多变元 Hash 函数的构造与分析

王后珍[1,2],张焕国[1],杨 ▮[1]
(1.武汉大学计算机学院空天信息安全与可信计算教育部重点实验室,湖北武汉 430072;
2.中国科学院数学机械化重点实验室,北京 100080)

摘 要: 本文在基于非线性多变元多项式方程组难解性的基础上,提出了一种新的 Hash 算法,新算法与目前广泛使用的 Hash 算法相比具有下列优点:安全性基于一个公认的数学难题;输出 Hash 值长度可变;引入了整体随机性,从一族 Hash 函数中随机选择 Hash 函数而不是随机化消息本身;设计自动化,用户可根据实际需求构造满足其特定要求的 Hash 函数.本文还详细讨论了新 Hash 算法的安全性、效率和性能,并通过仿真实验,指出了新算法的具体构造方法.实验结果表明,新算法在效率和性能方面与其它 Hash 函数具有可比性.

关键词: 密码学; Hash 函数; MQ 问题; 多变元多项式
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0237-05

Design and Analysis of Multivariate Hash Function

WANG Hou-zhen[1,2], ZHANG Huan-guo[1], YANG Yang[1]
(1. *Key Laboratory of Space Information Security and Trusted Computing of Ministry of Education, Wuhan University, Wuhan, Hubei* 430072, *China*;
2. *Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, Beijing* 100080 *China*)

Abstract: The novel Hash algorithm whose security is based on the difficult of multivariate polynomial equations over a finite field is designed and implemented. We propose the idea of building a secure hash using higher degree multivariate polynomials as the compression function of MPH. The new algorithm compared with the current widespread use of the Hash algorithms has the following advantages: Security based on a recognized difficult problem of mathematics; Hash length can be free to change, according to the needs of the user; Hash function as a whole is Randomly selected; Design automation, users can be constructed to meet the actual needs of the specific Hash function. We analyze some security properties and potential feasibility, where the compression functions are randomly chosen 3rd polynomials, the experiment results show that the new algorithm has good properties in the efficiency and performance, and is comparable with other Hash functions.

Key words: cryptography; hash function; MQ problem; multivariate polynomials

1 引言

Hash 函数在数字签名[1]、消息认证[2]等现代信息安全技术中被广泛应用,它是一类特殊的单向函数,对于输入的任意长度消息序列,输出固定长度的 Hash 函数值(又称数字指纹).目前使用最广泛的 Hash 函数是 MD 系列和 SHA 系列,它们都是基于逻辑运算直接构造的,近年来对于这类 Hash 函数的研究取得了重大突破,MD5 已不安全[3],虽然还未找到 SHA-1 的碰撞,但其计算复杂度已经约减到 2^{63} 次[4].美国国家标准和技术研究所在 2005 年 10 月和 2006 年 8 月举办了两次研讨会,评估了当前 Hash 函数的使用状况,决定公开征集新的 Hash 函数标准 SHA-3[5].预计这一计划将在 2012 年完成.文献[3,4]的分析结果使人们对直接采用大量逻辑运算构造方法本身的安全性产生了严重质疑,设计新的高安全度的 Hash 函数已迫在眉睫.鉴于此,本文基于非线性多变元多项式方程组的难解性构造了一种新的 Hash 函数.

2 多变元 Hash 函数的构造

2.1 MQ 问题与 Hash 函数

有限域 F_q 上 n 个变元的二次多项式形式为:

$$p_i(x_1,\cdots,x_n)=\sum_{1\leqslant j\leqslant k\leqslant n}a_{i,j,k}x_jx_k+\sum_{1\leqslant j\leqslant n}b_{i,j}x_j+c_i$$

其中 $1\leqslant i\leqslant m$, $a_{i,j,k}, b_{i,j}, c_i\in F_q$.

定义 1 随机给定一个 F_q 上 n 个变量的二次方程组 $P=(p_1,\cdots,p_m)$, $m\leqslant n$.对于已知元素 $y\in F_q^m$,求解一个元素 $x\in F_q^n$,使得 $y=(p_1(x),\cdots,p_m(x))$,称为 MQ 问题.

