**3 中组件的一些基本性质**

**3.1 的性质**

算法的定义在有限域上，其特征多项式是次有限域上的本原多项式。因此生成的上的非零序列为序列，其周期为。令 是由生成的上的非零序列。注意可以表示为：

对于时，其中是有限域的一组基。 我们称从导出的序列 作为第个坐标序列。那么由特征多项式性质可知，生成的每个序列坐标序列都是域上的一个序列，其特征多项式是上次的本原多项式。并且容易验证生成的非零序列的每个坐标序列的特征多项式的非零系数的个数为。

此外，在选择多项式时，为了更好地抵抗线性区分攻击和快速相关攻击，我们尽可能避免具有低度低权重的倍数，其所有非零系数均为。

**3.2 函数的性质**

非线性函数包含一个的内存单元并使用盒作为构建块。本身对线性区分攻击和快速相关攻击有很好的抵抗能力。简单的计算表明，关于的以下性质成立。

**性质 1** 盒的代数次数、非线性度、差分均匀度和代数免疫度分别为。

**性质 2** 当我们把看作在矢量空间上的一个变换，它的线性分支数等于。

概率为的线性近似的偏差定义为。那么下面两个性质也容易证明。

**性质 3** 轮函数的任意线性近似的偏差为零。

**性质 4** 轮函数的任意线性近似的活跃盒的数量至少为 。

**3.3 结构的性质**

盒

**性质 5** 盒的代数次数、非线性度、差分均匀度和代数免疫度分别为。

**定义 1** 设是有限域上的映射，其中包含个元素，其中为正整数。如果和都是上的置换，则 被称为正态置换。

**性质 6** 盒是上的正形置换。

的平衡性

设两个随机变量和独立且均匀分布，为描述简单，将和 称为随机变量。

**定义 2** 假设变量和的输入 是时刻上的成对随机变量。用表示在时间的输出。然后被称为平衡的，且,我们有

**性质 7** 是平衡的，当且仅当盒是上的正态置换。

首先证明充分性。令且。那么和都是在集合上的随机变量。由于，并且和都是随机变量，容易看出对于任意给定的 ，有。现在我们考虑记忆单元的更新。 我们注意到在时刻只更新了两个单元和，因此我们只需要证明

对于任意给定的，下面我们考虑两种情况。

1.。

由于，且与是相互独立的，其中是一个盒置换，因此我们有

同理，由于，注意和也是独立的，同理可得。

2.。

在这种情况下，只更新了一个单位。注意

且是一个正形置换，因此我们有

其次证明必要性。 在上面我们已经证明了

根据的平衡性质，我们有。由于

因此对于任意，我们有。因此，方程对于任意有且只有一个解，即 是一个置换。 所以是一个正形置换。

□