基于反交换拟群的消息认证码 *

李伟强 徐允庆

(宁波大学理学院, 宁波 315211)

(E-mail: xuyunqing@nbu.edu.cn)

摘 要 $(Q,\circ)$ 是一个拟群。如果对 $(Q,\circ)$ 中任何两个不同元素 x, y 皆有 $x\circ y\neq y\circ x$, 则称 $(Q,\circ)$ 是反交换的. 本文给出一种基于反交换拟群的消息认证码, 并讨论反交换拟群的构造方法.

关键词 拟群; 拉丁方; 消息认证码

MR(2000) 主题分类 05B15; 94A62

中图分类 O157.2; TP309.7

1 引言

消息认证码 (Message Authentication Code 或简称 MAC) 是用来保证数据完整性的一种工具. 数据完整性是信息安全的一项基本要求, 可以防止数据未经授权被篡改. 随着网络技术的不断进步, 尤其是电子商务的不断发展, 保护信息的完整性变得越来越重要. 特别是双方在一个不安全的信道通讯的时候, 就需要有一种方法能够防止数据未经授权而被篡改. 消息认证码就能够达到这一目的, 其方法是: 通信双方 (如 Alice 和 Bob) 共享一个密钥 k. 当 Alice 要向 Bob 发送消息时, 她将计算该消息的 MAC, MAC 作为消息 M 和密钥 k 的一个函数值: MAC=$h_k(M)$, 然后将 M 与 MAC 一起发给 Bob. 使用相同的密钥, Bob 对收到的 M 执行相同的计算并得到 MAC. 将收到的 MAC 与计算得到的 MAC 进行比较, 如果二者相等, 则可判断: (1) 接收者确信消息未被更改过; (2) 接收者确信来自声称的发送者.

将组合设计应用于密码学是近些年来组合数学的一个发展方向. Denes 和 Keedwell[1] 较早地讨论了利用拟群构造消息认证码, Dawson 和 Donovan[2] 对这个认证码系统的安全性进行了分析. Meyer[3] 构造了一种基于拟群不满足结合律的消息认证码. 本文将讨论基于反交换拟群的消息认证码, 并讨论了构造反交换拟群的存在谱及构造方法. 本文涉及到的哈希函数的有关性质可参阅 [4–6]; 拟群的有关性质可参阅 [7, 8].

定义 1.1 哈希函数 h 是字符串集合 D 到字符串集合 R 的映射, 具有下列性质:

(1) 压缩: 字符串 $x\in D$ 任意长, $h(x)\in R$ 固定长;

(2) 容易计算: 向哈希函数 h 输入 x, 容易计算 $h(x)$;

(3) 单向性: 基本上对所有事先指定的 $y\in R$, 可以找到 $x\in D$, 使 $h(x)=y$ 在计算上是困难的;

(4) 弱抗碰撞: 已知 x, 找 $x'\neq x$, 使 $h(x)=h(x')$ 在计算上是困难的;

(5) 强抗碰撞: 找任何两个不同的输入 x, x', 使 $h(x)=h(x')$ 在计算上是困难的.

本文 2008 年 7 月 9 日收到. 2008 年 9 月 2 日收到修改稿.

* 国家自然科学基金 (60873267), 浙江省自然科学基金 (Y607026) 和宁波市自然科学基金 (2006A610094) 资助项目.

定义 1.2 消息认证码是一个带密钥的哈希函数 h_k, 其中 k 是密钥, 且有以下特点:

1) 给定密钥 k, $h_k(x)$ 容易计算. $h_k(x)$ 称为消息 x 的认证标记.

2) 给定 m 个输入输出 $(x_i, h_k(x_i))$, $i \in [1,m]$, $\forall x' \notin \{x_1, x_2, \ldots, x_m\}$, 在不知道密钥 k 时, 计算 $h_k(x')$ 是困难的.

