全距特征排列及全距置换 [1]

费如纯 王丽娜 董晓梅 于 戈

(东北大学信息学院 沈阳 110004)

摘 要 全距置换具有良好的密码学性质。该文首次提出了全距特征排列的概念，对全距特征排列的性质、计数进行了研究，并在此基础上讨论了全距置换与全距特征排列之间的映射关系，最后基于全距特征排列给出了全距置换的一种有效的构造方法，首先构造全距特征排列，再求出全距置换。

关键词 全距特征排列，全距特征映射，全距置换

中图号 TN918

1 引 言

Dr.Lothrop Mittental[1] 在 1996 年指出，全距置换作用于数据可打乱原数据的位置，同时又使元素间距离的所有可能性都出现，因而具有良好的密码学性质，可以被用于安全性很强的分组密码。在一个密钥作用下，一个私钥分组密码是二元域上的 n 维向量空间上的一个置换 [2,3]，另外，很多分组密码的换位操作都由置换来完成，例如 DES[4] 等。鉴于此，许多人对置换进行了深入的研究 [5-12]。因此，研究全距置换具有重要意义，其性质、计数和构造是研究的重点。亢保元、田建波、王育民 [1] 对全距置换做了有意义的研究，给出了全距置换的若干性质，得到了全距置换的总数为偶数的计数结论，并在全距拉丁方的基础上给出了全距置换的一种构造方法。

本文从研究全距置换中元素间距离在排列上的特征入手，首次提出了全距特征排列的概念，并对其性质以及计数进行了深入的探讨，然后给出了全距特征排列和全距置换之间的关系，最后基于全距特征排列给出了全距置换的一种更有效的构造方法。本文得到了一些很有价值的结论，包括全距特征排列的基本性质、计数及全距特征排列之间的关系、全距特征排列与全距置换之间的关系。本文所提出的全距特征排列的概念以及相关结论将为全距置换的进一步研究提供一条新的思路。

2 全距特征排列

定义 1 设 $P_1P_2\cdots P_n$ 为 $1,2,\cdots,n$ 的一个排列，若对任意 $s,t,1\le s\le t\le n$ 满足：$\sum_{i=s}^{t}P_i\neq 0(\mathrm{mod}(n+1))$，则称该排列为 n 阶全距特征排列。n 阶全距特征排列集合记为 $\mathrm{QTS}(n)$。

定理 1 存在 $P_1P_2\cdots P_n\in\mathrm{QTS}(n)$ 的充分必要条件是 n 为正奇数。

证明 (1) 充分性 当 $n=1$ 时结论显然成立。当 n 为奇数且 $n\ge 3$ 时，考虑排列：$1,n-1,3,n-3,\cdots,n-2,2,n$，即排列 $P_1P_2\cdots P_n$ 满足：对任意 $i,1\le i\le n$，如果 i 为奇数则 $P_i=i$，如果 i 为偶数则 $P_i=n+1-i$，可以验证此排列为 n 阶全距特征排列。总之，n 为正奇数时必存在 n 阶全距特征排列。

(2) 必要性 假设 n 为偶数时存在 $P_1P_2\cdots P_n\in\mathrm{QTS}(n)$，则 $\sum_{i=1}^{n}p_i=n(n+1)/2\equiv 0(\mathrm{mod}(n+1))$，这显然不符合 n 阶全距特征排列的要求，因此，若存在 n 阶全距特征排列，则 n 必须为正奇数。 证毕

[1] 2000-09-18 收到，2001-01-09 定稿

教育部跨世纪优秀人才基金和高等学校优秀青年教师教学和科研奖励基金资助

定理 2　设 n 为奇数且 $n \geq 3$，$P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，则 $\sum_{i=1}^{m} P_i \neq (n+1)/2(\mathrm{mod}(n+1))$，$\sum_{i=u}^{n} P_i \neq (n+1)/2(\mathrm{mod}(n+1))$，其中 $1 \leq m < n$，$1 < u \leq n$。