收稿日期:2009-07-08;修回日期:2010-01-18
基金项目:国家自然科学基金(No.60673071,No.60970115);中国科学院数学机械化重点实验室开放课题(No.KLMM0903);武汉理工大学自主创新研究基金(No.2010-Ia-058)

定理 1[6] MQ 问题是一个 NP 难解性问题.

当上述方程组的次数大于 2 时,它的求解问题仍然是一个 NP 难解性问题[7].

直接利用 MQ 问题构造多变元 Hash 函数是不安全的,不能抵御多变元差分攻击[7,8].因此本文我们采用有限域上高次(最高项次数大于 2)多变元多项式方程组来构造新 Hash 函数的压缩函数,并将这种新的多变元 Hash 函数称之为 MPH(Multivariate Polynomails for Hash).为了便于叙述,文中仅以有限域上的三次多项式为例讨论 MPH 的安全性、效率及其具体构造方法.

2.2 MPH 的结构

定义 2 MPH 的压缩函数 $CF(x)$ 为

$$CF: F_q^{2n} \to F_q^n, CF(x) = (f_1(x_1,\cdots,x_{2n}),\cdots,f_n(x_1,\cdots,x_{2n}))$$

其中,$x=(x_1,\cdots,x_{2n})\in F_q^{2n}$,$f_i$ 是在有限域 F_q 上随机选择的三次多项式,其形式如下:

$$f_i(x) = \sum a_{i,j,k,t}x_jx_kx_t + \sum b_{i,j,k}x_jx_k + \sum c_{i,j}x_j + d_i \quad (1)$$

其中,$1\leqslant i\leqslant n$,$a_{i,j,k,t}, b_{i,j,k}, c_{i,j}, d_i\in F_q$,$q=2^b$,$b\in Z^+$.

压缩函数 $CF(x)$ 多项式方程组的项数最大约为 $2n^2(2n^2+6n+7)/3$,其中方程组的三次项个数为 $2n^2(n+1)(2n+1)/3$,二次项的个数为 $2n^3+n^2$,一次项的个数为 $2n^2$,常数项的个数为 n.

我们仍采用目前通用的 Merkle-Damgård[9,10]结构来构造 Hash 函数 MPH(如图 1).以 $x\in F_{256}^{32}$ 为例,Hash 值长度为 256bit,压缩函数 $CF(x)$ 大约需要 1.5M 字节存储空间,效率也很低,缺乏实用性.因此,本文新 Hash 函数的压缩函数将采用如下随机稀疏多项式:

$$f_i(x) = \sum_S a_{i,k,t,v}x_kx_tx_v + \sum_{1\leqslant j\leqslant n} b_{i,j}x_jx_{(2n+2-i-j)\bmod(2n)} + \sum_{1\leqslant j\leqslant 2n} c_{i,j}x_j + d_i \quad (2)$$

其中 $1\leqslant i\leqslant n$,系数 $a_{i,k,t,v}, b_{i,j}, c_{i,j}, d_i\in F_q$ 均为随机选取,三次项 $x_kx_tx_v$ 也是随机选取(随机选取下标 $k,t,v\in[1,2n]$即可);每个多项式 f_i 中二次项共 n 项.

构造形如式(2)的稀疏多项式代替式(1)作为 MPH 的压缩函数,主要是用于提高其实现效率,这也是 MQ 密码系统中用于提高效率的常用手段,其安全性将在第 3 节中详细讨论.

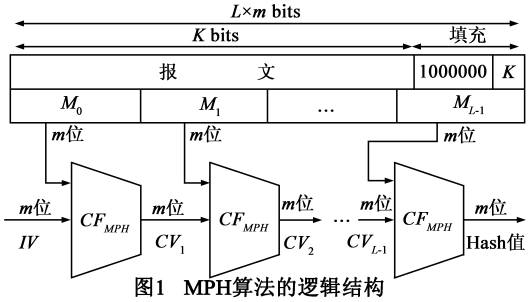

图1 MPH算法的逻辑结构

算法 1 MPH 算法

输入:任意报文 M.MPH 的基本域为 F_q,$q=2^k$.

输出:m 位 Hash 值 $H(M)$.