定义 1.3 $(Q,\circ)$ 是一个广群, 若 $\forall a,b \in Q$, 方程 $x \circ a = b$ 和 $a \circ y = b$ 在 Q 上有唯一解, 则称 $(Q,\circ)$ 是一个拟群. 集合 Q 的基数 $|Q|$ 称为拟群 $(Q,\circ)$ 的阶数.

一个 n 阶拉丁方是一个由 n 个元素构成的 $n \times n$ 矩阵, 每个元素在矩阵的每一行、每一列中恰好出现一次. 一个拟群的乘法表就是一个拉丁方, 反之, 一个拉丁方可定义一个拟群. 所以拟群与拉丁方是相互等价的.

定义 1.4 一个 n 阶拉丁方的一个截态是位于该拉丁方的不同行不同列的 n 个位置, 且此 n 个位置的元素两两互异.

定义 1.5 称拟群 $(Q,\circ)$ 为反交换的, 如果 $\forall a,b \in Q$, $a \neq b$, 有 $a \circ b \neq b \circ a$. 与反交换拟群等价的拉丁方称为反对称拉丁方.

2 基于反交换拟群的消息认证码

本节介绍基于反交换拟群的认证码系统.

设 $(Q,\circ)$ 为一个反交换拟群, 消息 $M = m_1 m_2 \cdots m_{s+1}$, 其中 $m_i \in Q$ $(i = 1,2,\cdots,s+1)$. 先对 M 作如下处理:

$$\begin{cases} u_1 = m_1 \circ m_2, \\ u_i = u_{i-1} \circ m_{i+1}, \qquad i = 2,3,\cdots,s, \end{cases}$$

得到字符串 $u_1 u_2 \cdots u_s$. 再令 $m'_1 = u_s$, $m'_2 = u_{s-1}$, $\cdots$, $m'_s = u_1$ 得到字符串 $M' = m'_1 m'_2 \cdots m'_s$. 容易看出, 如果 $m = m_1 m_2 \cdots m_s$ 的第 i 位 m_i 被篡改为 x_i $(\neq m_i)$, 则 u_i, u_{i+1}, $\cdots$, u_s 将全部改变, 由此带来 m'_1, m'_2, $\cdots$, m'_{s-i+1} 的全部改变.

设 $s = t \cdot \ell$ 即 $M' = m'_1 m'_2 \cdots m'_{t\ell}$, 其中 $m'_i \in Q$, $i = 1,2,\cdots,t\ell$. 必要时在 M' 的后面进行扩充使其长度为 t 的倍数. 将 M' 划分为长是 t 的 ℓ 个段: $M' = M'_1 \parallel M'_2 \parallel \cdots \parallel M'_\ell$, 其中 $M'_{i+1} = m'_{it+1} m'_{it+2} \cdots m'_{it+t}$, $i = 0,1,\cdots,\ell-1$.

设 $K = k_1 k_2 \cdots k_{(t-1)\ell}$ 是由一个伪随机序列生成器 [9] 产生的长为 $(t-1)\ell$ 二进制密钥序列. 将密钥序列 K 划分为 ℓ 个长 $t-1$ 的段: $K = K_1 \parallel K_2 \parallel \cdots \parallel K_\ell$, 其中 $K_{i+1} = k_{i(t-1)+1} k_{i(t-1)+2} \cdots k_{i(t-1)+t-1}$, $i = 0,1,\cdots,\ell-1$. 然后进行以下计算:

$$\begin{cases} x_{i1} = m'_{it+1} \otimes_{k_{it+1}} m'_{it+2}, \\ x_{ij} = x_{i(j-1)} \otimes_{k_{it+j}} m'_{it+j+1}, \quad j = 2,3,\cdots,t-1, \quad i = 0,1,\cdots,\ell-1 \end{cases}$$

其中

$$x \otimes_{k_r} y = \begin{cases} y \circ x, & \text{当 } k_r = 1, \\ x \circ y, & \text{当 } k_r = 0. \end{cases}$$

