变换可表示为$(x_1,x_2,x_3,x_4,x_5)\rightarrow\chi(f(x_1),f(x_2),f(x_3),f(x_4),f(x_5))$。

4.1　χ 变换的真值表

根据 χ 变换的表达式,可得到 χ 变换的真值表,如表 5 所示。

表 5　χ 的真值表

(x_1,x_2,x_3,x_4,x_5)	$\chi(f(x_1),f(x_2),f(x_3),f(x_4),f(x_5))$
(0,0,0,0,0)	(0,0,0,0,0)
(0,0,0,0,1)	(0,0,1,0,1)
(0,0,0,1,0)	(0,1,0,1,0)
(0,0,0,1,1)	(0,1,0,1,1)
(0,0,1,0,0)	(1,0,1,0,0)
(0,0,1,0,1)	(1,0,0,0,1)
(0,0,1,1,0)	(1,0,1,1,0)
(0,0,1,1,1)	(1,0,1,1,1)
(0,1,0,0,0)	(0,1,0,0,1)
(0,1,0,0,1)	(0,1,1,0,0)
(0,1,0,1,0)	(0,0,0,1,1)
(0,1,0,1,1)	(0,0,0,1,0)
(0,1,1,0,0)	(0,1,1,0,1)
(0,1,1,0,1)	(0,1,0,0,0)
(0,1,1,1,0)	(0,1,1,1,1)
(0,1,1,1,1)	(0,1,1,1,0)
(1,0,0,0,0)	(1,0,0,1,0)
(1,0,0,0,1)	(1,0,1,0,1)
(1,0,0,1,0)	(1,1,0,0,0)
(1,0,0,1,1)	(1,1,0,1,1)
(1,0,1,0,0)	(0,0,1,1,0)
(1,0,1,0,1)	(0,0,0,0,1)
(1,0,1,1,0)	(0,0,1,0,0)
(1,0,1,1,1)	(0,0,1,1,1)
(1,1,0,0,0)	(1,1,0,1,0)
(1,1,0,0,1)	(1,1,1,0,1)
(1,1,0,1,0)	(1,0,0,0,0)
(1,1,0,1,1)	(1,0,0,1,1)
(1,1,1,0,0)	(1,1,1,1,0)
(1,1,1,0,1)	(1,1,0,0,1)
(1,1,1,1,0)	(1,1,1,0,0)
(1,1,1,1,1)	(1,1,1,1,1)

4.2　χ^{-1}的布尔函数表达式

根据 χ 的真值表,可将其逆变换 χ^{-1} 的布尔函数表达式推导出来。将 $\chi(f(x_1),f(x_2),f(x_3),f(x_4),f(x_5))$看作输入,$(x_1,x_2,x_3,x_4,x_5)$看作输出,利用布尔函数推导出 χ 变换的逆变换 $\chi^{-1}(f^{-1}(x_1),f^{-1}(x_2),f^{-1}(x_3),f^{-1}(x_4),f^{-1}(x_5))$。这里只给出了 $f^{-1}(x_1)$ 的详细推导:

$$f^{-1}(x_1)=(x_2+1)(x_3+1)(x_5+1)x_1x_3+(x_2+1)(x_4+1)x_1x_3x_5+(x_3+1)(x_4+1)(x_5+1)x_1x_2+(x_3+1)x_1x_2x_4x_5+$$

$(x_1+1)(x_2+1)(x_5+1)x_3x_4+(x_1+1)(x_2+1)(x_3+1)(x_4+1)x_5+(x_1+1)(x_2+1)(x_4+1)(x_5+1)x_3+(x_1+1)(x_2+1)x_3x_4x_5+(x_3+1)(x_5+1)x_1x_2x_4+(x_4+1)x_1x_2x_3x_5+(x_5+1)x_1x_2x_3x_4+(x_2+1)(x_3+1)(x_4+1)(x_5+1)x_1+(x_2+1)(x_3+1)x_1x_4x_5+(x_3+1)(x_4+1)x_1x_2x_5+(x_4+1)(x_5+1)x_1x_2x_3+x_1x_2x_3x_4x_5=x_1+x_3+x_5+x_2x_3+x_2x_5+x_4x_5+x_2x_4x_5$

同理可得

$f^{-1}(x_2)=x_1+x_2+x_4+x_1x_3+x_1x_5+x_3x_4+x_1x_3x_5$

$f^{-1}(x_3)=x_2+x_3+x_5+x_1x_2+x_2x_4+x_4x_5+x_1x_2x_4$

$f^{-1}(x_4)=x_1+x_3+x_4+x_3x_5+x_2x_3+x_1x_5+x_2x_3x_5$

$f^{-1}(x_5)=x_2+x_4+x_5+x_1x_2+x_1x_4+x_3x_4+x_1x_3x_4$

综上推导可得到χ变换的逆变换χ^{-1}的布尔函数表达式为：

$\chi^{-1}(f^{-1}(x_1),f^{-1}(x_2),f^{-1}(x_3),f^{-1}(x_4),f^{-1}(x_5))=(x_1+x_3+x_5+x_2x_3+x_2x_5+x_4x_5+x_2x_4x_5,x_1+x_2+x_4+x_1x_3+x_1x_5+x_3x_4+x_1x_3x_5,x_2+x_3+x_5+x_1x_2+x_2x_4+x_4x_5+x_1x_2x_4,x_1+x_3+x_4+x_3x_5+x_2x_3+x_1x_5+x_2x_3x_5,x_2+x_4+x_5+x_1x_2+x_1x_4+x_3x_4+x_1x_3x_4)$

