第 22 卷 第 1 期 电 子 科 学 学 刊 Vol.22 No.1
2000 年 1 月 JOURNAL OF ELECTRONICS Jan. 2000

正交组的差分分布表的特征 [1]

冯登国

(中国科学院软件所信息安全技术工程研究中心 北京 100080)

摘 要 一个正交组是否可通过它的的差分分布表来刻画是一个至今未解决的问题. 本文解决了这个问题.

关键词 正交组, 差分分布表, S-盒

中图号 TN918.1

1 引 言

差分分析方法是分析分组密码的一种比较流行的方法 [1] , 自从这种方法提出以后, 人们就着手研究和构造对差分分析免疫的 S-盒 [2] , 并提出了衡量一个 S-盒抵抗差分分析能力强弱的指标—— δ-差分均匀度. 正交组是用于设计分组密码的一种重要资源, 研究它的密码学特性具有十分重要的应用价值. 本文刻画了正交组的差分分布表的特征. 文中限制在二元域 F_2 上讨论, 当然, 这些结果对一般的有限域亦成立.

2 正交组的差分分布表的特征

定义 1 设 n 和 m 是两个正整数, $n \geq m$, $F(x) = (f_1(x), f_2(x), \cdots, f_m(x)) : F_2^n \to F_2^m$, 如果对所有的 $a \in F_2^m$, 都有 $\#\{x \in F_2^n : F(x) = a\} = 2^{n-m}$, 那么我们就称 $F(x)$ 是正交的 (又称 $F(x)$ 是一个多输出平衡函数) . 特别地, 当 $n = m$ 时, 称 $F(x)$ 是一个置换. 当 $m = 1$ 时, 称 $F(x)$ 是一个平衡 (布尔) 函数. 其中 $\#\{*\}$ 表示集合 $\{*\}$ 中元素的个数.

定义 2 设 n 和 m 是两个正整数, $n \geq m, F(x) = (f_1(x), f_2(x), \cdots, f_m(x)) : F_2^n \to F_2^m$, 我们将 $\delta_F = \max\limits_{\substack{\beta \in F_2^m \\ 0 \neq \alpha \in F_2^n}} \#\{x \in F_2^n : F(x \oplus \alpha) \oplus F(x) = \beta\}$ 称为 $F(x)$ 的 δ-差分均匀度.

显然, 对任何 $F(x) : F_2^n \to F_2^m$, 都有 $\delta_F \geq 2^{n-m}$, 2^{n-m} 是 δ_F 的一个平凡下界. δ_F 越小, F 抵抗差分攻击的能力就越强. 反之, δ_F 越大, F 抵抗差分攻击的能力就越弱.

定义 3 设 n 和 m 是两个正整数, $n \geq m, F(x) = (f_1(x), f_2(x), \cdots, f_m(x)) : F_2^n \to F_2^m$, 我们称 $S_{(F)}(u, v) = \frac{1}{2^n} \sum_{x \in F_2^n} (-1)^{F(x) \cdot u + v \cdot x}$, $u \in F_2^m$, $v \in F_2^n$, 为 $F(x)$ 的 Walsh 谱. 其中 $v \cdot x$ 表示 v 与 x 的点积.

定义 4 设 n 和 m 是两个正整数, $n \geq m, F(x) = (f_1(x), f_2(x), \cdots, f_m(x)) : F_2^n \to F_2^m$, 定义一个矩阵 A_F , A_F 的第 α 行第 β 列的元素是 $\delta_F(\alpha, \beta)$, 它是一个 2×2 阶矩阵, 我们将该矩阵称为 $F(x)$ 的差分分布表.

易知, A_F 的每一行的元素之和都等于 2^n . 第一行总是 $(2^n, 0, 0, \cdots, 0)$.

引理 1 设 n 和 m 是两个正整数, $n \geq m, F(x) = (f_1(x), f_2(x), \cdots, f_m(x)) : F_2^n \to F_2^m$, 若记 $\delta_F(\alpha, \beta) = \#\{x \in F_2^n : F(x \oplus \alpha) \oplus F(x) = \beta\}$, 则

$$\delta_F(\alpha, \beta) = 2^{n-m} \sum_{\substack{u \in F_2^m \\ v \in F_2^n}} S_{(F)}^2(u, v) (-1)^{u \cdot \beta + v \cdot \alpha}.$$

引理 1 可由 $\delta_F(\alpha, \beta)$ 的定义及定义 3 推出.

