单向 Hash 函数 SHA-1 的统计分析与算法改进

刘建东 余有明 江慧娜
(北京石油化工学院信息工程学院 北京 102617)

摘 要 对SHA-1算法的完备度、雪崩效应度、严格雪崩效应及抗碰撞性进行了逐拍统计分析。针对目前密码学界所揭示出的SHA-1设计缺陷,主要以增强SHA-1算法的非线性扩散特性及抗碰撞性为目标,对其进行改进。改进算法在混合函数中逆序使用改进后的扩展码字序列,并在算法首轮的混合函数中引入整数帐篷映射,加速了差分扩散,改变了原来固定的链接变量传递方式,修正了算法内部结构的设计缺陷。测试与分析结果表明,改进算法提高了非线性扩散程度,增强了算法的安全性。

关键词 Hash函数,安全散列函数算法,码字扩展,帐篷映射,扩散
中图法分类号 TP309.2 **文献标识码** A

Statistical Analysis of One-way Hash Function SHA-1 and its Algorithm Improvement

LIU Jian-dong YU You-ming JIANG Hui-na
(Information Engineering College, Beijing Institute of Petrochemical Technology, Beijing 102617, China)

Abstract The degrees of completeness and avalanche effect and strict avalanche criterion for SHA-1 with increased number of steps were statistically analyzed. In order to improve the performance of collision resistance and nonlinear diffusion for SHA-1, the original algorithm was improved for its design defects and vulnerability indicated in the field of the current cryptology. The improved algorithm with mix function applied inverse message expansions sequence and inserted Integer tent maps at the first round of mix function, to accelerate differential diffusion, to alter the original linked variables passing method, to correct the inner design architecture defects of the algorithm. The test and analysis results proved the reforming algorithm improved the degrees of nonlinear diffusion and enhanced the security of the algorithm.

Keywords Hash function, SHA-1, Message expansions, Tent map, Diffusion

1 引言

1995年,美国国家标准与技术研究所(NIST)在FIPS PUBS(Federal Information Processing Standards Publication 1995 April 17)上公布了新的Hash函数标准,即FIPS PUBS 180-1-1995,替代了1993年颁布的Hash函数标准PUBS 180-1-1993。新颁布的Hash函数标准算法称为安全散列函数算法SHA-1[1]。SHA-1是目前国际通用的Hash函数算法,被认为是现代网络安全的基石,广泛使用于银行、安全通讯以及电子商务中。2005年2月13日,王小云等人宣告破解了SHA-1[2],此举成为破译MD5之后,国际密码学领域的又一突破性研究成果,她们已将碰撞攻击的复杂度提高到2^{63}[3]。

一个具有n比特输出长度的Hash函数共有2^n个可能的输出值,用穷举法只要计算$2^{n/2}$个消息,就能期望找到一对碰撞,因此,值$2^{n/2}$决定了Hash函数抗强行攻击的强度。如果一个输出长度为n比特的Hash函数可以以小于$2^{n/2}$的计算找到一对碰撞,则该Hash函数理论上被认为是可破解的。对于SHA-1算法,使用穷举法寻找它的碰撞至少需要进行2^{80}次运算,而使用王小云等人的密码分析方法,则可以将攻击速度提高2^{17}倍,这充分暴露了SHA-1在碰撞处理方面存在严重的安全缺陷。

由于王小云等人揭示出SHA-1的脆弱性,NIST计划举行Hash函数标准的公开征集,并在2007年初公布了可接受的最低设计标准及评估标准[4]。虽然当前使用的算法有严重缺陷,但是我们也看到,这么多年来没有比现有算法更安全的算法,所以专家们建议在设计下一代Hash算法时应更多地考虑改进现有的算法和设计范例。由于SHA-1已有多年的软硬件设备积淀,有着深厚的应用基础和商用社会资源,因此,我们认为有必要修改完善SHA-1算法,并保持对现有软硬件的良好兼容性。