Step1.填充报文.数据填充方式与 SHA 类似(如图 1).填充后的报文分组为 $M_0,\cdots,M_{L-1}$,其中 M_i 的长度为 m 位,$m=nk$.再将每个分组 M_i 编码为基本域上一个 n 维向量;

Step2.初始化 n 维向量 IV;

Step3.执行算法主循环;

$CV_0=$ IV;

for ($i=1; i\leqslant L; i++$)

$CV_i = \mathrm{CF}(CV_{i-1}\|M_{i-1})$;

$H(M)=CV_L$;

Step4.返回 m 位 Hash 值 $H(M)$.

算法 1 给出了新 Hash 算法的具体实现方法,这里 $\|$ 表示将有限域上的两个 n 维向量级联成一个 $2n$ 维向量,即 $CV_i\|M_i\in F_q^{2n}$.

3 安全性分析

定理 2 假设构造 MPH 的压缩函数 CF 是在有限域 F_q 上随机选择的三次多项式,则有:对于给定一个消息摘要 z,找到一个消息 x,满足 $z=CF(x)$ 是不可计算的,即抗原像攻击;CF 是抗第二原像攻击的;CF 是抗碰撞攻击的.

证明 抗原像攻击.由于 $z=CF(x)$ 为 n 个方程 $2n$ 个变元的不定方程组,对于有限域上的一般性不定方程组,目前还没有一种确切的算法,求解复杂度约等于穷搜的复杂度 $O(q^n)$,其中 n 为方程的个数,q 为有限域的阶,这也是多变量公钥密码采用"减模式"方法能增加安全性的一个重要原因[6];抗第二原像及抗碰撞攻击.由于前者包含于后者,只需证明抗碰撞攻击即可,假设碰撞差分为 $\Delta x\in F_q^{2n}$,寻找压缩函数 $CF(x)$ 的碰撞等价于解方程 $CF(x+\Delta x)-CF(x)=0$,只要 Δx 不为零,根据定义 1 和定理 1 上述求解过程为 MQ 问题,是不可计算的. 证毕

下面我们讨论压缩函数 $CF(x)$ 取形如式(2)稀疏多项式的情形.代数攻击方法的提出,使得很多密码体制都可以转化为 MQ 问题(如 AES).因此近年来 MQ 问题受到了广泛关注,并提出了一些求解算法,但效率均不理想.如构造 Gröbner 基的 Buchberger 算法及其变型 $F4$、$F5$ 算法[11]、XL 系列算法[12]等,但这些算法对多项式的稀疏程度并不敏感[7].文献[13~15]中指出如果 MQ 是稀疏的,且具有一个规则的结构,那么问题就很容易解决,但对于一般的稀疏 MQ 问题并不十分有效.文献[16]定义了一个新的分组密码 BES,只使用 $GF(2^8)$ 上的简单代数结构,并且与 AES 有相同的信息空间和密钥空间,由此得到的一个重要结果是:AES-128加

密体制可以描述成一个 $GF(2^8)$上的非常稀疏的超定多变元二次方程组,其中方程数量 5248 个(二次方程 3840 个,线性方程 1408 个),3968 个变元,组成非零项 7808 个,它的解就是 AES 的密钥,上述方程理论项数大约为 2^{35},可见其代数表达式的稀疏程度,目前代数攻击 AES-128 最好的复杂度超过 2^{200},大大超过穷尽搜索密钥的复杂度.从目前的研究进展来看,域 $F_q(q>2)$上随机稀疏 MQ 问题仍然是难解的,这也是本文多变元 Hash 函数 MPH 结构安全性的理论依据.因此我们认为定理 2 中的压缩函数为随机选择的稀疏方程时结论仍然成立.不过选择时应该谨慎,尽量避免文献[13~15]中具有特殊规则的稀疏多项式方程,以及根据实际需求折中考虑压缩函数的稀疏度和实现效率.

定理 2 表明压缩函数 CF 满足安全 Hash 函数的三个性质,即抗原像攻击、抗第二原像攻击及抗碰撞攻击[10].通过 Merkle 级联算法构造新的多变元 Hash 函数 MPH 也具有上述性质[9,10].

