**飞比-樱花-有家动态密码生成运算说明**

**一、加密因子的概述：**

1、用户种子的概念：是用于区分保洁、用户等不同类型用户的唯一数值，由服务端单独下发给门锁，门锁需要保存；种子另区分1次性用户种子、2次性用户种子、3次性用户种子……n次性用户种子，服务器下发时会指明。

2、秘钥Key来源：“用户种子” + “IEEE地址”作为秘钥key。

3、原始密码Source 来源：“当天有效的时间 ” 作为原始密码Source 。

4、将”秘钥” 与 “原始密码” 以xxTea方式进行加密运算，将计算结果的十进制显示方式(低4位)作为“动态密码”的前四位十进制数，“前四位十进制数”与“当天有效的时间段”做混淆运算其得数作为“动态密码”的后四位十进制数。

**二、动态密码生成举例：**

例：生成保洁啊姨A其用户种子为AB CD EF 00 12 34，于12：00-14：00之间有效的动态密码xxxx xxxx，。

保洁啊姨A的用户种子：AB CD EF 00 12 34

读取门锁IEEE为：00 15 8D 00 02 A9 0F EE (低三字节为：A9 0F EE)

即秘钥key为: 第一步 “用户种子” + “IEEE” = AB CD EF 00 12 34 A9 0F EE

第二步 修改 “用户种子” ，用“IEEE”对其进行异或运算，如下所示

key[0] ^= key[6];

key[1] ^= key[7];

key[2] ^= key[8];

原始密码Source：由有效时间段12：00-13：00得00 12 13

使用秘钥key，对原始密码Source 进行xxTea加密，进行运算后Source加密成为0x8B 09 9C (十进制表示为9,111,964)；将结果低4位1,964作为“动态密码”的前四位十进制数；运算|1964-1213|=751（混淆运算）作为“动态密码”的后四位十进制数；最后得出的完整8位动态密码为1964 0751。