文章编号: 1001 - 2486(2003)05 - 0090 - 04

密码体制中布尔置换的构造*

金君娥, 朱华安, 谢端强
(国防科技大学理学院, 湖南 长沙 410073)

摘 要: 布尔置换在密码体制中有着非常重要的应用。在分组密码的设计中需要用到高阶的布尔置换。论述了一种通过组合一些低阶布尔置换来构造高阶布尔置换的方法, 给出了一个例子。所得结论对布尔置换的构造具有一定的意义。

关键词: 布尔置换; 平衡函数; 密码体制
中图分类号:TN918.1 文献标识码: A

The Construction of Boolean Permutations in Cryptosystems

JIN Jun-e, ZHU Hua-an, XIE Duan-qiang
(College of Science, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Boolean permutations are in very important applications in cryptosystems. In the design of block cipher, those of high degree are needed. In this paper, a method of constructing boolean permutations of high degree by combining some boolean permutations of low degree is provided, and an example is given. The results are useful to the construction of boolean permutations.

Key words: Boolean permutation; balanced function; cryptosystem

布尔置换在密码体制的设计中有重要的应用, 任何没有信息扩张的密码体制都可以看做置换的结果, 常用的分组密码体制 DES 算法是明文在密钥控制下的置换, 公钥密码体制 RSA 可以看做是一种多项式置换[1]。对本质上是一个置换的分组密码则主要取决于它所使用的置换的好坏, 特别是差分密码分析和线性密码分析的提出以及对DES 密码体制的破译, 迫使人们设计更好的密码算法, 寻找更好的置换源。

关于置换理论的研究是近年来密码学研究的热点之一。文献[2] 讨论了布尔置换的性质和结构, 文献[3] 讨论了布尔置换的基于级联运算的迭代构造方法。本文改进了文献[4] 中由低阶布尔置换构造高阶布尔置换的构造方法, 理论上可以构造出任意高阶的布尔置换。

1 基本概念

定义 **1** 设 F 为 $GF(2)^n$ 到 $GF(2)^n$ 上的双射, 即对任意 $a \in GF(2)^n$, 有且仅有唯一的 $x \in GF(2)^n$, 使得 $F(x) = a$, 则称 F 为 $GF(2)^n$ 上的布尔置换。

设 F_n 为全体 n 元布尔函数的集合, 一般地, 对 n 阶布尔置换 F, 习惯地表示 $F(x) = (f_1(x), f_2(x), \cdots, f_n(x))$, 其中 $f_i \in F_n$, $1 \leqslant i \leqslant n$。

定义 **2** 设 $f(x) \in F_n$, 记 $W(f) = \sum_{x \in GF(2)^n} f(x)$ 为 $f(x)$ 的 Hamming 重量。如果 $W(f) = 2^{n-1}$, 则称 $f(x)$ 是 $GF(2)^n$ 上的平衡函数。

引理 **1**[2] $F(x) = (f_1(x), f_2(x), \cdots, f_n(x))$ 为 $GF(2)^n$ 上布尔置换的充要条件为 $F(x)$ 的分量函数的任意非零线性组合 $\sum_{i=1}^{n} c_i f_i(x)$ 为 $GF(2)^n$ 上的平衡函数, $c = (c_1 c_2 \cdots c_n) \in GF(2)^n$, 且 $c \neq 0$。

由引理 1, 布尔置换的构造就转化为如何构造满足引理 1 的 n 个平衡布尔函数。

* 收稿日期: 2003 - 03 - 19
作者简介: 金君娥(1977—), 女, 硕士生。

引理 **2** 设$f_i(u_i)$为$GF(2)^{n_i}$上的布尔函数, $u_i \in GF(2)^{n_i}$, $i = 1, 2, \cdots, s$, 如果其中有一个是平衡函数, 则$f(u_1, u_2, \cdots, u_s) = f_1(u_1) \dot{\vee} f_2(u_2) \dot{\vee} \cdots \dot{\vee} f_s(u_s)$是$GF(2)^m$上的平衡函数, $m = n_1 + n_2 + \cdots + n_s$。