4　仿真实验及性能评估

4.1　MPH 的效率分析

本文新 Hash 函数 MPH 的基本域 F_q 一般取 $q=2^8$,压缩过程中主要运算为 F_q 上的乘法运算和加法运算,因此实现效率较高,也易于硬件实现.由于基本域 F_q 较小,因此可预运算并存储其乘法表,与 AES 相仿乘法运算可通过查表完成.压缩函数式中一个 n 次项需要 n 次查表运算,从而新 Hash 函数的效率主要取决于其压缩函数的项数,项数越少效率越高,同时,当压缩函数的项数一定时,高次项的比重越小,其运算效率越高.本文实验环境为 Inter Core2 P8600 2.4GHz CPU、2G 内存 PC,随机选择形如式(2)的多项式组作为 MPH 的压缩函数,表 1 给出了 MPH-k 系列与安全 Hash 函数 SHA-k 系列(k 表示 Hash 函数的输出值长度)相应长度效率比较的测试结果,*Terms* 表示多变元 Hash 函数的压缩函数中每个方程的三次项数,效率单位:MB/sec.

表 1　$GF(256)$上 MPH 与 SHA 系列的效率比较

Terms	MPH over GF(256)			
	MPH-160	MPH-256	MPH-384	MPH-512
10	7.832	7.446	7.365	7.011
60	1.457	1.310	1.237	1.192
100	0.811	0.751	0.731	0.725
500	0.156	0.153	0.147	0.136
SHA	14.418	13.061	6.924	6.519

如表 1 所示,MPH 的实现效率主要取决于压缩函数的三次项数,当 $Terms\approx 10$ 时 MPH 与 SHA 的效率大致相仿,当 $Terms\approx 100$ 时 MPH 效率大约只有 SHA 的十分之一.其原因为 MPH 的效率主要取决于基本域上的乘法查表运算,d 次多变元多项式每一项最多需要 d 次查表运算,假设 MPH 压缩函数的方程个数为 n,则 MPH 的每轮压缩运算共需查表次数为 $d\times n\times Terms$,因此 MPH 的效率与其压缩函数的项数大致为线性关系.

4.2　MPH 的存储空间

MPH 的存储包括两个部分:基本域上的乘法表和压缩函数.乘法表的大小取决于基本域 F_q,压缩函数的存储大小与方程的个数 n、方程的次数 d 及其每个方程的项数 *Terms* 有关.MPH 的存储空间 S(单位:bit)可表示为

$$S(n,q,d,Terms)=[n(\log_2^q+d\log_2^{2n})Terms+(2n^3+n^2)\log_2^q]+(q-1)^2\cdot\log_2^q$$

图 2 给出了 $GF(2^8)$上 MPH 系列存储空间与压缩函数项数之间的关系.

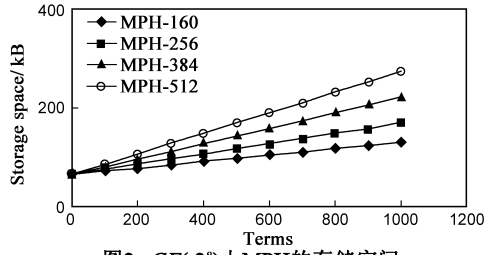

图2　$GF(2^8)$上MPH的存储空间

4.3　随机性统计分析

对于一个密码算法来说,其输出序列的随机性是其安全性的很重要的一方面.Hash 函数将任意长度的消息比特序列压缩为某一固定长度的摘要,就安全性而言,摘要应该具有良好的随机性.文献[17]中给出了随机数的五种基本测试方法.