[1] 1998-02-11 收到, 1999-04-15 定稿

引理 2　设 n 和 m 是两个正整数，$n \geq m$, $F(x) = (f_1(x), f_2(x), \cdots, f_m(x))$：$F_2^n \to F_2^m$，若记 $\delta_F(\alpha, \beta) = \#\{x \in F_2^n : F(x \oplus \alpha) \oplus F(x) = \beta\}$，则

$$S_{(F)}^2(u, v) = \frac{1}{2^{2n}} \sum_{\substack{\beta \in F_2^m \\ \alpha \in F_2^n}} \delta_F(\alpha, \beta)(-1)^{u \cdot \beta + v \cdot \alpha}.$$

引理 2 可由引理 1 推出.

引理 3　设 n 和 m 是两个正整数，$n \geq m$, $F(x) = (f_1(x), f_2(x), \cdots, f_m(x))$：$F_2^n \to F_2^m$，则 $F(x)$ 是正交的，当且仅当 $f_1(x), f_2(x), \cdots, f_m(x)$ 的所有非零线性组合都是平衡布尔函数，当且仅当对任何 $u \in F_2^m$，$u \neq 0$，有 $S_{(F)}(u, 0) = 0$.

引理 3 是一个已有结果.

定理　设 n 和 m 是两个正整数，$n \geq m$, $F(x) = (f_1(x), f_2(x), \cdots, f_m(x))$：$F_2^n \to F_2^m$，则 $F(x)$ 是正交的，当且仅当对任何 $\beta \in F_2^m$，$\sum_{\alpha \in F_2^n} \#\{x \in F_2^n : F(x \oplus \alpha) \oplus F(x) = \beta\} = 2^{2n-m}$.

证明　假定 $F(x)$ 是正交的，则由引理 1 和引理 3 的充分条件立即可推出：对任何 $\beta \in F_2^m$，$\sum_{\alpha \in F_2^n} \delta_F(\alpha, \beta) = \sum_{\alpha \in F_2^n} \#\{x \in F_2^n : F(x \oplus \alpha) \oplus F(x) = \beta\} = 2^{2n-m}$. 反之，假定对任何 $\beta \in F_2^m$，$\sum_{\alpha \in F_2^n} \delta_F(\alpha, \beta) = \sum_{\alpha \in F_2^n} \#\{x \in F_2^n : F(x \oplus \alpha) \oplus F(x) = \beta\} = 2^{2n-m}$，则由引理 2 知，对任何 $u \in F_2^m$，$u \neq 0$，有 $S_{(F)}^2(u, 0) = 0$，即 $S_{(F)}(u, 0) = 0$. 再由引理 3 的充分条件知，$F(x)$ 是正交的.　　证毕

上述定理表明，$F(x)$ 的正交性可以通过它的差分分布表 A_F 来刻画. 也就是说，$F(x)$ 是正交的，当且仅当 $F(x)$ 的差分分布表 A_F 具有如下特征：A_F 的每一列的元素之和都等于一个常数 $C = 2^{2n-m}$. 这一事实在实际应用中是非常重要的.

3 结 束 语

一个函数 $F(x)$：$F_2^n \to F_2^m$ 的差分分布表 A_F 可以反映这个函数的许多密码学特性，比如光滑性，差分均匀性，非线性性等. 本文说明了差分分布表还可以反映一个函数的正交性.

参 考 文 献

[1] Biham E, Shamir A. Differential Cryptanalysis of the Data Encryption Standard. New York: Springer-Verlag, 1993, Chapter 2.

[2] Seberry J, Zhang X M, Zheng Y. Systematic generation of cryptographically robust S-boxes, In Proceedings of the first ACM Conference on Computer and Communications Security, New York: 1993, 172–182.

CHARACTERIZATION OF THE DIFFERENCE DISTRIBUTION TABLE OF OTHOGONAL SYSTEM

Feng Dengguo

(*Engineering Research Center for Information Security Technology,*

Institute of Software, Chinese Academy of Sciences, Beijing 100039)

Abstract　It is an open problem whether a orthogonal system is characterized by its difference distribution table. The problem is solved in this paper.

Key words　Orthogonal system, Difference distribution table, S-box

冯登国：　男，1965 年生，研究员，主要从事信息安全理论和技术以及纠错编码方面的教学和科研工作.