证明　使用反证法，假设存在 m，u，$1 \leq m < n$，$1 < u \leq n$，使 $\sum_{i=1}^{m} P_i \equiv (n+1)/2(\mathrm{mod}(n+1))$，$\sum_{i=u}^{n} P_i \equiv (n+1)/2(\mathrm{mod}(n+1))$，则 $\sum_{i=m+1}^{n} P_i = n(n+1)/2 - \sum_{i=1}^{m} P_i \equiv 0(\mathrm{mod}(n+1))$，$\sum_{i=1}^{u-1} P_i = n(n+1)/2 - \sum_{i=u}^{n} P_i \equiv 0(\mathrm{mod}(n+1))$，这与 $P_1P_2\cdots P_n$ 为 n 阶全距特征排列相矛盾。　　证毕

推论 1　设 n 为奇数且 $n \geq 3$，$P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，则 $P_1 \neq (n+1)/2$，$P_n \neq (n+1)/2$。

3 全距特征排列之间的关系

定理 3　设 n 为奇数且 $n \geq 3$，$P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，设其中 $P_u = (n+1)/2$，这里 $1 < u < n$，则 $P_{u-1}P_{u-2}\cdots P_1P_uP_nP_{n-1}\cdots P_{u+1} \in \mathrm{QTS}(n)$。

证明　将 $P_{u-1}P_{u-2}\cdots P_1P_uP_nP_{n-1}\cdots P_{u+1}$ 表示为 $Q_1Q_2\cdots Q_n$，当 $1 \leq s \leq t < u$ 时，$\sum_{i=s}^{t} Q_i = \sum_{i=s}^{t} P_{u-i} \neq 0(\mathrm{mod}(n+1))$；当 $u < s \leq t \leq n$ 时，$\sum_{i=s}^{t} Q_i = \sum_{i=s}^{t} P_{n+u+1-i} \neq 0(\mathrm{mod}(n+1))$；当 $1 \leq s \leq u \leq t \leq n$ 时，$\sum_{i=s}^{t} Q_i = \sum_{i=s}^{u-1} P_{u-i} + P_u + \sum_{i=u+1}^{t} P_{n+u+1-i} = (n+1)/2 + \sum_{i=1}^{u-s} P_i + \sum_{i=n+u+1-t}^{n} \neq 0(\mathrm{mod}(n+1))$。综上所证，$P_{u-1}P_{u-2}\cdots P_1P_uP_nP_{n-1}\cdots P_{u+1} \in \mathrm{QTS}(n)$。　　证毕

定理 4　设 n 为奇数，$P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，则 $P_nP_{n-1}\cdots P_1 \in \mathrm{QTS}(n)$。

定义 2　设 $P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，$Q_1Q_2\cdots Q_n = k\bullet(P_1P_2\cdots P_n)$ 表示对任意 i,$1 \leq i \leq n$，$Q_i = k \bullet P_i\mathrm{mod}(n+1)$，其中 k 为整数；若 $Q_1Q_2\cdots Q_n \in \mathrm{QTS}(n)$，则称 $Q_1Q_2\cdots Q_n$ 为 $P_1P_2\cdots P_n$ 和 k 导出的全距特征排列，并称此关系为导出关系，记为 $P_1P_2\cdots P_n \sim Q_1Q_2\cdots Q_n$。

注：$a = b\mathrm{mod}m$ 表示 b 除以 m 的余数为 a，与同余式的含义有所不同。

定理 5　设 $P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，$k$ 为整数，则 $Q_1Q_2\cdots Q_n = k\bullet(P_1P_2\cdots P_n) \in \mathrm{QTS}(n)$ 的充分必要条件是 $(k, n+1) = 1$。这里 $(k, n+1)$ 表示 k 与 $n+1$ 的最大公约数。

证明　(1) 充分性　因为 $(k, n+1) = 1$，所以对于任意的 i，$1 \leq i \leq n$，$Q_i = k \bullet P_i\mathrm{mod}(n+1) \neq 0$，且对于任意的 i,j，$1 \leq i,j \leq n$ 且 $i \neq j$，$k\bullet P_i \neq k\bullet P_j(\mathrm{mod}(n+1))$，得 $Q_i \neq Q_j$，所以 $Q_1Q_2\cdots Q_n$ 为 $1,2,\cdots,n$ 的一个排列。又对于任意的 s,t，$1 \leq s \leq t \leq n$，$\sum_{i=s}^{t} Q_i = \sum_{i=s}^{t}(k * P_i\mathrm{mod}(n+1)) \equiv k \bullet (\sum_{i=s}^{t} P_i) \neq 0(\mathrm{mod}(n+1))$，则 $Q_1Q_2\cdots Q_n \in \mathrm{QTS}(n)$。