本文对SHA-1算法的完备度、雪崩效应度、严格雪崩效应及抗碰撞性进行了逐拍统计分析,以便发现其存在的问题。以提高非线性扩散特性及抗碰撞能力为目标,给出SHA-1算法的改进方案。改进算法提高了消息差分扩散程度,增强了算法的安全性,执行效率与SHA-1相接近。

到稿日期:2008-09-25 返修日期:2009-04-24 本文受北京市教委科技发展计划项目(KM200710017007)资助。
刘建东(1966—),男,副教授,主要研究方向为信息安全等,E-mail:liujiandong@bipt.edu.cn;余有明(1968—),男,博士,副教授,主要研究方向为智能计算等;江慧娜(1980—),女,硕士,主要研究方向为计算机应用。

2 SHA-1 扩散特性及抗碰撞特性的统计分析

2.1 SHA-1 算法描述

SHA-1 算法使用了一组基本逻辑函数 $f_t(x,y,z)$及一组常数 K_t，采取 512 比特的消息分组，每一个消息分组 x_i 被分成 16 个字 $M_0,M_1,\cdots,M_{15}$。为便于理解，下面简要给出其 Hash 值的计算过程：

(1) 初始化 $H_0^{(0)}=0x67452301$，$H_1^{(0)}=0xEFCDAB89$，$H_2^{(0)}=0x98BADCFE$，$H_3^{(0)}=0x10325476$，$H_4^{(0)}=0xC3D2E1F0$；

(2) $W_t=$

$$\begin{cases} M_t, & 0\leqslant t\leqslant 15 \\ (W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16})<<<1, & 16\leqslant t\leqslant 79 \end{cases};$$

(3) 令 $A=H_0^{(i-1)}$，$B=H_1^{(i-1)}$，$C=H_2^{(i-1)}$，$D=H_3^{(i-1)}$，$E=H_4^{(i-1)}$；

(4) 对 $t=0\sim79$：$T=A<<<5+f_t(B,C,D)+E+W_t+K_t$，$B=B<<<30$，$E=D$，$D=C$，$C=B$，$B=A$，$A=T$；

(5) $H_0^{(i)}=H_0^{(i-1)}+A$，$H_1^{(i)}=H_1^{(i-1)}+B$，$H_2^{(i)}=H_2^{(i-1)}+C$，$H_3^{(i)}=H_3^{(i-1)}+D$，$H_4^{(i)}=H_4^{(i-1)}+E$；

(6) 以 $H_0^{(i)},\cdots,H_4^{(i)}$ 作为初始化常数，对剩下的消息分组进行处理，直到最后一个分组，最后输出 160 比特的 Hash 值。

2.2 非线性扩散特性分析

密码算法的混淆与扩散程度可以通过非线性扩散特性的统计检测给出一个概率上的结论。用统计方法对密码算法的非线性扩散程度进行分析通常要包括算法的完备性、雪崩效应及严格雪崩准则等方面。按文献[5]的定义：完备性是指函数输出值的每一个比特都与消息输入的所有比特有关，雪崩效应是指消息输入中任意一个比特的改变都应造成输出平均半数比特的改变，严格雪崩准则是指消息输入中任意一个比特的改变都会造成输出的每一个比特以 1/2 的概率发生改变。

设 H 是一个 n 比特输入 m 比特输出的 Hash 算法，输入向量为 $x=(x_1,\cdots,x_n)\in(0,1)^n$，仅改变 x 的第 i 比特后的输入向量为 $x(i)\in(0,1)^n$。它们经过压缩映射后对应的输出向量分别记为 $H(x)$、$H(x^{(i)})\in(0,1)^m$。

$(.)_j$ 表示向量的第 j 比特，$w(.)$表示向量的汉明重量，$\#\{.\}$表示集合的势。设 X 为 Hash 算法输入的样本空间，记 $a_{ij}=\#\{x\in X|(H(x))_j\neq(H(x^{(i)}))_j\}$(其中 $i=1,2,\cdots,n$；$j=1,2,\cdots,m$)表示 X 中的输入向量 x 和 $x^{(i)}$ 对应的输出向量之间第 j 比特不同的个数；$b_{ij}=\#\{x\in X|w(H(x^{(i)})-H(x))=j\}$(其中 $i=1,2,\cdots,n;j=1,2,\cdots,m$)表示 X 中的输入向量 x 和 $x^{(i)}$ 对应的输出向量之间的差分汉明重量为 j 的个数。定义 3 个统计度量：

