## 密码分析学

第4次实验：

**内容：**从以下算法中选择一个进行密钥恢复攻击（攻击方法和攻击轮数不限，要有详细分析和推导过程，不要照搬网上他人结果，如果基于他人工作请务必标明引用）。

可以分别给出一个复杂度在230的攻击和一个复杂度较高但优于穷举攻击的分析。

1. uBlock算法
2. Ballet算法
3. SM4算法
4. 提交日期：2023-11-**4**/5

提交资料：实验报告+可读性较好的程序源代码

提交邮箱：3658901621@qq.com

要求同实验一。