令 $h_{i+1}(M'_{i+1}) = x_{i(t-1)}$ $(i = 0,1,\cdots,\ell-1)$ 作为 M'_{i+1} 的认证标识, 并将

$$\begin{aligned} H_K(M) =& h_{K_1}(M'_1) \parallel h_{K_2}(M'_2) \parallel \cdots \parallel h_{K_\ell}(M'_\ell) \\ =& x_{0(t-1)} \parallel x_{1(t-1)} \parallel \cdots \parallel x_{(\ell-1)(t-1)} \end{aligned}$$

作为 M 的认证标识. 该认证码系统的密钥是产生二进制密钥序列 K 的伪随机序列生成器的初始密钥 K_0.

由上面的讨论可以看出，消息 M 的任何一位被篡改，都至少要导致 u_s, 即 m_1' 的变化，从而导致 $H_k(M)$ 的全部改变 (雪崩效应).

例 令 $Q=\{0,1,2,\cdots,7\}$, 反交换拟群 $(Q,\circ)$ 的二元运算 "$\circ$" 定义如下表所示：

$\circ$	0	1	2	3	4	5	6	7
0	2	7	1	3	6	0	5	4
1	4	1	7	6	3	5	0	2
2	0	6	3	1	7	2	4	5
3	6	0	5	4	2	7	1	3
4	1	4	2	0	5	3	6	7
5	7	2	4	5	0	6	3	1
6	3	5	0	2	4	1	7	6
7	5	3	6	7	1	4	2	0

假定消息 $M=14627714530327472 6124$, 则

$$u_1=1\circ 4=3,\qquad u_2=3\circ 6=1,\qquad u_3=1\circ 2=7,\qquad \cdots,\qquad u_{20}=1\circ 4=3,$$
$$M'=u_{20}\cdots u_3u_2u_1=31035331530265440713.$$

令 $t=5,\ \ell=4$, 则

$$M'=31035\parallel 33153\parallel 02654\parallel 40713.$$

设密钥序列 $K=1001\parallel 0101\parallel 0101\parallel 0001$, 则

$$\begin{aligned}x_{01}&=3\otimes_1 1=1\circ 3=6,\\ x_{02}&=6\otimes_0 0=6\circ 0=3,\\ x_{03}&=3\otimes_0 3=3\circ 3=4,\\ x_{04}&=4\otimes_1 5=5\circ 4=0.\end{aligned}$$

同样的方法可算得 $x_{14}=3, x_{24}=6, x_{34}=1$. 所以消息 M 的认证标识 $H(M)=0361$.

3　反交换拟群的构造

在前面介绍的基于反交换拟群的消息认证码 (MAC) 中，虽然拟群 $(Q,\circ)$ 不需要保密，但为了确保消息认证码 (MAC) 的安全性，必须构造阶数较大的拟群，且最好拟群对应的拉丁方主对角线上的元素互不相同.

引理 3.1 当 $n\geq 5$ 为奇数且 $3\not| n$ 时，存在 n 阶反交换拟群且该拟群有 n 个截态，其中之一在主对角线上.

证　当 $n=5$ 时，存在 5 阶反交换拟群 $(Q,*)$ 且该拟群有 5 个截态，其中之一在主对角线上. 如下表：

$*$	0	1	2	3	4
0	0	2	4	1	3
1	4	1	3	0	2
2	3	0	2	4	1
3	2	4	1	3	0
4	1	3	0	2	4

当 $n=7$ 时，存在 7 阶反交换拟群 $(Q,*)$ 且该拟群有 7 个截态，其中之一在主对角线上．如下表：

$*$	0	1	2	3	4	5	6
0	0	2	4	6	1	3	5
1	4	6	1	3	5	0	2
2	1	3	5	0	2	4	6
3	5	0	2	4	6	1	3
4	2	4	6	1	3	5	0
5	6	1	3	5	0	2	4
6	3	5	0	2	4	6	1