完备性程度的度量：

$$d_c=1-\frac{\#\{(i,j)\mid a_{ij}=0\}}{nm}$$

雪崩效应程度的度量：

$$d_a=1-\frac{\sum_{i=1}^{n}\left|\frac{1}{\#X}\sum_{j=1}^{m}2jb_{ij}-m\right|}{nm}$$

严格雪崩程度的度量：

$$d_{sa}=1-\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left|\frac{2a_{ij}}{\#X}-1\right|}{nm}$$

若 $H(.)$是随机变换(随机 oracle 模型)，$z_{\alpha/2}$ 表示标准正态分布的 $\alpha/2$ 分位点，文献[6]给出如下结论：

1) 测试的样本量 X 至少应为 $nm\times(z_{\alpha/2})^2$；

2) $p(d_c)=1-2^{-\#X}\approx1.0$；

3) $E\{d_a\}=1.0-\sqrt{2/(\pi\times m\times\#X)}$，其置信区间为 $(E\{d_a\}-z_{\alpha/2}\sqrt{1/(n\times m\times\#X)},E\{d_a\}+z_{\alpha/2}\sqrt{1/(n\times m\times\#X)})$；

4) $E\{d_{sa}\}=1.0-\sqrt{2/(\pi\times\#X)}$，其置信区间为 $(E\{d_{sa}\}-z\alpha/2\sqrt{1/(n\times m\times\#X)},E\{d_{sa}\}+z\alpha/2\sqrt{1/(n\times m\times\#X)})$。

理想的 Hash 函数应该是从所有可能的输入值到有限可能的输出值集合的一个随机映射。严格地讲，像随机 oracle 模型这样的 Hash 函数是不存在的。因为 Hash 函数是确定性的，而确定性和均匀输出特性意味着输出的熵大于其输入的熵。但根据香农熵理论，一个确定性函数决不可能放大熵。一个实际的 Hash 函数，测试其统计量 d_c，d_a，d_{sa}，若落入其置信区间，则说明 Hash 算法满足非线性扩散的基本要求，即可以认为 Hash 函数具有很好的完全性和雪崩效应，满足严格雪崩准则。

取输入长度 $n=512$ 比特，输出长度 $m=160$ 比特，在显著水平 $\alpha=0.05$ 下，对于随机 oracle 模型，得到如下结果：

1) $z_{\alpha/2}=1.92$，选取样本容量 X 为 320000；

2) $d_c=1.000000$；

3) $E\{d_a\}=0.999888$，其置信区间为(0.999876，0.999900)；

4) $E\{d_{sa}\}=0.998589$，其置信区间为(0.998577，0.998601)。

在上述条件下，随机选取 320000 组 512 比特字(取自 Visual C 的 Rand())的样本集 X 作为 SHA-1 算法的消息输入，对 SHA-1 算法的扩散性能进行逐拍统计测试，实际的测试结果如表 1 所列。

表 1 SHA-1 算法扩散性能的逐拍统计结果

number of Iterations	d_c	d_a	d_{sa}
1	0.006396	0.001559	0.000574
3	0.051648	0.009894	0.004823
5	0.145032	0.036693	0.024572
7	0.267920	0.092986	0.073287
10	0.456213	0.237795	0.212311
15	0.768115	0.544870	0.518823
20	0.987427	0.845407	0.823081
25	1.000000	0.993809	0.989917
30	1.000000	0.999892	0.998594
40	1.000000	0.999885	0.998594
60	1.000000	0.999887	0.998587
80	1.000000	0.999896	0.998589

从表 1 可以看出，在显著水平 $\alpha=0.05$ 的情况下，SHA-1 算法的完备度 d_c 在迭代 25 拍之后开始与随机映射无法区分，统计量 d_a，d_{sa} 在迭代 30 拍之后才落入了各自的置信区间，与随机映射无法区分。