2 主要结果

设$F_1(u_1) = (f_{11}(u_1), f_{12}(u_1), \cdots, f_{1n_1}(u_1))$, $u_1 \in GF(2)^{n_1}$, $F_2(u_2) = (f_{21}(u_2), f_{22}(u_2), \cdots, f_{2n_2}(u_2))$, $u_2 \in GF(2)^{n_2}$, $n_1 < n_2$。当$n_2 \geqslant i > n_1$时, 约定$f_{1i}(u_1) = 0$, 并定义$F_1(u_1) \dot{\vee} F_2(u_2)$如下:

$$\begin{aligned} & F_1(u_1) \dot{\vee} F_2(u_2) \\ = & (f_{11}(u_1) \dot{\vee} f_{21}(u_2), f_{12}(u_1) \dot{\vee} f_{22}(u_2), \cdots, f_{1n_1}(u_1) \dot{\vee} f_{2n_1}(u_2), f_{2(n_1+1)}(u_2), \cdots, f_{2n_2}(u_2)) \\ = & (f_{11}(u_1) \dot{\vee} f_{21}(u_2), f_{12}(u_1) \dot{\vee} f_{22}(u_2), \cdots, f_{1n_1}(u_1) \dot{\vee} f_{2n_1}(u_2), \cdots, f_{1n_2}(u_1) \dot{\vee} f_{2n_2}(u_2)) \end{aligned}$$

它是$GF(2)^{n_1+n_2}$上的函数。在下面的论述中与此相同。

定理 **1** 设$F_1(u_1) = (f_{11}(u_1), f_{12}(u_1), \cdots, f_{1n_1}(u_1))$, $F_2(u_2) = (f_{21}(u_2), f_{22}(u_2), \cdots, f_{2n_2}(u_2))$, $\cdots$, $F_s(u_s) = (f_{s1}(u_s), f_{s2}(u_s), \cdots, f_{sn_s}(u_s))$分别是$GF(2)^{n_1}$, $GF(2)^{n_2}$, $\cdots$, $GF(2)^{n_s}$上的布尔置换, 其中$u_i \in GF(2)^{n_i}$, $1 \leqslant i \leqslant s$; 设$A = (a_{ij})_{s\times s}$为$GF(2)$上的$s$阶可逆矩阵, 且满足: $\forall j, 1 \leqslant j \leqslant s$, 当$n_i > n_j$时$a_{ij} = 0$, $1 \leqslant i \leqslant s$, 则$F(u_1, u_2, \cdots, u_s) = (F_1(u_1), F_2(u_2), \cdots, F_s(u_s))A$为$GF(2)^l$上的布尔置换, 其中$l = n_1 + n_2 + \cdots + n_s$。

证明 设$n = \max\{n_1, n_2, \cdots, n_s\}$。先证$n_1 \leqslant n_2 \leqslant \cdots \leqslant n_s$的情形。

$(F_1(u_1), F_2(u_2), \cdots, F_s(u_s))$与$A$的第一列$(a_{11}, a_{21}, \cdots, a_{s1})$相乘为: $h_1 = a_{11}F_1(u_1) \dot{\vee} a_{21}F_2(u_2) \dot{\vee} \cdots \dot{\vee} a_{s1}F_s(u_s)$, 设$t_1 = \max\{j \mid a_{j1} \neq 0, 1 \leqslant j \leqslant s\}$, 令$m_1 = n_{t_1}$, 则

$$\begin{aligned} h_1 &= a_{11}F_1(u_1) \dot{\vee} a_{21}F_2(u_2) \dot{\vee} \cdots \dot{\vee} a_{t_1 1}F_{t_1}(u_{t_1}) \\ &= \left(\dot{\bigvee_{i=1}^{t_1}} a_{i1}f_{i1}(u_i), \dot{\bigvee_{i=1}^{t_1}} a_{i1}f_{i2}(u_i), \cdots, \dot{\bigvee_{i=1}^{t_1}} a_{i1}f_{im_1}(u_i)\right) \end{aligned}$$