4.3 差分路径以概率 1 通过χ^{-1}

我国学者王小云教授提出的消息修改技术在差分攻击中有着重要意义，可大大提高攻击成功的概率。在对 Keccak 进行攻击时可对消息施加条件从而对给定输入差分的输出进行控制，使差分路径以概率 1 通过χ^{-1}。例如，对于输入差分(1,0,0,0,0)，其输出差分的布尔函数表达式为$(1,1+x_3+x_5+x_3x_5,x_2+x_2x_4,1+x_5,x_2+x_4+x_3x_4)$，若要使输出差分也为(1,0,0,0,0)，可令消息中$x_5=1,x_2=x_4=0$。满足以上三比特条件的消息必定符合给定的差分路径，即施加条件后输入与输出差分相等的概率为 1。

5 结束语

文中对 SHA-3 轮函数中ρ、π、χ三个变换进行了深入研究，得到了它们的逆变换。对于 SHA-3 轮函数中唯一的非线性变换χ，利用χ的真值表，通过布尔函数的推导得到了χ^{-1}的布尔函数表达式。π变换的逆变换可归结为矩阵求逆问题，但由于π变换的二阶方阵是基于 5 元有限域运算的，故在利用高斯消元法求逆过程中的所有运算都应符合 GF(5)的上运算规则。ρ变换的逆变换相对简单，只需对照其移位表沿 z 轴负方向移位相同距离即可得到其逆变换ρ^{-1}。

基于ρ^{-1}、π^{-1}、χ^{-1}可利用中间相遇攻击的思想构造差分路径对 SHA-3 进行攻击。结合王小云教授提出的消息修改技术及χ^{-1}的布尔函数表达式，通过对消息附加条件可使差分路径以概率 1 通过χ^{-1}，较之查找χ的差分分布表的方法大大提高了成功率。θ变换是 SHA-3 轮函数中的第一个变换，也是最复杂的一个变换，其扩散能力非常强。如果能够得到θ的逆变换将会进一步提高攻击成功的概率，因此求得θ^{-1}具有重要的意义。这也是进一步研究的重点。

参考文献：

[1] Wang Xiaoyun, Yu Hongbo. How to break MD5 and other Hash functions[C]//Proc of EUROCRYPT 2005. Berlin: Springer-Verlag, 2005: 19-35.

[2] Wang Xiaoyun, Yin Y L, Yu Hongbo. Finding collisions in the full SHA-1[C]//Proc of CRYPTO 2005. Santa, Barbara: [s. n.], 2005: 17-36.

[3] Wang Xiaoyun, Feng Dengguo, Yu Xiuyuan. An attack on hash function HAVAL-128[J]. Science in China Ser F, 2005, 48(5): 545-556.

[4] Wang Xiaoyun, Lai Xuejia, Feng Dengguo, et al. Cryptanalysis of the hash functions MD4 and RIPEMD[C]//Proc of EUROCRYPT 2005. [s. l.]: [s. n.], 2005: 1-18.

[5] NIST. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family[EB/OL]. 2007. http://csrc. nist. gov/groups/ST/hash/index. html.

[6] Bertoni G, Daemen J, Peeters M, et al. The KECCAK reference [EB/OL]. 2012. http://KECCAK. noekeon. org/KECCAK-reference-3.0.0. pdf.

[7] National institute of standards and technology: SHA-3 selection announcement [EB/OL]. 2012. http://csrc. nist. gov/groups/ST/hash/sha-3/sha-3_selection_announcement. pdf.

[8] 梁 晗. SHA-3 杂凑算法硬件实现研究[D]. 北京：清华大学，2011.

[9] 丁冬平. 基于 FPGA 的 SHA-3 五种候选算法设计实现[D]. 西安：西安电子科技大学，2012.

[10] 吴武飞，王 奕，李仁发. 可重构 Keccak 算法设计及 FPGA 实现[J]. 计算机应用，2012，32(3)：864-866.

[11] 刘 花，包小敏. SHA-3 候选算法 Keccak 的 Matlab 设计与实现[J]. 计算机科学，2012，39(6A)：425-428.

[12] 李梦东，邵鹏林，李小龙. SHA-3 获胜算法：Keccak 评析[J]. 北京电子科技学院学报，2013，21(2)：18-23.

[13] 薛 宇，吴文玲，王张宜. SHA-3 杂凑密码候选算法简评[J]. 中国科学院研究生院学报，2009，26(5)：577-586.

[14] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[C]//Proc of CRYPTO. [s. l.]: [s. n.], 1990: 2-21.

[15] Diffie W, Hellman M. Exhaustive cryptanalysis of the NBS data encryption standard[J]. Computer, 1977, 10(6): 74-84.

[16] Bertoni G, Daemen J, Peeters M, et al. Sponge functions[EB/OL]. 2007. http://sponge. noekeon. org/SpongeFunctions. pdf.

[17] Paar C, Pelzl J. 深入浅出密码学-常用加密技术原理与应用[M]. 马小婷，译. 北京：清华大学出版社，2012.

S HA-3轮函数中ρ、π及χ变换的逆变换

作者： 王淦， 张文英， WANG Gan， ZHANG Wen-ying
作者单位： 山东师范大学 信息科学与工程学院，山东 济南 250014；山东省分布式计算机软件新技术重点实验室，山东 济南 250014

刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2014(12)