2.3 抗碰撞性的统计分析

Hash 函数的值域与定义域相比规模要小得多，是“多对一”映射。找出两个不同的消息，使其产生相同的 Hash 结果称为碰撞攻击。通过以下的实验来定量测试 Hash 算法的抗碰撞能力[7]：在明文空间中随机选取一段明文求出其 Hash

值，并以单字节字符的方式来表示，然后随机地选择并改变明文中 1 比特的值得到另一新的 Hash 结果。定义两个 Hash 值之间的距离为：

$$d=\sum_{i=1}^{S}|t(e_i)-t(e_i')|$$

其中，e_i 和 e_i' 分别是最初的和新的 hash 值的第 i 个字符，S 为 Hash 值对应字符的个数，函数 $t(\cdot)$ 将 e_i 和 e_i' 转换成对应的十进制数。若两个 Hash 值分别由两个独立的均匀分布的随机序列所组成，则理论上 Hash 值的单位字符的平均距离为 85.33[7]。

取输入长度 $n=512$ 比特，随机选择输入样本，测试其输出的单位字符的平均距离。经 10 万次统计测试，得到实际的测试结果如表 2 所列。

表 2　SHA-1 算法抗碰撞性的逐拍统计结果

number of Iterations	1	5	10	20	30	40	80
Average distances /character	0.006	0.714	21.22	73.22	85.34	85.40	85.36

从表 2 可以看出，SHA-1 算法在迭代 30 拍之后，其输出的单位字符的平均距离才趋于稳定，并接近理论值。

3　算法改进及其特性分析

3.1　SHA-1 码字扩展分析

所谓码字扩展，是指输入的消息分组被扩展成许多消息字。MDx 类(MD4，MD5，HAVAL，RIPEMD，RIPEMD-160)的消息扩展是在每轮中对输入的消息分组进行置换，SHA 类(SHA-1，SHA-256，383，512)是通过递归关系进行扩展。MDx 类的消息扩展码字重量远小于 SHA 类。以 MD5 为例，在一个消息分组(512 比特)中，若有 1 比特不同，则在其消息扩展码中会有 4 比特位不同，因此，MD5 差分消息扩展码字的最小码字重量仅为 4。SHA 类采取递归方式进行消息扩展，保证了消息的每个比特都会影响到更多的比特位。为了说明消息的扩展过程，随机选取一个消息分组(512 比特)，每次改变一个比特，观察其在随后的递归过程中对 2048(64 * 32)个扩展比特位的影响，得到的结果如图 1 所示。

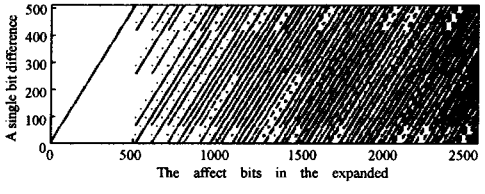


图 1　SHA-1 的码字扩展

从图 1 可看出，递归过程会逐渐加剧码字差分扩散程度。用 2.2 节的方法，在 SHA-1 混合函数中逆序使用消息扩展码，并对逆序使用消息扩展码的 SHA-1 算法的扩散性能进行逐拍统计测试，实际的测试结果如表 3 所列。

表 3　逆序使用消息扩展码时 SHA-1 算法的扩散特性

number of Iterations	d_c	d_a	d_{sa}
1	0.167395	0.085208	0.032819
5	0.974169	0.759469	0.580398
7	1.000000	0.957792	0.876638
10	1.000000	0.999130	0.997290
15	1.000000	0.999886	0.998589
20	1.000000	0.999890	0.998584
40	1.000000	0.999885	0.998589
60	1.000000	0.999879	0.998589
80	1.000000	0.999886	0.998587

从表 3 可以看出，在显著水平 $\alpha=0.05$ 的情况下，逆序使用消息扩展码时 SHA-1 算法的完备度 d_c 在迭代 7 拍之后开始与随机映射无法区分，统计量 d_a，d_{sa} 在迭代 15 拍之后落入了各自的置信区间，与随机映射无法区分。显然，与 SHA-1 算法的非线性扩散特性相比(如表 1 所列)，在逆序使用消息扩展码的情况下，算法的非线性扩散特性得到了明显改善。