(2) 必要性　已知 $Q_1Q_2\cdots Q_n \in \mathrm{QTS}(n)$，使用反证法，假设 $(k, n+1) = d \neq 1$，则 $P_1P_2\cdots P_n$ 中必存在某个 $P_u = (n+1)/d$，$Q_u = k\bullet P_u\mathrm{mod}(n+1) = k/d\bullet(n+1)\mathrm{mod}(n+1) = 0$，这与 $Q_1Q_2\cdots Q_n$ 是 $1,2,\cdots,n$ 的一个排列相矛盾，必要性得证。　　证毕

定理 6　设 $P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，$(k, n+1) = (r, n+1) = 1$，则 $k \bullet (P_1P_2\cdots P_n) = r \bullet (P_1P_2\cdots P_n)$ 的充分必要条件是 $k \equiv r\mathrm{mod}(n+1)$。

定理 7　全距特征排列之间的导出关系为等价关系。

证明 设 $P_1P_2\cdots P_n, Q_1Q_2\cdots Q_n, R_1R_2\cdots R_n \in \mathrm{QTS}(n)$

(1) 自反性：显然成立；

(2) 对称性：若 $P_1P_2\cdots P_n \sim Q_1Q_2\cdots Q_n$，则必存在 k，$(k, n+1) = 1$，使 $Q_1Q_2\cdots Q_n = k\bullet(P_1P_2\cdots P_n)$，进而 $P_1P_2\cdots P_n = k^{-1}\bullet(Q_1Q_2\cdots Q_n)$ 且 $(k^{-1}, n+1) = 1$，所以 $Q_1Q_2\cdots Q_n \sim P_1P_2\cdots P_n$；其中 $k^{-1} \bullet k \equiv 1((\mathrm{mod}(n+1))$；

(3) 传递性：若 $P_1P_2\cdots P_n \sim Q_1Q_2\cdots Q_n$，$Q_1Q_2\cdots Q_n \sim R_1R_2\cdots R_n$，则存在 k_1,k_2 且 $(k_1, n+1)=(k_2, n+1)=1$ 使得 $R_1R_2\cdots R_n = k_2 \bullet (Q_1Q_2\cdots Q_n) = k_2 \bullet k_1 \bullet (P_1P_2\cdots P_n)$ 且 $(k_2 \bullet k_1, n+1)=1$，所以 $P_1P_2\cdots P_n \sim R_1R_2\cdots R_n$。综上所证，$\sim$ 关系为等价关系。 证毕

由定理 7 可知，按全距特征排列间的等价关系可以把全距特征排列集划分为若干个等价类，若已知任意一个全距特征排列，就可以导出它所属等价类中的所有全距特征排列。

定义 3 设 $1 \le a \le n$，定义集合 $S_a(n) = \{t | 1 \le t \le n, (t, n+1) = a\}$；定义集合 $F(n)\{a | S_a(n) \ne \Phi\}$；设 $a \in F(n)$，定义集合 $T_a(n) = \{t | t \in S_1(n)$ 且不存在 $h < t$ 且 $h \in S_1(n)$ 使 $a \bullet h \equiv a \bullet t (\mathrm{mod}(n+1))\}$。很显然，当 $S_a(n) \ne \Phi$ 时，$|T_a(n)| = |S_a(n)|$。

对于任意的 i, $1 \le i \le n$, 如何由第 i 个元素为 a 的全距特征排列，通过定义 2 中的乘 t 运算导出一系列全距特征排列，是本文下面要讨论的一个关键问题。定义 3 中的 $|T_a(n)|$ 是能使这一系列全距特征排列的第 i 个元素不出现重复的 t 的个数。

定理 8 对于任意的 i，$1 \le i \le n$，则 $P_i = s$ 的任一个 n 阶全距特征排列 $P_1P_2\cdots P_n$ 能导出 $Q_i = t$ 的一个 n 阶全距特征排列 $Q_1Q_2\cdots Q_n$ 的充分必要条件是存在 a 使 $s,t \in S_a(n)$。

证明 下面证明充分性，其逆过程可证明必要性：

因为 $(s, n+1) = (t, n+1) = a$ 且 $1 \le s, t \le n$，设 $u = s/a, v = t/a, w = (n+1)/a$，则同余方程 $s \bullet x \equiv t (\mathrm{mod}(n+1))$ 有解 $x = u^{-1} \bullet v \mathrm{mod} w$ 且 $(x, n+1) = 1$，其中 $u^{-1} \bullet u \equiv 1 (\mathrm{mod} w)$。