同理, $(F_1(u_1), F_2(u_2), \cdots, F_s(u_s))$与$A$的其它列相乘依次为:

$$h_2 = \left(\dot{\bigvee_{i=1}^{t_2}} a_{i2}f_{i1}(u_i), \dot{\bigvee_{i=1}^{t_2}} a_{i2}f_{i2}(u_i), \cdots, \dot{\bigvee_{i=1}^{t_2}} a_{i2}f_{im_2}(u_i)\right)$$

$$\vdots$$

$$h_s = \left(\dot{\bigvee_{i=1}^{t_s}} a_{is}f_{i1}(u_i), \dot{\bigvee_{i=1}^{t_s}} a_{is}f_{i2}(u_i), \cdots, \dot{\bigvee_{i=1}^{t_s}} a_{is}f_{im_s}(u_i)\right)$$

于是$F(u_1, u_2, \cdots, u_s) = (F_1(u_1), F_2(u_2), \cdots, F_s(u_s))A = (h_1, h_2, \cdots, h_s)$是$GF(2)^m$上的函数, $m = m_1 + m_2 + \cdots + m_s$。对$1 \leqslant k \leqslant s$, h_k的每一个分量函数是若干平衡函数的和, 由引理2知, 它是平衡的。设h_k的分量函数的线性组合为

$$L(h_k) = c_{k1}\left[\dot{\bigvee_{i=1}^{t_k}} a_{ik}f_{i1}(u_i)\right] \dot{\vee} c_{k2}\left[\dot{\bigvee_{i=1}^{t_k}} a_{ik}f_{i2}(u_i)\right] \dot{\vee} \cdots \dot{\vee} c_{km_k}\left[\dot{\bigvee_{i=1}^{t_k}} a_{ik}f_{im_k}(u_i)\right]$$

因为当$i > t_k$时$a_{ik} = 0$, 当$i \leqslant t_k$且$j > m_k$时按照我们的约定$f_{ij}(u_i) = 0$, 故

$$\begin{aligned} L(h_k) &= c_{k1}\left[\dot{\bigvee_{i=1}^{s}} a_{ik}f_{i1}(u_i)\right] \dot{\vee} c_{k2}\left[\dot{\bigvee_{i=1}^{s}} a_{ik}f_{i2}(u_i)\right] \dot{\vee} \cdots \dot{\vee} c_{km_k}\left[\dot{\bigvee_{i=1}^{s}} a_{ik}f_{im_k}(u_i)\right] \dot{\vee} \cdots \dot{\vee} c_{kn}\left[\dot{\bigvee_{i=1}^{s}} a_{ik}f_{in}(u_i)\right] \\ &= \left[\dot{\bigvee_{i=1}^{n}} a_{1k}c_{kj}f_{1i}(u_1)\right] \dot{\vee} \left[\dot{\bigvee_{i=1}^{n}} a_{2k}c_{kj}f_{2i}(u_2)\right] \dot{\vee} \cdots \dot{\vee} \left[\dot{\bigvee_{i=1}^{n}} a_{sk}c_{kj}f_{si}(u_s)\right] \end{aligned}$$