3.2　改进的 SHA-1 码字扩展分析

SHA-1 采用递归方式进行码字扩展，增强了算法的安全性。但近年来的分析表明，SHA-1 的消息递归扩展方式仍有缺陷，致使在 MD5 被攻破不久，SHA-1 就遭受重创。主要原因是 SHA-1 消息扩展码字重量的下界太低。在 SHA-1 的消息空间中，16 个 32 比特的自由变量生成的搜索空间可达到 2^{512}，然而，由于 SHA-1 所采用的消息扩展是一种准循环码，具有线性化特征，通过直观观察分析，就可以将搜索最小码字重量的范围缩小到 2^{38}，王小云等在这个缩小的子空间中找到一组码字重量为 44 的消息扩展码字(后 64 个字的码字重量仅为 30)[2]。

对 Hash 函数的差分攻击的复杂度与压缩函数中消息的差分扩散程度成正比(在目前较成功的模减差分攻击方法中，一般认为，扩展了的输入消息中的一个差分点大概对应 $2^{2.5}$ 个碰撞差分链的导出条件)。消息扩展码字的最小码字重量越大，则对压缩函数的差分攻击的复杂度就越大。文献[8]对 SHA-1 的码字扩展方式进行了改进，并且证明改进后的最小码字重量为 82(后 64 个码字)。其改进后的码字递归扩展方式为：

$$W_t=\begin{cases}M_t, & 0\leqslant t\leqslant 15\\ W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16}\oplus (W_{t-1}\oplus W_{t-2}\oplus W_{t-5})<<<13, & 16\leqslant t\leqslant 36\\ W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16}\oplus (W_{t-1}\oplus W_{t-2}\oplus W_{t-5}\oplus W_{t-20})<<<13, & 36\leqslant t\leqslant 79\end{cases}$$

我们仍随机选取一个消息分组(512 比特)，每次改变一个比特，观察其在随后的递归过程中对 2048(64 * 32)个扩展比特位的影响，得到的结果如图 2 所示。

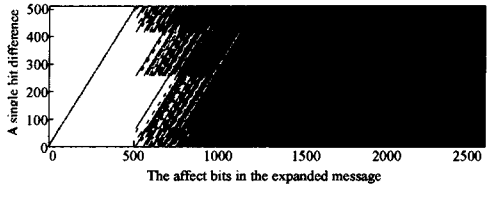


图 2　改进的 SHA-1 码字扩展

3.3　SHA-1 算法的局部碰撞[2]

在 SHA-1 的内部结构中，链接变量 A 经过 6 个操作步的传递、混合后，又回到 A，链接变量 B,C,D,E 同样如此，这样，就容易实现 6 操作步的局部碰撞(或局部近似碰撞)。例如，若在 SHA-1 算法第 i 步存在 1 比特消息差分，这 1 比特差分将在随后的 5 操作步中依次影响 5 个链接变量。若能阻止差分传播，则可构造一个局部碰撞差分链，进而产生 6 操作步的局部碰撞。

3.4 改进的 SHA-1 算法

为了增强算法的非线性扩散特性，修正算法内部结构的设计缺陷，将 SHA-1 算法中 Hash 值的计算过程作了如下改进：

(1) 定义 G=0x80000000；

初始化 $H_0^{(0)}$=0x67452301，$H_1^{(0)}$=0xEFCDAB89，$H_2^{(0)}$=0x98BADCFE，$H_3^{(0)}$=0x10325476，$H_4^{(0)}$=0xC3D2E1F0；

(2) W_t=

$$\begin{cases} M_t, & 0\leqslant t\leqslant 15 \\ W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16}\oplus(W_{t-1} \\ \quad \oplus W_{t-2}\oplus W_{t-5})<<<13, & 16\leqslant t\leqslant 36 \\ W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16}\oplus(W_{t-1} \\ \quad \oplus W_{t-2}\oplus W_{t-5}\oplus W_{t-20})<<<13, & 36\leqslant t\leqslant 79 \end{cases}$$