4.3.1　频数检测(Frequency Test)

频数检测用来检验一个比特序列中 0、1 个数的平衡性.对于一个好的 n 比特序列,当其长度充分大时(一般大于 100),若令 n_1 表示序列中 0 或 1 的个数,则统计量 V 应该符合标准正态分布,其中

$$V=2\sqrt{n}\left(\frac{n_1}{n}-\frac{1}{2}\right)$$

4.3.2　双比特检测(Two-bit Test)

双比特测试的目的是判定一个序列中子序列 00、01、10、11 所出现的次数是否近似相等.令 n_0、n_1、n_{00}、n_{01}、n_{10}、n_{11}分别表示 n 位序列中 0、1、00、01、10、11 的个数,则当 n 不小于 21,统计量 V 应近似地服从自由度为 2 的 χ^2 分布,其中

$$V=\frac{4}{n-1}(n_{00}^2+n_{01}^2+n_{10}^2+n_{11}^2)-\frac{2}{n}(n_0^2+n_1^2)+1$$

4.3.3　游程检测(Runs Test)

游程是序列的一个字串,有连续的 0 或 1 组成,且其前导和后继的元素与其本身的元素不同.一个随机的 n 位序列中长度为 i 的游程的数目期望值为 $e_i=(n$

$-i+3)/2^{i+2}$. 令 k 是满足 $e_i \leqslant 5$ 的最大正整数 i, b_i、g_i 分别是一个比特流中长度为 i 的 0 游程和 1 游程的数目,则统计量 V 应近似地服从自由度为 $2k-2$ 的 χ^2 分布,其中

$$V = \sum_{i=1}^{k} \frac{(b_i - e_i)^2}{e_i} + \sum_{i=1}^{k} \frac{(g_i - e_i)^2}{e_i}$$

4.3.4 扑克检测(Poker Test)

对于任意的正整数 m,长度为 m 位的二进制序列有 2^m 种可能性.我们将待检测 n 位序列划分成 $k = \lfloor n/m \rfloor$ 个长度为 m 的非叠加的子序列,用 $n_i (1 \leqslant i \leqslant 2^m)$ 表示第 i 种子序列类型的个数.扑克检测用来检验这 2^m 种子序列类型的个数是否近似相等,则统计量 V 应近似地服从自由度为 $2^m - 1$ 的 χ^2 分布,其中

$$V = \frac{2^m}{k} \sum_{i=1}^{2^m} n_i^2 - k$$

待检序列长度 n 与子序列长度 m 之间应满足关系式 $\lfloor n/m \rfloor \geqslant 5 \times 2^m$.

4.3.5 自相关检测(Autocorrelation Test)

自相关检测用来检验待检序列与将其左移 d 位的序列的关联程度.一个随机的序列应该和将其左移任意位的序列都是独立的,故其关联程度也应该很低.

用 $A(d) = \sum_{i=0}^{n-d-1} (\kappa_i \oplus \kappa_{i+d})$ 表示待检序列与将其左移 d 位的序列之间不同的元素个数,则统计量 V 应服从标准正态分布,其中

$$V = \frac{2\left(A(d) - \frac{n-d}{2}\right)}{\sqrt{n-d}}$$

待检序列长度 n 与左移位数 d 之间应满足关系式 $1 \leqslant d \leqslant \lfloor n/2 \rfloor$ 和 $(n-d) > 10$.

表 2 $GF(2^8)$上 MPH-160 算法的摘要流随机性检测结果

检查项目	三次项项数					
	10	50	100	200	500	1000
频数	926	957	943	961	982	974
双比特	937	954	976	968	972	969
游程	945	921	976	965	983	976
扑克	980	978	985	977	982	987
自相关	941	963	965	970	973	968

目前存在的局部随机性测试方法不下百种,而且根据参数的改变一个检验有时可以变换为很多个检验,它们均可从不同的角度检验序列的随机性.要让一个算法通过所有的随机性检验是件很困难的事,但是有些基本的检验是必须要通过的,比如频数检验.本文仅对 MPH-160 做了最为常见的五种基本测试,其中扑克检验的子块长度为 4.

随机选取 1000 个 160 位的消息分组,分别对每个分组进行杂凑得到 1000 个 160 位的摘要分组,将摘要分组连接起来构成一个长为 1000×160 比特的检测样本序列,显著性水平为 0.05. 表 3 中第一行中的数据 10、50、…、1000 分别表示相应压缩函数的每个方程中三次项的项数.其它的检测数据,如频数一栏的第一个数据 917 表示:在压缩函数的每个方程中三次项的项数为 10 项的情形下,随机构造 1000 个 MPH-160 算法有 917 个通过频数测试,其它的类推.从表 2 的检测结果可以看出,MPH-160 算法具有良好的随机统计特性.

