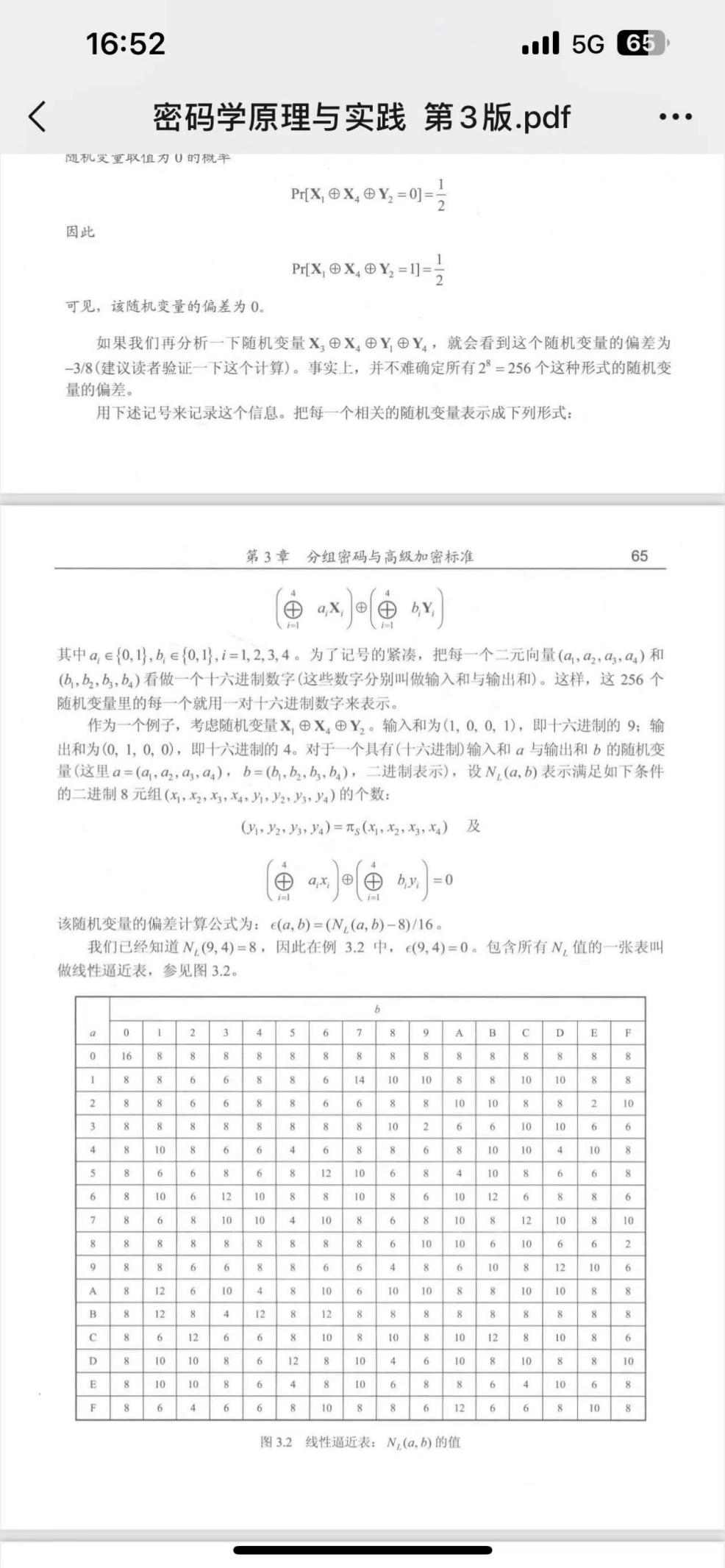
AES Sbox线性逼近表分析报告

2112155 梁婧涵

1. 线性逼近表：线性逼近表是一种用于分析加密算法中S-Box的工具，它用于描述S-Box中输入和输出之间的线性关系。它包括S-Box中所有输入差异与差分对的组合，并对每个组合计算对应的线性逼近概率。