(3) 令 $A=H_0^{(i-1)}$，$B=H_1^{(i-1)}$，$C=H_2^{(i-1)}$，$D=H_3^{(i-1)}$，$E=H_4^{(i-1)}$；

(4) 对 t=0～19：$T=A<<<5+f_t(B,C,D)+E+W_{(79-t)}+K_t$，$B=B<<<30$，

$A=T<G$? $(E=D,D=C,C=B,B=A,(T<<1)+1)$：$(D=B,B=E,E=C,C=A,(\sim T)<<1)$；

对 t=20～79：$T=A<<<5+f_t(B,C,D)+E+W_{(79-t)}+K_t$，$B=B<<<30$，

$E=D,D=C,C=B,B=A,A=T$；

(5) $H_0^{(i)}=H_0^{(i-1)}+A$，$H_1^{(i)}=H_1^{(i-1)}+B$，$H_2^{(i)}=H_2^{(i-1)}+C$，$H_3^{(i)}=H_3^{(i-1)}+D$，$H_4^{(i)}=H_4^{(i-1)}+E$；

(6) 以 $H_0^{(i)}$，…，$H_4^{(i)}$ 作为初始化常数，对剩下的消息分组进行处理，直到最后一个分组，最后输出 160 比特的 Hash 值。

对改进算法的两点说明：

(1) 改进了码字扩展方式，并且在混合函数中逆序使用了扩展码字序列。

(2) 在算法第一轮的混合函数中，引入了整数帐篷映射[9]，目的在于加速首轮的差分扩散，并且打破原来固定的链接变量传递方式，使传递过程具有“随机性”，消除局部碰撞的依从条件。

在以上的改进算法中，定义 $G=2^{31}$，在 $GF(2^{32})$ 内，用 C 语言中的三元运算符(?:)对整数帐篷映射的计算过程进行了描述，可用简单的逻辑判断、逻辑取反及移位操作予以实现。整数帐篷映射具有拉伸与折叠的非线性本质，其伸长特性最终导致相邻点的指数分离，其折叠特性则保持生成序列有界，且引起映射不可逆。这与香农在经典论文《communication theory of secrecy systems》[10]中所指出的好的保密系统需要基本的“rolled-out and folded-over”操作极为相似。若用汇编语言或硬件实现，则其操作可以进一步简化为：测试字的最高位是否为 0，若为 0，则左移一位加 1，否则，则各位求反后，左移一位。实测结果表明，执行效率与 SHA-1 所使用的逻辑函数相当。

3.5 改进算法扩散特性分析

用 2.2 节的方法，对改进的 SHA-1 算法的扩散性能进行逐拍统计测试，实测结果如表 4 所列。

表 4 改进算法扩散性能的逐拍统计结果

number of Iterations	d_c	d_a	d_{sa}
1	0.542443	0.540134	0.396988
3	1.000000	0.983498	0.914854
7	1.000000	0.999882	0.996341
10	1.000000	0.999888	0.998596
15	1.000000	0.999891	0.998586
20	1.000000	0.999879	0.998593
30	1.000000	0.999885	0.998587
40	1.000000	0.999896	0.998585
60	1.000000	0.999892	0.998587
80	1.000000	0.999890	0.998586

从表 4 可以看出，在显著水平 α=0.05 的情况下，改进的 SHA-1 算法的完备度 d_c 在迭代 3 拍之后就与随机映射模型无法区分，雪崩效应度 d_a 及严格雪崩效应度 d_{sa} 分别在迭代 7 拍及 10 拍之后就落入了各自的置信区间，与随机映射模型无法区分。显然，与 SHA-1 算法及逆序使用消息扩展码的 SHA-1 算法的非线性扩散特性相比(如表 1、表 3 所列)，算法的非线性扩散特性有了更大程度的改善。

3.6 改进算法抗碰撞性分析

用 2.3 节的方法，对改进的 SHA-1 算法的抗碰撞特性进行逐拍统计测试，实测结果如表 5 所列。

表 5 改进 SHA-1 算法抗碰撞性的逐拍统计结果

number of Iterations	1	5	10	20	40	80
Average distances /character	61.411	83.621	85.342	85.346	85.341	85.336