4.4 雪崩性质测试分析

为了隐藏明文消息的冗余度,Shannon 提出了混乱与散布的概念,加密体制中要求充分且均匀地利用密文空间,Hash 函数同样如此,要尽量做到相应消息串与对应的 Hash 值不相关,而对于结果的二进制表示,每 bit 只有 0 或 1 两种可能,因此理想 Hash 的散布效果应该是初值的细微变化将导致结果的每 bit 都以 50% 的概率变化.考察 Hash 算法在消息串发生 1bit 变化的情况下,引起 Hash 结果的变化比特数为 B.

定义 3 设平均变化比特数 $\bar{B}$、平均变化概率 P、B 的均方差 ΔB、P 的均方差 ΔP 分别为

$$\bar{B} = \frac{1}{N} \sum_{i=1}^{N} B_i, P = \frac{\bar{B}}{m} \times 100\%,$$

$$\Delta B = \sqrt{\frac{1}{N-1} \sum_{i=1}^{N} (B_i - \bar{B}_i)^2},$$

$$\Delta P = \sqrt{\frac{1}{N-1} \sum_{i=1}^{N} \left(\frac{B_i}{m} - P\right)^2},$$

其中 N 为统计次数,B_i 为第 i 次测试变化的比特数,m 为 Hash 值的长度.

每次测试方法为在消息空间中随机选取一段消息进行新的 Hash 函数压缩,然后改变消息串 1bit 得到另一 Hash 结果,比较两个结果得到变化的比特数为 B_i.限于篇幅,本文仅以 $GF(2^8)$上的 MPH-160 为例,其中统计次数 $N = 1000$.

表 3 $GF(2^8)$上 MPH-160 的性能测试

Terms	$\bar{B}$	ΔB	$P/\%$	ΔP
10	73.97	1.62	46.23	0.19
50	75.92	1.31	47.44	0.14
100	76.74	0.96	48.37	0.05
200	78.46	1.15	49.28	0.06

由表 3 可知,MPH-160 算法的 $\bar{B}$ 和 P 非常接近理想状况下 80 和 50% 的变化概率,相当充分均匀地利用了消息空间,消息的任何扰动,都使得 Hash 结果在统计上产生接近等概率的均匀分布,从统计效果上看,保证了攻击者在已知一些消息 Hash 值对的情况下无法得到任何 Hash 值分布的有用信息.而 ΔB 与 ΔP 越接近于零,则表明算法对消息的混淆与扩散性质的稳定性越好,表 3 显示 MPH 算法具有良好的雪崩性质.

5 结论及进一步工作

本文提出了一种基于有限域上非线性方程组难解性问题的新 Hash 函数算法,与目前广泛使用的 Hash 算法如 SHA 系列相比具有下列特点:安全性基于一个公认的数学难题(MQ 问题),碰撞分析等价于解有限域上的非线性方程组,为提高算法效率,我们对压缩函数做了稀疏化处理,稀疏度对 MQ 问题求解难度的影响仍是一个开放难题;Hash 函数的输出长度可变;引入了整体随机性,即压缩函数是随机的,从而导致整个 Hash 算法具有随机性;设计自动化,设置安全性、性能等控制参数结合文献[18,19]中将智能算法应用到密码设计的思想,根据用户的实际需求自动产生满足其特定要求的多变元 Hash 函数.另外,新算法的基本域也可以取大域如 $GF(2^{16})$等,但此时有限域上的乘法需要采用其他专用算法,一般推荐使用 $GF(2^8)$,结合 MQ 公钥密码[6]的实践经验,压缩函数每个方程项数一般取 50 ~ 1000 为宜,假如在安全性要求相对较低的领域如低廉智能卡上使用,压缩函数的项数还可取得更为稀疏.本文是对多变元 Hash 函数构造的初探,许多问题如域参数的选取、压缩函数的稀疏程度与安全性之间的定量分析、选用其它的结构(如 HAIFA)、并行化实现以及构造可证明安全的多变元 Hash 函数等是我们下一步的研究工作.