当$j > m_k$时, 令$c_{kj} = 0$。

现在考虑$F(u_1, u_2, \cdots, u_s) = (h_1, h_2, \cdots, h_s)$的分量函数的任意非零线性组合:

$$L(h_1) \dot{\vee} L(h_2) \dot{\vee} \cdots \dot{\vee} L(h_s)$$

$$= \left[\prod_{i=1}^{n}\left(\sum_{k=1}^{s} a_{1k}c_{ki}\right)f_{1i}(u_1)\right] \times \left[\prod_{i=1}^{n}\left(\sum_{k=1}^{s} a_{2k}c_{ki}\right)f_{2i}(u_2)\right] \times \cdots \times \left[\prod_{i=1}^{n}\left(\sum_{k=1}^{s} a_{sk}c_{ki}\right)f_{si}(u_s)\right]$$

$$= \left[\prod_{i=1}^{n} a_1 c_i f_{1i}(u_1)\right] \times \left[\prod_{i=1}^{n} a_2 c_i f_{2i}(u_2)\right] \times \cdots \times \left[\prod_{i=1}^{n} a_s c_i f_{si}(u_s)\right]$$

$$= \left[\prod_{i=1}^{n_1} a_1 c_i f_{1i}(u_1)\right] \times \left[\prod_{i=1}^{n_2} a_2 c_i f_{2i}(u_2)\right] \times \cdots \times \left[\prod_{i=1}^{n_s} a_s c_i f_{si}(u_s)\right] \quad (1)$$

其中 $a_k = (a_{k1}, a_{k2}, \cdots, a_{ks})$, $k = 1, 2, \cdots, s$, $c_i = (c_{1i}, c_{2i}, \cdots, c_{si})^{\mathrm{T}}$, $i = 1, 2, \cdots, n$, $a_k c_i \in \{0, 1\}$。

令矩阵 $C = (c_1, c_2, \cdots, c_n)$。易见 A, C 有如下特点:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1l} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2l} & \cdots & a_{2s} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & a_{ll} & \cdots & a_{ls} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & a_{ss} \end{pmatrix} = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}$$

$$C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1m_1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ c_{21} & c_{22} & \cdots & c_{2m_1} & c_{2(m_1+1)} & \cdots & c_{2m_2} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ c_{s1} & c_{s2} & \cdots & c_{sm_1} & c_{s(m_1+1)} & \cdots & c_{sm_2} & c_{s(m_2+1)} & \cdots & c_{sn} \end{pmatrix}$$

$$AC = \begin{pmatrix} a_1c_1 & a_1c_2 & \cdots & a_1c_{n_1} & * & \cdots & * & * & \cdots & * \\ a_2c_1 & a_2c_2 & \cdots & a_2c_{n_1} & a_2c_{n_1+1} & \cdots & a_2c_{n_2} & * & \cdots & * \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_sc_1 & a_sc_2 & \cdots & a_sc_{n_1} & a_sc_{n_1+1} & \cdots & a_sc_{n_2} & a_sc_{n_2+1} & \cdots & a_sc_n \end{pmatrix}$$

可见, 只要证明 AC 中除"*"位置外的元素中必有一个非零, 设为 $a_k c_j, j \leqslant n_k$, 则因为 $F_k(u_k)$ 为布尔置换, 由引理1知, 非零线性组合 $\prod_{i=1}^{n_k} a_k c_i f_{ki}(u_k)$ 为平衡函数, 再由引理2, (1) 式为 $GF(2)^m$ 上的平衡函数, 即 $F(u_1, u_2, \cdots, u_s)$ 的分量函数的任意非零线性组合为平衡函数, 则由引理1, $F(u_1, u_2, \cdots, u_s)$ 为 $GF(2)^m$ 上的布尔置换。下面证明 AC 中除"*"位置外的元素中必有一个非零。

因为 A 为可逆矩阵, 所以 A_2 也是可逆矩阵。下面分三种情形讨论。

情形1: 若存在某个 $j, j \leqslant n_1$, 有 $c_j \neq 0$。此时 $Ac_i \neq 0$, 即 $a_1c_j, a_2c_j, \cdots, a_sc_j$ 中至少有一个非零。