当 $n\geq 9$ 为奇数且 $3\nmid n$ 时，考虑剩余类环 $(Z_n,+,\cdot)$．取 $p=\lfloor\log_2 n\rfloor\geq 3$, 则 $2^p<n<2^{p+1}$. 取 $k=2^r$, $\ell=2^{r+1}(1\leq r\leq p-2)$, 则 k, ℓ, $k-\ell$, $k+\ell\in Z_n$ 且它们都与 n 互素．

在 Z_n 上定义二元运算“$*$”如下：$x*y\equiv k\cdot x+\ell\cdot y\pmod n,\ \forall x,\ y\in Z_n$.

首先证明 $(Z_n,*)$ 是拟群．考虑 $(Z_n,*)$ 第 x_0 行的元素．由 $x_0*y\equiv k\cdot x_0+\ell\cdot y\pmod n$, x_0, $y\in Z_n$ 可知第 x_0 行元素互不相同．若不然，设 $(Z_n,*)$ 在位置 (x_0,s) 和 (x_0,t) 上的元素相同，其中 $s,t\in Z_n$, $s\neq t$. 由 $x_0*s\equiv k\cdot x_0+s\cdot\ell\pmod n$, $x_0*t\equiv k\cdot x_0+t\cdot\ell\pmod n$ 和 $x_0*s\equiv x_0*t\pmod n$, 可得 $(s-t)\cdot\ell\equiv 0\pmod n$. 又 ℓ 可逆，所以 $s=t$, 矛盾．同理可证 $(Z_n,*)$ 每一列的元素也互不相同．所以 $(Z_n,*)$ 是拟群．

其次证明拟群 $(Z_n,*)$ 是反交换的．即 $\forall x,y\in Z_n$, $x\neq y$, 必有 $x*y\neq y*x\pmod n$. 若不然，由 $x*y\equiv k\cdot x+\ell\cdot y\pmod n$, $y*x\equiv k\cdot y+\ell\cdot x\pmod n$ 和 $x*y\neq y*x\pmod n$, 可得 $(k-\ell)\cdot(x-y)\equiv 0\pmod n$. 又 $k-\ell$ 可逆，所以 $x=y$, 矛盾．

最后证明拟群 $(Z_n,*)$ 有 n 个截态．考虑乘法表中 n 个位置 $(0,x)$, $(1,x+1)$, $(2,x+2)$, $\cdots$, $(n-1,x+n-1)$, 其中 $x\in Z_n$, 加法“+”为 mod n 加法．若这 n 个位置上的元素出现重复，设拟群 $(Z_n,*)$ 在位置 $(s,x+s)$ 和 $(t,x+t)$ 上的元素相同，其中 s, $t\in Z_n$, $s\neq t$. 由 $s*(x+s)\equiv k\cdot s+\ell\cdot(x+s)\pmod n$, $t*(x+t)\equiv k\cdot t+\ell\cdot(x+t)\pmod n$ 和 $s*(x+s)\equiv t*(x+t)\pmod n$, 可得 $(k+\ell)\cdot(s-t)\equiv 0\pmod n$. 又 $k+\ell$ 可逆，所以 $s=t$, 矛盾．所以位置集合 $T_x=\{(x,y),(x+1,y+1),(x+2,y+2),\cdots,(x+n-1,y+n-1)\}$ 构成拟群 $(Z_n,*)$ 的一个截态．x 取 $0,1,\cdots,n-1$ 可得 $(Z_n,*)$ 的 n 个截态．其中 T_0 在主对角线上．