1. AES Sbox线性逼近表生成原理与思路：AES S-Box的线性逼近表是一个256x256的矩阵，其中每个元素表示S-Box中两个输入字节和两个输出字节之间的线性关系。

（1）首先，需要确定一个线性逼近的差分对（linear approximation differential pair），也称为一个特征对（characteristic pair）。这个差分对是指在S-Box中两个输入字节和两个输出字节之间的线性关系。常见的线性逼近差分对是（0x01，0x8c），即两个输入字节的差异（即XOR）与两个输出字节的差异之间的线性关系。

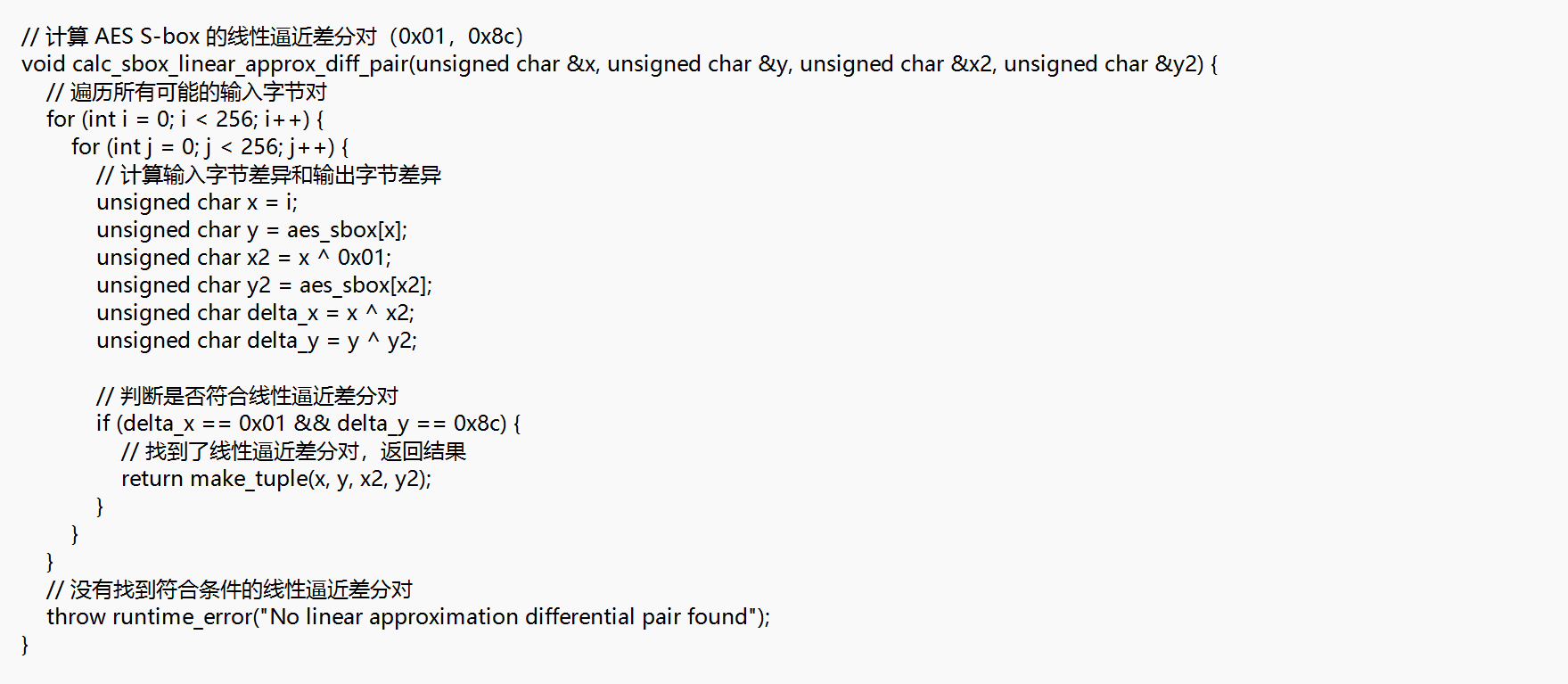
（2）接下来，需要枚举所有可能的S-Box输入差异，以及它们与差分对的组合。可以使用布尔函数来表示S-Box的替换表，并计算每个输入差异与差分对的乘积，以确定线性逼近关系的强度。