所以对于任意一个 $P_i = s (1 \le i \le n)$ 的 n 阶全距特征排列 $P_1P_2\cdots P_n$，必存在一个 n 阶全距特征排列 $Q_1Q_2\cdots Q_n = x \bullet (P_1P_2\cdots P_n)$。 证毕

定理 9 $P_1P_2\cdots P_n \in \mathrm{QTS}(n)$，$t_1, t_2 \in T_a(n)$ 且 $t_1 \ne t_2$，则 $t_1 \bullet (P_1P_2\cdots P_n)$ 与 $t_2 \bullet (P_1P_2\cdots P_n)$ 对等位置的元素不同时为 a，其中 $a \in F(n)$。由 $T_a(n)$ 的定义易推知此定理成立。

定理 10 任取 i, $1 \le i \le n$, 则 $\{t \bullet (P_1P_2\cdots P_n) | P_1P_2\cdots P_n \in \mathrm{QTS}(n), t \in T_a(n), P_i = a\} = \{P_1P_2\cdots P_n | P_1P_2\cdots P_n \in \mathrm{QTS}(n), P_i \in S_a(n)\}$，其中 $a \in F(n)$。

证明 (1) 令 $A = \{t \bullet (P_1P_2\cdots P_n) | P_1P_2\cdots P_n \in \mathrm{QTS}(n),\ t \in T_a(n), P_i = a\}$，$B = \{P_1P_2\cdots P_n | P_1P_2\cdots P_n \in \mathrm{QTS}(n),\ P_i \in S_a(n)\}$，很显然，任取 $P_1P_2\cdots P_n \in A$ 及 $t \in T_a(n)$，得 $t \bullet (P_1P_2\cdots P_n) \in B$，得 $A \subseteq B$；

(2) 又任取 $u \in S_a(n)$ 及 $P_1P_2\cdots P_n \in B$ 且 $P_i = u$，一定存在一个 $R_i = a$ 的 $R_1R_2\cdots R_n \in \mathrm{QTS}(n)$ 及 $k \in S_1(n)$ 使 $P_1P_2\cdots P_n = k \bullet (R_1R_2\cdots R_n)$。如果 $k \in T_a(n)$，则 $P_1P_2\cdots P_n \in A$；如果 $k \notin T_a(n)$，则按 $T_a(n)$ 的定义，一定存在一个小于 k 的 $h \in T_a(n)$，满足 $a \bullet h \equiv a \bullet k (\mathrm{mod}(n+1))$，进而一定存在一个 $Q_i = a$ 的 $Q_1Q_2\cdots Q_n \in \mathrm{QTS}(n)$ 使 $P_1P_2\cdots P_n = h \bullet (Q_1Q_2\cdots Q_n) \in A$，得 $B \subseteq A$，所以 $A = B$。 证毕

推论 2 任取 i,$1 \le i \le n$ 和 $a \in F(n)$，则由所有的 $t \in T_a(n)$ 和所有 $P_i = a$ 的 n 阶全距特征排列交叉相乘可不重复地导出所有的 $P_i \in S_a(n)$ 的 n 阶全距特征排列。

4 全距特征排列的计数

定义 4 定义 $C(n)$ 为 n 阶全距特征排列的个数；定义 $N_{P_i=a}(n)$ 为满足 $P_i = a (1 \le i \le n)$ 的 n 阶全距特征排列 $P_1P_2\cdots P_n$ 的个数。

定理 11 若 n 为奇数且 $n \ge 5$，则 $4 | C(n)$。

证明 当 n 为奇数且 $n \ge 5$ 时，设 $P_1P_2\cdots P_n$ 为任一 n 阶全距特征排列，由推论 1 可知，$P_1 \ne (n+1)/2$，$P_n \ne (n+1)/2$，则必存在 t，$1 < t < n$ 使 $P_t = (n+1)/2$；

又根据定理 3 和定理 4，$P_{t-1}P_{t-2}\cdots P_1P_tP_nP_{n-1}\cdots P_{t+1}$，$P_nP_{n-1}\cdots P_{t+1}P_tP_{t-1}P_{t-2}\cdots P_1$，$P_{t+1}P_{t+2}\cdots P_nP_tP_1P_2\cdots P_{t-1}\in \mathrm{QTS}(n)$ 且互不相同，所以 $4|C(n)$。　　证毕