引理 3.2 当 $n\geq 9$ 为奇数且 $3\mid n$ 时，存在 n 阶主对角线上元素互不相同的反交换拟群．

证 这时有 $3\nmid n-4$, 且 $n-4\geq 5$. 由引理 3.1 知，存在 $n-4$ 阶反交换拟群 $(Z_{n-4},\cdot)$ 且该拟群有 $n-4$ 个截态，其中之一在主对角线上．我们考虑利用拟群 $(Z_{n-4},\cdot)$ 构造 n 阶拟群 $(Q,\circ)$, 其中 $Q=Z_{n-4}\cup\{\infty_1,\infty_2,\infty_3,\infty_4\}$. 取拟群 $(Z_{n-4},\cdot)$ 中的 4 个截态 T_1, T_2, T_3, T_4, 且此 4 个截态不在拟群 $(Z_{n-4},\cdot)$ 的主对角线上．在集合 Q 上定义二元运算“$\circ$”如下：

(1) $\forall(x,y)\in T_i$, 定义 $x\circ\infty_i=\infty_i\circ y=x\cdot y$, $x\circ y=\infty_i$; $i=1,2,\cdots,4$.

(2)$\forall$ x, $y\in Z_{n-4}$, $(x,y)\notin T_k$, $1\leq k\leq 4$, 定义 $x\circ y=x\cdot y$, $0\leq x,y\leq n-5$.

(3) $\forall x,y\in\{\infty_1,\infty_2,\infty_3,\infty_4\}$, 其运算可根据引理 3.4 中的 4 阶拟群来定义．

容易验证拟群 $(Q,\circ)$ 为主对角线上元素互不相同的反交换拟群．

定义 1.6 设 A, B 分别为集合 X 和 X' 上的 m 阶和 n 阶拉丁方，记

$$A \times B = \begin{pmatrix} c(1,1) & c(1,2) & \cdots & c(1,n) \\ c(2,1) & c(2,2) & \cdots & c(2,n) \\ \cdots & \cdots & & \cdots \\ c(n,1) & c(n,2) & \cdots & c(n,n) \end{pmatrix},$$

其中 $c(x,y) = \Big((a_{i,j}, b_{x,y})\Big)_{m\times m}$ $(1 \le x, y \le n)$. 称 mn 阶拉丁方 $A \times B$ 为集合 $X \times X'$ 上的拉丁方 A 与拉丁方 B 的积复合拉丁方.

引理 3.3 若 A 和 B 分别是 m 阶和 n 阶反对称拉丁方，则 $A \times B$ 是 mn 阶的反对称拉丁方.

证　由定义 1.6 知，$A \times B$ 是 mn 阶的拉丁方.

下面证明 $A \times B$ 是反对称拉丁方. 首先由拉丁方 A 的反对称性可知 $c(x,x)$ 的反对称性. 其次考虑 $c(x,y)$ 和 $c(y,x)$ 中对称位置上的元素，其中 $x \ne y$. $c(x,y)$ 中位置 (i,j) 上的元素为 (a_{ij}, b_{xy}), $c(y,x)$ 中位置 (j,i) 上的为 (a_{ji}, b_{yx}). 由 B 的反对称性可知 $(a_{ij}, b_{xy}) \ne (a_{ji}, b_{yx})$. 所以 $A \times B$ 是 mn 阶的反对称拉丁方. 证毕.

引理 3.4 当 $n \ge 4$ 为素数幂时，存在 n 阶主对角线上元素互不相同的反交换拟群.

证　当 $n \ge 4$ 为素数幂时，考虑有限域 $(F_n, +, \cdot)$. 令 $F_n = \{a_0 = 0, a_1, a_2, \ldots, a_{n-1}\}$. 取 $a_k, a_\ell \in F_n^* = F_n \setminus \{0\}$, 使得 $a_k \ne a_\ell$，$a_k \ne -a_\ell$.

在 F_n 上定义二元运算 “$*$” 如下：$a_x * a_y = a_k a_x + a_\ell a_y$，$\forall a_x$，$a_y \in F_n$.