情形2: 若 $j = n_1 + 1$ 时 $c_j \neq 0$。

若 $n_2 > n_1$, 则有 $n_i > n_1$, 故 $a_{i1} = 0, 2 \leqslant i \leqslant s$, 即矩阵 A 的第一列为 $(1, 0, 0, \cdots, 0)$, 此时 $m_1 = n_1$, $c_j = (0, c_{2j}, \cdots, c_{sj})^{\mathrm{T}}$, $A = \begin{pmatrix} 1 & * \\ 0 & A_2 \end{pmatrix}$, 令 $c'_j = (c_{2j}, \cdots, c_{sj})^{\mathrm{T}}$, 则有 $c'_j \neq 0, A_2c'_j \neq 0$, 于是 $a_2c_j, \cdots, a_sc_j$ 中至少有一个非零。

若 $n_2 = n_1$, 设 $n_b > n_{b-1} = \cdots = n_2 = n_1$, 同理有 $A = \begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}$, A_2 为 $(s - b + 1) \times (s - b + 1)$ 的可逆矩阵, 此时 $m_i = n_{t_i} = n_1 = n_i, 1 \leqslant i < b$, 故 $c_j = (0, 0, \cdots, c_{bj}, \cdots, c_{sj})^{\mathrm{T}}$, 令 $c'_j = (c_{bj}, \cdots, c_{sj})^{\mathrm{T}}$, 则有 $c'_j \neq 0, A_2c'_j \neq 0$, 于是 $a_bc_j, \cdots, a_sc_j$ 中至少有一个非零。

注意 A_2 为可逆矩阵, 它的第一列非零, 设其第一列的第 k 个元素非零, 则 $n_{b+k} > n_{b+k-1} = \cdots = n_b$, $m_i = n_{t_i} = n_b = n_i, b \leqslant i < b + k$。同理, 可得 $m_i = n_{t_i} = n_b = n_i, b + k \leqslant i \leqslant s, 2 \leqslant b \leqslant s$, 所以综上所述, $m = m_1 + m_2 + \cdots + m_s = n_1 + n_2 + \cdots + n_s = l$。

情形 3: 若存在某个 j, $j > n_1 + 1$, $c_j \neq 0$。与情形 2 同理。

至此, $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_s$ 的情形证毕。当 $n_1, n_2, \cdots, n_s$ 不满足 $n_1 \leqslant n_2 \leqslant \cdots \leqslant n_s$ 时, 改变 $(h_1, h_2, \cdots, h_s)$ 的分量函数的非零线性组合的排列顺序, 让 C 作行变换, 相应地 A 作列变换, 再让 AC 作行变换, 相应地 A 作行变换, 使得矩阵 A、C 具有前面所说的特点, 此时 $(h_1, h_2, \cdots, h_s)$ 的分量函数的非零线性组合却不变, 故同理可证该非零线性组合是平衡函数, 由引理 1 得到 $F(u_1, u_2, \cdots, u_s)$ 为 $GF(2)^l$ 上的布尔置换。证毕。

推论 **1** 设 $F_1(u_1) = (f_{11}(u_1), f_{12}(u_1), \cdots, f_{1n}(u_1))$, $F_2(u_2) = (f_{21}(u_2), f_{22}(u_2), \cdots, f_{2n}(u_2))$, $\cdots$, $F_s(u_s) = (f_{s1}(u_s), f_{s2}(u_s), \cdots, f_{sn}(u_s))$ 是 $GF(2)^n$ 上的布尔置换, 其中 $u_i \in GF(2)^n$, $1 \leqslant i \leqslant s$, 设 $A = (a_{ij})_{s\times s}$ 为 $GF(2)$ 上的 s 阶可逆矩阵, 则有 $F(u_1, u_2, \cdots, u_s) = (F_1(u_1), F_2(u_2), \cdots, F_s(u_s))A$ 为 $GF(2)^{sn}$ 上的布尔置换。