定理 12　$\Phi(n+1)|C(n)$。

证明　设 $K_1=1,K_2,\cdots,K_{\Phi(n+1)}$ 为 $1,2,\cdots,n$ 中 $\Phi(n+1)$ 个与 $n+1$ 互素的数，且两两互不相同，则根据上一节的知识可知：若 $P_1P_2\cdots P_n$ 为任一 n 阶全距特征排列，则 $K_1\bullet(P_1P_2\cdots P_n)$，$K_2\bullet(P_1P_2\cdots P_n),\cdots,K_{\Phi(n+1)}\bullet(P_1P_2\cdots P_n)\in\mathrm{QTS}(n)$，它们互不相同且仅有 $K_1\bullet(P_1P_2\cdots P_n)=P_1P_2\cdots P_n$ 所以 $\Phi(n+1)|C(n)$。　　证毕

定理 13　若存在 a 使 $s,t\in S_a(n)$，则对于任意的 i，$1\le i\le n$，$N_{P_i=s}(n)=N_{P_i=t}(n)$。

定理 14　任取 $i,1\le i\le n$，则 $C(n)=\sum_{a\in F(n)}(N_{P_i=a}(n)\bullet|S_a(n)|)$。

证明 (1) 设 $t\in S_a(n)$，由定理 13 可知，$N_{P_i=a}(n)=N_{P_i=t}(n)$，因此满足 $P_i\in S_a(n)$ 的 n 阶全距特征排列的总数为 $N_{P_i=a}(n)\bullet|S_a(n)|$；

(2) 任取 $i,1\le i\le n$，令 $a=(i,n+1)$，则 $i\in S_a(n)$ 且 $a\in F(n)$，另外，对于任意 $a\ne b$ 且 $a,b\in F(n)$，显然 $S_a(n)\cap S_b(n)=\Phi$，所以，集合 $\{S_a(n)|a\in F(n)\}$ 为集合 $\{1,2,\cdots,n\}$ 的一个划分；综上所证，n 阶全距特征排列的总数 $C(n)=\sum_{a\in F(n)}(N_{P_i=a}(n)\bullet|S_a(n)|)$。　　证毕

5 全距特征排列与全距置换的关系

定义 5[1]　设置换 $\pi=\begin{bmatrix}1,2,\cdots,n\\ a_1,a_2,\cdots,a_n\end{bmatrix}$，简记为 $\pi=(a_1,a_2,\cdots,a_n)$，称 i 为置换 π 中 a_i 的坐标，记为 $p(a_i)$；定义 $D(i,j)=(p(j)-p(i))\mathrm{mod}n$，若 $D(1,2),D(2,3),\cdots,D(n-1,n)$ 两两互不相同，则称 π 为一个 n 阶全距置换。n 阶全距置换集合记为 $\mathrm{QTP}(n)$。

定理 15　任意一个 $\pi=(a_1,a_2,\cdots,a_n)\in\mathrm{QTP}(n)$ 必对应于一个 $P_1P_2\cdots P_{n-1}\in\mathrm{QTS}(n-1)$，对应关系为对于任意 $i,1\le i\le n-1$，$P_i=D(i,i+1)$。

证明　由全距置换的定义可知 $P_1P_2\cdots P_{n-1}$ 必为一个 $1,2,\cdots,n-1$ 的排列，使用反证法，假设 $P_1P_2\cdots P_{n-1}\ne\mathrm{QTS}(n-1)$，即存在 $s,t,1\le s\le t\le n-1$ 使 $\sum_{i=s}^{t}P_i\equiv 0(\mathrm{mod}n)$，则 $p(s+1)-p(s)+p(s+2)-p(s+1)+\cdots+p(t+1)-p(t)=p(t+1)-p(s)\equiv 0(\mathrm{mod}n)$，$p(t+1)=p(s)$，这与 π 为一个置换相矛盾。　　证毕