从表 5 可以看出，改进 SHA-1 算法在迭代 10 拍之后，其输出的单位字符的平均距离就趋于稳定，并接近理论值；与此相比，SHA-1 算法从第 30 操作步才开始趋于稳定。这一测试结果表明，仅有 1 比特不同的两个明文分组(512 比特)，改进 SHA-1 算法压缩函数经 10 拍迭代处理后，所得到的两组不同的链接变量的值在统计上即相当于由相互独立的两个均匀随机序列构成。

3.7 改进算法的执行效率

表 6 给出在 P4，2.0GHz 主频条件下，用 C 语言实现的 SHA-1 及改进的 SHA-1 算法的速度测试结果。从表 6 可见，改进算法的执行效率与原算法很接近。

表 6 改进算法与 SHA-1 的速度比较

Data Length(B)	240	2048
Speed of SHA-1(Mbps)	164.68	189.95
Speed of the Improved SHA-1(Mbps)	148.22	176.98

结束语 目前对 Hash 函数的有效攻击方法是针对其内部结构的模差分分析。因此，在分析 Hash 算法的安全性时，仅对 Hash 函数的最终输出结果进行扩散与碰撞特性分析是远远不够的。正如对对称加密算法的评测应逐轮进行一样，对 Hash 函数的评估也应逐拍进行。本文对 SHA-1 的非线性扩散特性及抗碰撞特性进行了逐拍分析，主要以增强差分扩散特性为目标，对 SHA-1 算法进行了改进。改进算法在消息填充及整体结构上未进行改动，因此，在现有 SHA-1 软硬件产品的基础上稍作修改，即可实现本文给出的改进的 SHA-1 算法，容易实现原有的基于 SHA-1 的软硬件产品的升级。

参 考 文 献

[1] NIST. Secure hash standard[S]. Federal Information Processing Standards, FIPS-180-1, April 1995

[2] Wang X Y, Yin Y L, Yu H B. Finding collisions on the Full SHA-1[C]// Advances in Cryptology—Crypto'05, LNCS 3621. 2005: 17-36

[3] Wang X, Yao A, Yao F. New Collision Search for SHA-1[C]// Presentation at rump session of Crypto 2005

[4] National Institute of Standards and Technology. Announcing the Development of New Hash Algorithms for the Revision of FIPS 180-2[S]. Secure Hash Standard. Federal Register, January 2007

[5] Weister AF, TavaresSE. On the design of S-boxes[A]// Dvances in Cryptology-CRYPTO'85[C]. Berlin: Springer-Verlag, 1986: 523-533

[6] 朱明富，张宝东，吕述望. 分组密码算法扩散特性的一种统计分析[J]. 通信学报，2002，23(10)：122-128

[7] 盛利元，李更强，李志炜. 基于切延迟椭圆反射腔映射系统的单向 Hash 函数构造[J]. 物理学报，2006，55(11)：5700-5706

[8] Jutla C S, Patthak A C. A Simple and Provably Good Code for SHA Message Expansion[R]. Cryptology ePrint Archive, Report 2005/247, 2005. http://eprint.iacr.org/

[9] 刘建东. 基于整数耦合帐篷映射的单向 Hash 函数及其性能分析[J]. 计算机研究与发展，2008，45(3)：563-569

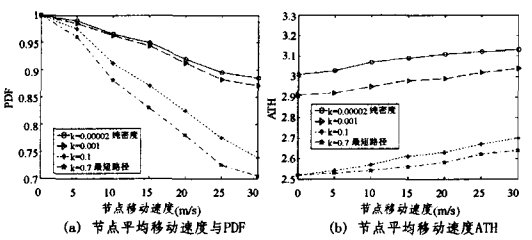
[10] Shannon C E. Communication Theory of Secrecy Systems[J]. Bell Systems Technical Journal, 1949, 28: 656-715

(上接第 119 页)

