布尔函数的基本概念

满足 且 的全体元素的集合称之为 的开集，记为 ；

满足 且 的全体元素的集合则称之为 的闭集，记为 。

集合 的基数称为 的汉明重量，记为 。

如果一个 元布尔函数 满足 ，则称该函数为平衡的，即意味着:

用 来表示布尔函数 和 的汉明距离，则它也即为布尔函数 的汉明重量。

汉明距离：它是一种概念。即两个等长的字符串对应位置上的字符不同的个数。

汉明重量：它是一种特殊的汉明距离。指一个字符串与一个等长的“零”字符串的汉明距离，即一个字符串中非零的字符个数。

布尔函数 的 变换，也称 谱，是研究布尔函数密码学性质最重要的数学工具之一。 谱是 上的一个实值函数，其定义为：

这里“.”表示两个 元向量的点乘，即 ，其中，。其逆变换为：

布尔函数的 谱的基本性质：

1.

2.（Parseval 等式）