推论 3　存在 n 阶全距置换的充分必要条件是 n 为正偶数。

定义 6　按定理 15 中的对应关系建立的映射 f：$\mathrm{QTP}(n)\to\mathrm{QTS}(n-1)$ 称为全距特征映射；设 $Q_1Q_2\cdots Q_{n-1}\in\mathrm{QTS}(n-1)$，将 $Q_1Q_2\cdots Q_{n-1}$ 在 f 下的全原像记为 $f_I(Q_1Q_2\cdots Q_{n-1})$。

定理 16　设 $Q_1Q_2\cdots Q_{n-1}\in\mathrm{QTS}(n-1)$，则 $f_I(Q_1Q_2\cdots Q_{n-1})=\{(b_1,b_2,\cdots,b_n)^{-1}|1\le b_1\le n$，对于任意 $i,2\le i\le n$，$b_i=(b_{i-1}+Q_{i-1}-1)\mathrm{mod}n+1\}$，$|f_I(Q_1Q_2\cdots Q_{n-1})|=n$。

证明　取 b_1 为 $1,2,\cdots,n$ 中任一数，对于 $i=2,3,\cdots,n$，取 $b_i=(b_{i-1}+Q_{i-1}-1)\mathrm{mod}n+1$，由全距特征排列的定义可知，$b_1b_2\cdots b_n$ 为一个 $1,2,\cdots,n$ 的排列，再定义一个置换 $\pi=(a_1,a_2,\cdots,a_n)=(b_1,b_2,\cdots,b_n)^{-1}$，显然 π 为一个全距置换且 $f(\pi)=Q_1Q_2\cdots Q_{n-1}$，并且当 b_1 取 n 个不同的数时可得到 n 个不同的 π。　　证毕

推论 4　$\{f_I(Q_1Q_2\cdots Q_{n-1})|Q_1Q_2\cdots Q_{n-1}\in\mathrm{QTS}(n-1)\}$ 是 $\mathrm{QTP}(n)$ 的一个划分。

推论 5　n 阶全距置换的总数 $|\mathrm{QTP}(n)|=n\bullet C(n-1)$。

6 全距置换的构造

由上述讨论推知，要构造 n 阶 (n 为正偶数) 全距置换，可先构造 $n-1$ 阶全距特征排列，再按定理 16 证明过程中的变换方法可构造 n 阶全距置换。由定理 2 知，$n-1\geq 3$ 时，全距特征排列 $P_1P_2\cdots P_{n-1}$ 满足 $P_1\neq n/2$，又根据推论 2，只要构造出 $P_1\in F(n-1)-\{n/2\}$ 的所有 $n-1$ 阶全距特征排列，就可导出所有的 $n-1$ 阶全距特征排列，进而可得到所有的 n 阶全距置换。在整个构造过程中，$n-1$ 阶全距特征排列的构造是关键。

算法 1 构造一个 $n-1$ 阶 ($n-1\geq 3$ 且为奇数) 全距特征排列。

步骤 (1) 初始化：对于 $i=1,2,\cdots,n-1$ 取 QTAG[i]=PTAG[i]=FALSE；

步骤 (2) 取 $Q_1=n$，QTAG[$n/2$]=TRUE，任取 $Q_2=P_1\in F(n-1)-\{n/2\}$；

步骤 (3) 对 $i=2,3,\cdots,n-2$ 进行如下处理：

(a) QTAG$\lfloor Q_i\rfloor$=TRUE，PTAG$\lfloor P_{i-1}\rfloor$=TRUE；

(b) 选择 Q_{i+1} 并取 $P_i=(Q_{i+1}-Q_i)\bmod n$，满足 QTAG$\lfloor Q_{i+1}\rfloor$=PTAG$\lfloor P_i\rfloor$=FALSE；若无可选的 Q_{i+1}，则进行回溯处理；

步骤 (4) 取 $P_{n-1}=(n/2-Q_{n-1})\bmod n$；

步骤 (5) 任选 $t\in T_{P1}(n-1)$，计算 $t\bullet(P_1P_2\cdots P_{n-1})$ 即为所求。

算法 1 实际上是构造两个序列：$P_1P_2\cdots P_{n-1}$ 和 $Q_1Q_2\cdots Q_{n-1}Q_n$ 满足 $P_i=(Q_i-Q_{i+1})\bmod n(i=1,2,\cdots,n-1)$，其中 $Q_n=n/2$，由算法处理过程可知 $Q_1Q_2\cdots Q_n$ 是一个 $1,2,\cdots,n$ 的排列，$P_1P_2\cdots P_{n-1}$ 是一个 $n-1$ 阶全距特征排列。