参考文献:

[1] 辛向军,李刚,等.一个高效的随机化的可验证加密签名方案[J].电子学报,2008,36(10):1378 – 1382.
Xin Xiangjun, Li Gang, et al. An efficient randomized verfiably encrypted signature scheme[J]. Acta Electronica Sinica, 2008, 36(10):1378 – 1382. (in Chinese)

[2] 马文平,王新梅.多发送认证码的几个新的构造方法[J].电子学报,2000,28(4):117 – 119.
Ma Wenping, Wang Xinmei. Several new constructions on multitransmitters authentication codes[J]. Acta Electronica Sinica, 2000, 28(4):117 – 119. (in Chinese)

[3] X Wang, H Yu. How to break MD5 and other hash functions [A]. In Advances in Cryptology-EUROCRYPT[C]. Springer-Verlag, 2005. 19 – 35.

[4] X Wang, A Yao, F Yao. Cryptanalysis of SHA-1 Hash Function [R]. Cryptographic Hash Workshop, Invited Report, 2005.

[5] NIST. Plan for new cryptographic hash functions[OL]. http://www.nist.gov/hash-function/, 2006.

[6] J Ding. Multivariate Public Key Cryptosystems[M]. Springer-Verlag, 2006. 11 – 190.

[7] J Ding, B Y Yang. Multivariates polynomials for hashing[A]. Information Security and Cryptology (Inscrypt), Lecture Notes in Computer Seience[C]. Vol. 4990, 2007. 358 – 371.

[8] P A Fouque, L Granboulan, J Stern. Differential cryptanalysis for multivariate schemes[A]. In Eurocrypt, LNCS 3494[C]. Springer-Verlag, 2005. 341 – 353.

[9] R C Merkel. A fast software one-way Hash function[J]. Journal of Cryptology, 1990, 3:43 – 58.

[10] Damgard I B. A design principle for Hash functions[A]. Advances in Cryptology-Crypto[C]. Spring-Verlag, 1990. 416 – 427.

[11] J C Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero(F5)[A]. ISSAC2002[C]. ACM Press, 2002. 75 – 83.

[12] Adi Shamir, Jacques Patarin, Nicolas Courtois, Alexander Klimov. Efficient algorithms for solving overdefined systems of multivariate polynomial equation[A]. Eurocrypt 2000, LNCS1807[C]. Springer, 2000. 392 – 407.

[13] 唐樺瑾,冯勇. Dixon 结式在密码学中的应用[J].软件学报. 2007, 18(7):1738 – 1745.

[14] Raddum, Semaev. New technique for solving sparse equation systems[A]. Cryptology ePrint Archive[C]. Report 2006/475.

[15] G V Bard, N T Courtois, C Jefferson. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over GF(2) via SAT-solvers[A]. Cryptology ePrint Archive[C]. Report 2007/024, 2007.

[16] Sean Murphy, Matthew J B Robshaw. Essential algebraic structure within the AES[A]. CRYPTO2002[C]. 2002. 1 – 16.

[17] 胡磊,王鹏.应用密码学手册[M].北京:电子工业出版社,2005. 158 – 166.

[18] 孟庆树,张焕国,王张宜. Bent 函数的演化设计[J].电子学报,2004,32(11):1901 – 1903.
Meng Qingshu, Zhang Huanguo, Wang Zhangyi. Designing bent functions using evolving method[J]. Acta Electronica Sinica, 2004, 32(11):1901 – 1903. (in Chinese)

[19] 张焕国,冯秀涛,覃中平,刘玉珍.演化密码与 DES 的演化研究[J].计算机学报,2003,26(12):1678 – 1684.

作者简介:

王后珍　男,1981 年生于湖北建始.武汉大学计算机博士研究生.研究方向为信息安全、信息编码等.
E-mail:wanghouzhen@126.com

张焕国　男,1945 年出生于河北元氏,武汉大学教授,博士生导师,担任中国密码学会理事,中国计算机学会容错专业委员会副主任,创建了全国第一个信息安全本科专业,发表论文 100 多篇,出版著作 6 部,主要研究领域包括:演化密码、可信计算、纠错编码、云计算、智能卡、网络安全等.