首先证明 $(F_n, *)$ 是拟群. 考虑 $(F_n, *)$ 第 x_0 行的元素. 由 $a_{x_0} * a_y = a_k a_{x_0} + a_\ell a_y$，$a_{x_0}$, $a_y \in F_n$ 可知第 x_0 行元素互不相同. 若不然，设 $(F_n, *)$ 在位置 (a_{x_0}, a_s) 和 (a_{x_0}, a_t) 上的元素相同，其中 $a_s, a_t \in F_n$，$a_s \ne a_t$. 由 $a_{x_0} * a_s = a_k a_{x_0} + a_\ell a_s$，$a_{x_0} * a_t = a_k a_{x_0} + a_\ell a_t$ 和 $a_{x_0} * a_s = a_{x_0} * a_t$, 可得 $(a_s - a_t)a_\ell = 0$. 又 a_ℓ 可逆，所以 $a_s = a_t$, 矛盾. 同理可证 $(F_n, *)$ 每一列的元素也互不相同. 所以 $(F_n, *)$ 是拟群.

其次证明拟群 $(F_n, *)$ 是反交换的，即 $\forall a_x, a_y \in F_n$，$a_x \ne a_y$, $a_x * a_y \ne a_y * a_x$. 若不然，由 $a_x * a_y = a_k a_x + a_\ell a_y$，$a_y * a_x = a_k a_y + a_\ell a_x$ 和 $a_x * a_y = a_y * a_x$, 可得 $(a_k - a_\ell)(a_x - a_y) = 0$. 又 $a_k - a_\ell \ne 0$, 所以 $a_x = a_y$, 矛盾. 所以拟群 $(F_n, *)$ 为反交换的.

下面证明拟群 $(F_n, *)$ 主对角线上的元素互不相同. 由 $a_x * a_x = (a_k + a_\ell)a_x$, 可知主对角线上的元素必不相同. 若不然，设拟群 $(F_n, *)$ 在位置 (a_s, a_s) 和 (a_t, a_t) 上的元素相同，其中 a_s, $a_t \in F_n$, $a_s \ne a_t$. 由 $a_s * a_s = a_s(a_k + a_\ell)$, $a_t * a_t = a_t(a_k + a_\ell)$ 和 $a_s * a_s = a_t * a_t$, 可得 $(a_k + a_\ell)(a_s - a_t) = 0$. 又 $a_k + a_\ell \ne 0$, 所以 $a_s = a_t$, 矛盾. 证毕.

引理 3.5 当 $n \ge 4$ 为偶数且 $4 \mid n$ 时，存在 n 阶主对角线上元素互不相同的反交换拟群.

证　这时可设 $n = 2^t m$, 其中 m 为奇数，$t \ge 2$.

当 $m = 1$ 时，由引理 3.4 知，存在 2^t 阶主对角线上元素互不相同的反交换拟群.

当 $m = 3$ 时，$n = 2^t \cdot 3$, 则奇数 $n - 1 \ge 11$ 且 $3 \nmid n - 1$. 由引理 3.1 知，存在 $n - 1$ 阶反交换拟群 $(Z_{n-1}, \cdot)$ 且该拟群有 $n - 1$ 个截态，其中之一在主对角线上. 我们考虑利用拟群 $(Z_{n-1}, \cdot)$ 构造 n 阶拟群 $(Q, \circ)$, 其中 $Q = Z_{n-1} \cup \{\infty\}$. 取拟群 $(Z_{n-1}, \cdot)$ 的一个截态 T, 且该截态不在拟群 $(Z_{n-1}, \cdot)$ 的主对角线上. 在集合 Q 上定义二元运算 “$\circ$” 如下：

(1) 对每个 $(x, y) \in T$, 定义 $x \circ \infty = \infty \circ y = x \cdot y$，$x \circ y = \infty$.

(2) $\forall x, y \in Z_{n-1}$，$(x, y) \notin T$, 定义 $x \circ y = x \cdot y$，$0 \le x$，$y \le n - 2$.

(3) $\infty \circ \infty = \infty$.

容易验证拟群 $(Q, \circ)$ 为主对角线上元素互不相同的反交换拟群.