算法 2 构造一个 n 阶 ($n\geq 4$ 且为偶数) 全距置换。

步骤 (1) 任选一个 $n-1$ 阶全距特征排列 $P_1P_2\cdots P_{n-1}$ 及 $R_1,1\leq R_1\leq n$；

步骤 (2) 构造排列 $R_1R_2\cdots R_n$：对 $i=1,2,\cdots,n-1$，$R_{i+1}=(R_i+P_i)\bmod n$；

步骤 (3) 构造全距置换 $\pi=(a_1,a_2,\cdots,a_n)$：对 $i=1,2,\cdots,n$，若 $R_i=t$，则 $a_t=i$。

对上述两个算法稍加改造 (在算法 1 中加上搜索与回溯) 就可构造出所有的 $n-1$ 阶全距特征排列和 n 阶全距置换。

7 结 束 语

本文从全距特征排列入手，对全距置换做了有益的研究，得到并证明了一些很有价值、有启发性的结论，给出了一种基于全距特征排列的全距置换构造方法，但还存在一些问题有待于进一步探索，包括全距置换应用于密码学的深入研究、全距置换计数的进一步探讨和更高效的全距置换构造方法。

参 考 文 献

[1] 冗保元，田建波，王育民，全距置换，密码学进展— CHINACRYPT'98，北京，科学出版社，1998，207-211.

[2] 王育民，刘建伟，通信网的安全——理论与技术，第一版，西安，西安电子科技大学出版社，1999，126-128.

[3] 冯登国，裴定一，密码学导引，第一版，北京，科学出版社，1999，107-108.

[4] NBS, Data Encryption Standard, FIPS PUB 46, National Bureau of Standards, Washington D.C, 1977.

[5] K. D. Paterson, Imprimitive permutation groups and trapdoors in iterated block cipher, Proc. Fast Software Encryption FSE'99, LNCS 1636, 1999, 201–214.

[6] S. Even, Y. Mansour, A Construction of a cipher from a single pseudo-random permutation, Journal of Cryptology, 1997, 10(3), 151–162.

[7] J. Patarin, Pseudo-random permutation based on the DES scheme, Proc. of EUROCODE'90, Lecture Notes in Computer Science, Springer-Verlag, 1991, 193–204.

[8] J. Patarin, Improved security bounds for pseudo-random permutations, 4th ACM Conference on Computer and Communications Security, 1997, 142–150.

[9] M. Naor, O. Reingold, On the construction of pseudo-random permutations: Luby-Rackoff Revisited, Proc. of the 29th ACM Symposium on Theory of Computing, 1997, 189–199.

[10] M. Luby, C. Rackoff, How to construct pseudo-random permutations from pseudo-random functions, In SLAM Journal on Computing, 1988, 17(2), 373–386.

[11] S. W. Golomb, Oscar Moreno, On periodicity of costas arrays and a conjecture on permutation polynomials, IEEE Trans. on Information Theory, 1996, 42(6), 2252–2253.

[12] S. W. Golomb, H. Taylor, Constructions and properties of costas arrays, Proc. IEEE, 1984, 72(9), 1143 -1163.

QUICK TRICKLE CHARACTERISTIC SEQUENCE AND QUICK TRICKLE PERMUTATION

Fei Ruchun Wang Lina Dong Xiaomei Yu Ge

(*Northeastern University, Shenyang* 110004, China)

Abstract Quick trickle permutation has good cryptographic properties. In this paper, the concept of quick trickle characteristic sequence is presented, the properties and count of quick trickle characteristic sequence are researched, the mapping relation between quick trickle characteristic sequence and quick trickle permutation is discussed. Finally, a effective construction of quick trickle permutation based on quick trickle characteristic sequence is given, by which quick trickle permutation can be figured out after constructing quick trickle characteristic sequence.

Key words Quick trickle characteristic sequence, Quick trickle characteristic mapping, Quick trickle permutation

费如纯： 男， 1969 年生，硕士生，主要研究方向为计算机安全及密码学.
王丽娜： 女， 1965 年生，副教授，主要研究方向为分布式数据库及网络安全.
董晓梅： 女， 1970 年生，讲师，主要研究方向为计算机安全及密码学.
于 戈： 男， 1962 年生，教授，博士生导师，主要研究方向为分布式数据库及网络安全.