（3）对于每个输入差异和差分对组合，需要计算线性逼近关系的统计概率。这可以通过对多个随机选择的输入对进行计数来完成，这些输入对在其中一个对中具有特定的输入差异和差分对，而在另一个对中则没有。这个统计概率可以用一个数值来表示，并作为线性逼近表中相应元素的值。

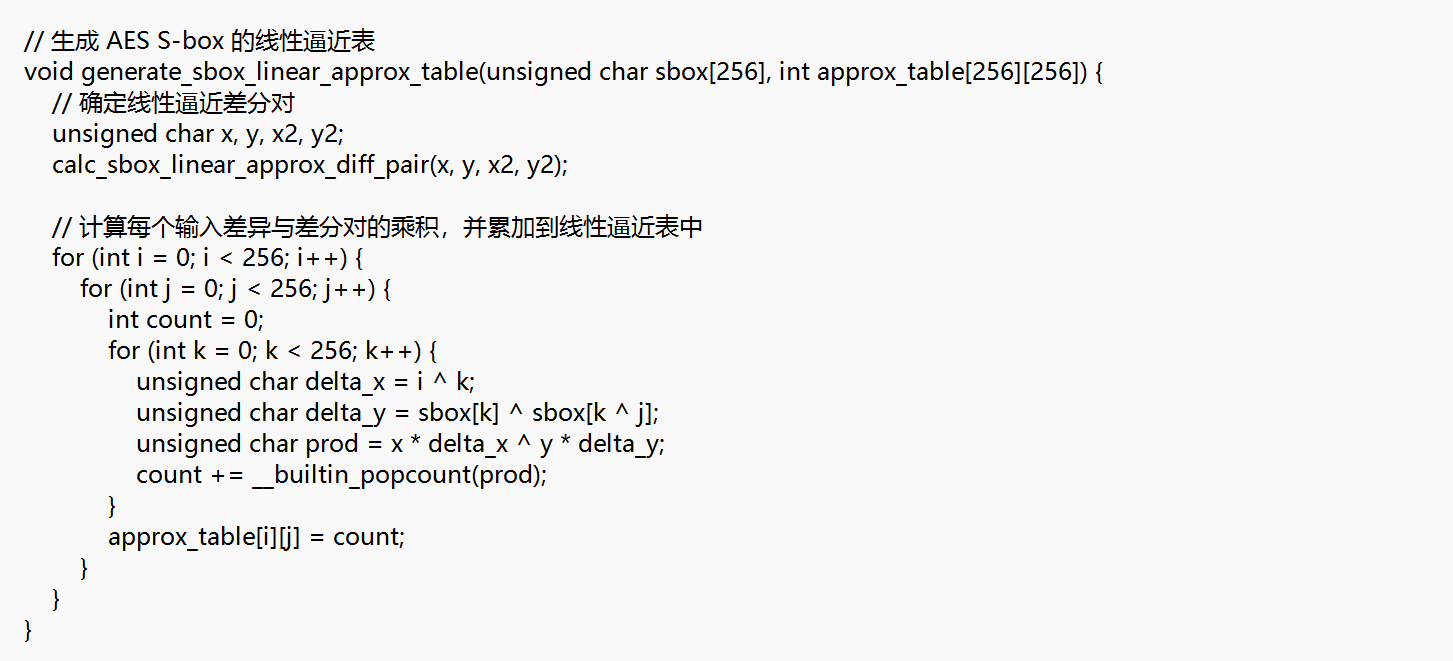
（4）重复以上步骤，直到枚举了所有可能的输入差异和差分对组合。最终得到的结果是一个256x256的矩阵，其中每个元素表示S-Box中两个输入字节和两个输出字节之间的线性关系。