当 $m \geq 5$ 时，由于拟群的乘法表为拉丁方，由引理 3.1 和引理 3.2 知，存在 m 阶主对角线上元素互不相同的反对称拉丁方 $L(m)$. 由引理 3.4 知，存在 2^t 阶的主对角线上元素互不相同的反对称拉丁方 $L(2^t)$. 由引理 3.3 知， $L(2^t) \times L(m)$ 是 $n = 2^t m$ 阶的反对称拉丁方. 记拉丁方 $L(2^t) \times L(m)$ 对应的拟群为 $(Q, \circ)$, 则拟群 $(Q, \circ)$ 为反交换的.

最后证明拟群 $(Q, \circ)$ 主对角线上的元素互不相同. 设拉丁方 $L(2^t)$ 的主对角线上的元素为 $a_1, a_2, \cdots, a_{2^t}$, 其中 $a_x \neq a_y$， $1 \leq x, y \leq 2^t$; 拉丁方 $L(m)$ 的主对角线上的元素为 $b_1, b_2, \cdots, b_m$, 其中 $b_x \neq b_y$， $1 \leq x, y \leq m$; 所以拉丁方 $L(2^t) \times L(m)$ 的主对角线上的元素为 $(a_x, b_1), (a_x, b_2), \cdots, (a_x, b_m)$, $x \in [1, 2^t]$. 容易验证 $L(2^t) \times L(m)$ 的主对角线上元素互不相同，所以 $L(2^t) \times L(m)$ 为主对角线上元素互不相同的反对称拉丁方，从而拟群 $(Q, \circ)$ 为主对角线上元素互不相同的反交换拟群. 证毕.

引理 3.6 当 $n \geq 6$ 为偶数， $4 \nmid n$ 且 $3 \nmid n-1$ 时，存在 n 阶主对角线上元素互不相同的反交换拟群.

证 这时 $n-1 \geq 5$, 由引理 3.1 知，存在 $n-1$ 阶反交换拟群 $(Z_{n-1}, \cdot)$ 且该拟群有 $n-1$ 个截态，其中之一在主对角线上. 我们考虑利用拟群 $(Z_{n-1}, \cdot)$ 构造 n 阶拟群 $(Q, \circ)$, 其中 $Q = Z_{n-1} \cup \{\infty\}$. 取拟群 $(Z_{n-1}, \cdot)$ 的一个截态 T, 且该截态不在拟群 $(Z_{n-1}, \cdot)$ 的主对角线上. 在集合 Q 上定义二元运算 “$\circ$” 如下：

(1) 对每个 $(x, y) \in T$, 定义 $x \circ \infty = \infty \circ y = x \cdot y$， $x \circ y = \infty$.

(2) $\forall\, x, y \in Z_{n-1}$， $(x, y) \notin T$, 定义 $x \circ y = x \cdot y$， $0 \leq x, y \leq n-2$.

(3) $\infty \circ \infty = \infty$.

容易验证拟群 $(Q, \circ)$ 为主对角线上元素互不相同的反交换拟群.

引理 3.7 当 $n \geq 10$ 为偶数， $4 \nmid n$ 且 $3 \mid n-1$ 时，存在 n 阶主对角线上元素互不相同的反交换拟群.

证 $n = 10$ 时，存在 10 阶主对角线上元素互不相同的反交换拟群 $(Q, \circ)$. 如下表：

$\circ$	0	1	2	3	4	5	6	7	8	9
0	0	2	8	6	9	7	1	5	4	3
1	5	1	3	0	7	9	8	2	6	4
2	7	6	2	4	1	8	9	0	3	5
3	4	8	7	3	5	2	0	9	1	6
4	2	5	0	8	4	6	3	1	9	7
5	9	3	6	1	0	5	7	4	2	8
6	3	9	4	7	2	1	6	8	5	0
7	6	4	9	5	8	3	2	7	0	1
8	1	7	5	9	6	0	4	3	8	2
9	8	0	1	2	3	4	5	6	7	9