如图 2(a)、(b)所示，随着链接平均故障率上升，k 越小，PDF 表现相对越好，ATH 表现则相对越差。这是由于 $k=0.00002$ 时，即纯密度选择时，会选择密度最大的 $G(A)$ 组员作为目标，数据包经过的距离会略有增加，传输效率会有所降低。但一旦目标或中间节点失效，数据包重路由的成功率却大大提高；而 $k=0.7$ 时，即最短路径选择，在选择目标时会选择距离最短的 $G(A)$ 组员，数据包所经过的距离最短，传输效率较高。但一旦目标或中间节点失效，数据包重路由的成功率相对较低；$k=0.001$ 和 $k=0.1$ 时，即选择时密度因素与距离因素都占一定比例的权重，在路由健壮性及路由效率测试中表现居中。

实验 2　不同 k 值下节点速度对 PDF 及 ATH 的影响

网络环境设置如下：采用 NS-2 仿真平台模拟一个 2000m×2000m 区域；设定网络内有 500 个随机分布的移动节点，每个节点的移动速度相同；每个节点的通信传输范围是 200m，因此可以得出网络直径 D 约为 10m；$G(A)$ 组员数目 N 为 10。在不同 k 值下不断调节移动节点的平均速度(0～30m/s)，计算 PDF 及 ATH。仿真结果如图 3(a)、(b)所示。



(a) 节点平均移动速度与PDF　(b) 节点平均移动速度ATH

图 3　实验 2 仿真结果

如图 3(a)、(b)所示，随着节点平均移动速度上升，k 越小，PDF 表现相对越好，ATH 表现则相对越差。原因是节点速度的提高，导致目标不可达的概率提高。因此随着节点平均移动速度上升，$k=0.0002$ 时，即纯密度选择，PDF 表现最好，ATH 表现最差；$k=0.7$ 时，即最短路径选择，PDF 表现最差，ATH 表现最好；$k=0.001$ 和 $k=0.1$ 时，PDF 及 ATH 表现居中。

结束语　本文提出了一种路由判据为目标的距离因素和密度因素的任播路由协议。本文协议的特点在于可调性和适应性。协议通过调节参数 k，调节距离、密度因素的权重，从而影响任播组员的选择优先顺序。当网络动态性较高时，调节至密度因素权重较大，较好地保证了协议的路由健壮性；当网络变化较小时，调节至距离因素权重较大，较好地保证了协议的传输效率。仿真实验表明，本文协议可以根据不同网络状况调节 k 值，可以在路由健壮性及路由效率两者之间做出较好的权衡。

参 考 文 献

[1] Xuan D, Jia W, Tu W Q, et al. Distributed Admission Control for Anycast Flows[J]. Transactions on Parallel and Distributed Systems, 2004, 15(8): 673-686

[2] Hsu W H, Tung M C, Wu L Y. An integrated end-to-end QoS anycast routing on DiffServ networks[J]. Computer Communications, 2007, 30(6): 1406-1418

[3] Wang X. Analysis and Design of a k - anycast Communication Model in IPv6[J]. Computer Communications, 2008, 31(10): 2071-2077

[4] Hou Y T, Yi S, Sherali H D. Optimal base station selection for anycast routing in wireless sensor networks[J]. IEEE Transactions on Vehicular Technology, 2006, 15(3): 813-821

[5] Dow C R, Hsuan R, Hwang S F. Design and implementation of Anycast protocols for mobile Ad-hoc networks[C]// Proceedings of ICACT'2006. Phoenix Park, Korea: IEEE, 2006: 419-424

[6] Perkins C E, Bhagwat P. Highly Dynamic Destination-sequenced Distance-Vector Routing(DSDV) for Mobile Computers[C]// Proceedings of ACM SIGCOMM'94. 1994: 234-244

[7] Lin T, Midkiff S F, Park J S. Mobility Versus Link Stability in Simulation of Mobile Ad hoc Networks[C]// Proceedings of CNDS'03. 2003: 3-8

[8] Haas Z J, Pearlman M R. The Performance of Query Control Schemes for the Zone Routing Protocol[J]. IEEE/ACM Transactions on Networking, 2001, 9(4): 427-438