设 $F_1(u_1) = (f_{11}(u_1), f_{12}(u_1))$, $F_2(u_2) = (f_{21}(u_2), f_{22}(u_2), f_{23}(u_2))$, $F_3(u_3) = (f_{31}(u_3), f_{32}(u_3), f_{33}(u_3))$, 其中 $u_1 = (u_{11}u_{12}) \in GF(2)^2$, $u_2 = (u_{21}u_{22}u_{23}) \in GF(2)^3$, $u_3 = (u_{31}u_{32}u_{33}) \in GF(2)^3$, 且:

$$f_{11}(u_1) = u_{12}; f_{12}(u_1) = u_{11} \dot{\vee} u_{12}; \quad f_{21}(u_2) = u_{22}; f_{22}(u_2) = u_{21} \dot{\vee} u_{23}; f_{23}(u_2) = u_{21};$$

$$f_{31}(u_3) = u_{31}; f_{32}(u_3) = u_{32} \dot{\vee} u_{31}u_{32} \dot{\vee} u_{31}u_{33}; f_{33}(u_3) = u_{31}u_{32} \dot{\vee} u_{31}u_{33} \dot{\vee} u_{33}$$

可验证 $F_1(u_1)$, $F_2(u_2)$, $F_3(u_3)$ 分别是 $GF(2)^2$, $GF(2)^3$, $GF(2)^3$ 上的布尔置换。

设 $A = (a_{ij})_{3\times 3}$ 为满足定理 1 中条件的 $GF(2)$ 上的 3 阶可逆方阵, 即必须有 $a_{21} = 0$, $a_{31} = 0$, 我们随便选取一个满足要求的 3 阶可逆矩阵 $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, 则

$$\begin{aligned} F(u_1, u_2, u_3) &= (F_1(u_1), F_2(u_2), F_3(u_3))A \\ &= (f_{11}, f_{12}, f_{11} \dot{\vee} f_{31}, f_{12} \dot{\vee} f_{32}, f_{33}, f_{21}, f_{22}, f_{23}) \end{aligned} \tag{2}$$

令 $x = (u_1, u_2, u_3) = (u_{11}u_{12}u_{21}u_{22}u_{23}u_{31}u_{32}u_{33}) \in GF(2)^8$, 记为 $(x_1x_2x_3x_4x_5x_6x_7x_8)$, 则(2) 式可写为: $F(x) = (d_1(x), d_2(x), d_3(x), d_4(x), d_5(x), d_6(x), d_7(x), d_8(x))$, 其中

$$d_1(x) = x_2; \quad d_2(x) = x_1 \dot{\vee} x_2; \quad d_3(x) = x_2 \dot{\vee} x_6;$$

$$d_4(x) = x_1 \dot{\vee} x_2 \dot{\vee} x_7 \dot{\vee} x_6x_7 \dot{\vee} x_6x_8; d_5(x) = x_6x_7 \dot{\vee} x_6x_8 \dot{\vee} x_8;$$

$$d_6(x) = x_4; d_7(x) = x_3 \dot{\vee} x_5; d_8(x) = x_3$$

经验证, $F(x)$ 为 $GF(2)^8$ 上的布尔置换。

3 结束语

定理 1 给出的构造方法, 可以从简单的具有较少自变量的布尔置换构造出很多的具有较多自变量的布尔置换, 而且由此方法可以得到任意阶的高阶布尔置换。因此, 本文给出的布尔置换构造方法, 对布尔置换的构造具有一定的理论和应用价值。

参 考 文 献:

[1] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120 – 126.

[2] 武传坤, 王新梅. 非线性置换的构造[J]. 科学通报, 1992, 37(12): 1147 – 1150.

[3] 刑育森, 杨义先. 密码体制中布尔置换的构造与计数[J]. 通信学报, 1998, 19(3): 74 – 76.

[4] 陈鲁生, 符方伟, 沈世镒. 关于密码体制中布尔置换的构造[J]. 工程数学学报, 2002, 19(2): 23 – 30.

[5] 温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000.