当 $n > 10$ 时，这时有 $3 \nmid n-5$, 且 $n-5 \geq 7$. 由引理 3.1 知，存在 $n-5$ 阶反交换拟群 $(Z_{n-5}, \cdot)$ 且该拟群有 $n-5$ 个截态，其中之一在主对角线上. 我们考虑利用拟群 $(Z_{n-5}, \cdot)$ 构造 n 阶拟群 $(Q, \circ)$, 其中 $Q = Z_{n-5} \cup \{\infty_1, \infty_2, \infty_3, \infty_4, \infty_5\}$. 取拟群 $(Z_{n-5}, \cdot)$ 中的 5 个截态 T_1, T_2, T_3, T_4, T_5, 且此 5 个截态不在拟群 $(Z_{n-5}, \cdot)$ 的主对角线上. 在集合 Q 上定义二元运算 “$\circ$” 如下：

(1) $\forall\, (x, y) \in T_i$, 定义 $x \circ \infty_i = \infty_i \circ y = x \cdot y$， $x \circ y = \infty_i$； $i = 1, 2, \cdots, 5$.

(2)$\forall\, x, y \in Z_{n-5}$， $(x, y) \notin T_k$, $1 \leq k \leq 5$, 定义 $x \circ y = x \cdot y$， $0 \leq x, y \leq n-6$.

(3) $\forall\, x, y \in \{\infty_1, \infty_2, \infty_3, \infty_4, \infty_5\}$, 其运算可根据引理 3.1 中的 5 阶拟群来定义.

容易验证拟群 $(Q, \circ)$ 为主对角线上元素互不相同的反交换拟群.

结合上述引理 3.1, 3.2, 3.5–3.7, 我们可以得到下面定理：

定理 3.8 对任意的正整数 $n \geq 4$, 存在 n 阶主对角线上元素互不相同的反交换拟群.

参 考 文 献

1 Denes J, Keedwell A D. A New Authtication Scheme Based on Latin Squares. *Descrete Mathmatics*, 1992, 106/107: 157–161

2 Dawson E, Donovan D, Offer A. Quasigroups, Isotopisms and Authention Schemes. *The Australasian Journal of Combinatorics*, 1996, 13: 75–88

3 Meyer K A. A New Message Authentication Code Based on the Non-associativity of Quasigroups. Ph. D. thesis, Iowa State University, 2006

4 Preneel B. The State of Cryptographic Hash Functions, Lectures on Data Security. Lectures Notes in Computer Science, Vol.1561, 1999

5 Wegman M N, Carter J L. New Hash Functions and Their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*, 1981, 22: 265–279

6 Carter J L, Wegman M N. Universal Class of Hash Functions. *Journal of Computer and System Sciences*, 1979, 18(2): 143–154

7 Denes J, Keedwell A D. Latin Squares and Their Applications. New York: Academic Press, 1974

8 Smith J D H. An Introduction to Quasigroups and Their Representations. Boca Raton, Florida: CRC Press, 2007

9 Menezes A, Oorschot P, Vanstone S. Handbook of Applied Cryptography. Boca Raton, Florida: CRC Press, 1997

A Message Authentication Code Based on Anti-commutative Quasigroups

LI Weiqiang XU Yunqing

(*Faculty of Science, Ningbo University, Ningbo* 315211)

(*E-mail: xuyunqing@nbu.edu.cn)*

Abstract Let $(Q, \circ)$ be a quasigroup. If for any two different elements x, y in Q, we always have $x \circ y \neq y \circ x$, then we say that $(Q, \circ)$ is anti-commutative. In this paper, we give a new kind of message authentication code based on anti-commutative quasigroups and discuss the constructions of such quasigroups.

Key words quasigroup; Latin square; message authentication code

MR(2000) Subject Classification 05B15; 94A62

Chinese Library Classification O157.2; TP309.7