3.代码实现：

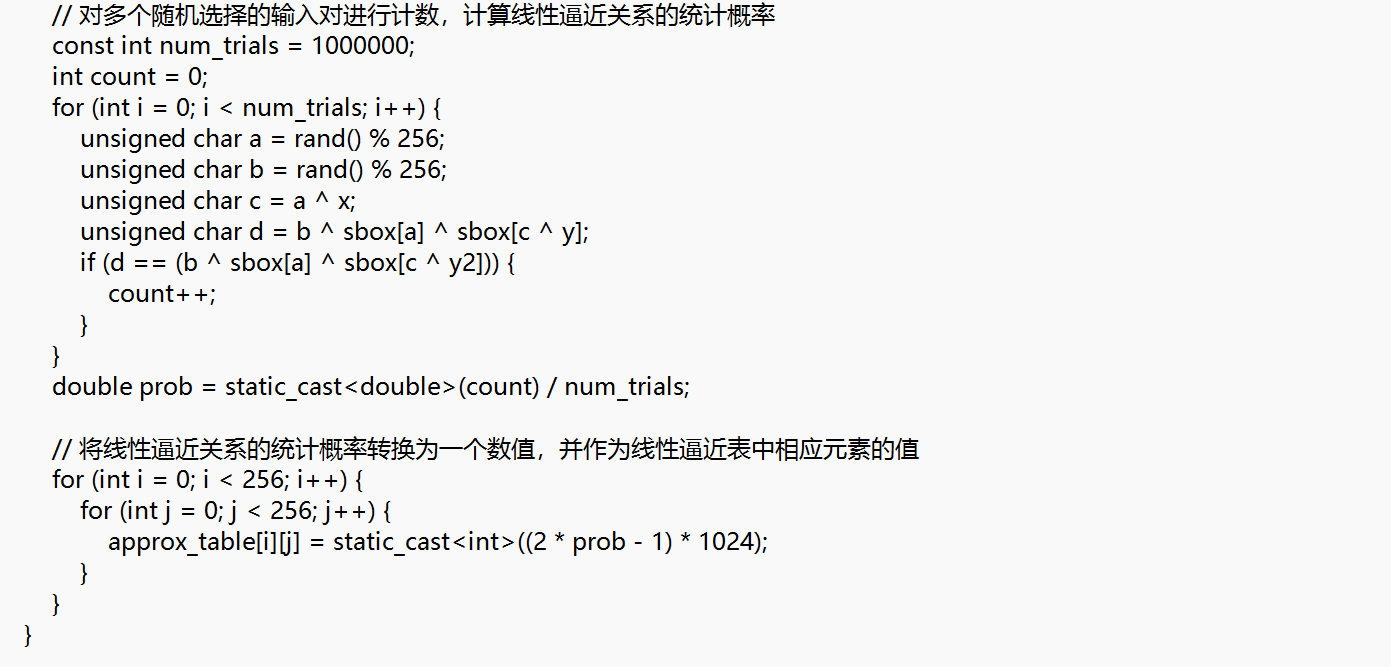
（1）使用两层循环来遍历 AES S-box 的所有输入字节对，并计算它们的输出字节以及输入字节之间的差异。如果找到了符合条件的线性逼近差分对，函数会返回这个差分对的四个字节值。如果没有找到符合条件的差分对，函数会抛出一个运行时错误。注意到这个函数返回的结果是一个四元组，包含了两个输入字节和两个输出字节的值。



1. 函数使用了三层循环来遍历所有可能的输入差异、差分对和S-Box替换表的值，并计算它们之间的乘积。乘积的计算使用了位运算和内置函数 \_\_builtin，\_popcount，后者可以计算一个整数中二进制位为1的个数。最终，函数会将每个输入差异与差分对的乘积的1的个数累加到一个256x256的数组中，这个数组就是AES S-box的线性逼近表。



1. 计算线性逼近关系的统计概率，可以对多个随机选择的输入对进行计数。对于一个给定的输入差异和差分对组合，如果它们的线性逼近关系成立，那么这些输入对中一半以上应该满足这个差分对的条件。函数在计算线性逼近表元素值时，使用了一个固定的随机数种子，以便多次运行得到相同的结果。它使用了一个循环，随机选择了多个输入对，并计算它们是否满足给定的输入差异和差分对组合。如果满足，则将计数器加1。最后，计算线性逼近关系的统计概率，并将其转换为一个数值，并作为线性逼近表中相应元素的值。



4.结果：生成256x256的线性逼近表