## mim密码分析学

第3次实验：

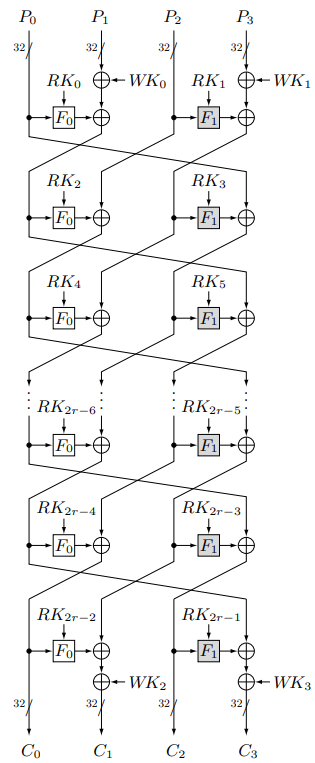
1. 根据分组密码算法CLEFIA-128或杂凑函数Whirlpool算法中分组密码的结构（任选其一即可），利用算法（或手工推导等其他方式）尝试寻找不可能差分。

* 广义feistel结构（CLEFIA）:

Clefia算法描述：<https://www.sony.net/Products/cryptography/clefia/download/>

设和为伪随机置换，和为相互独立的密钥，不考虑和的具体构造。

尝试寻找不可能差分。

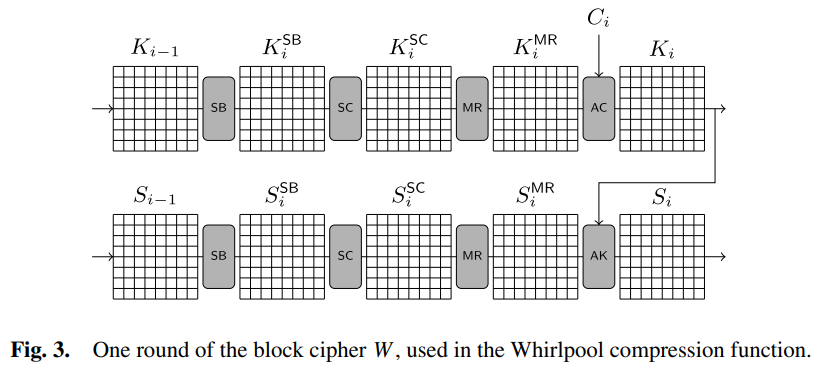


* SPN结构（仅考虑Whirlpool中的分组密码W）:

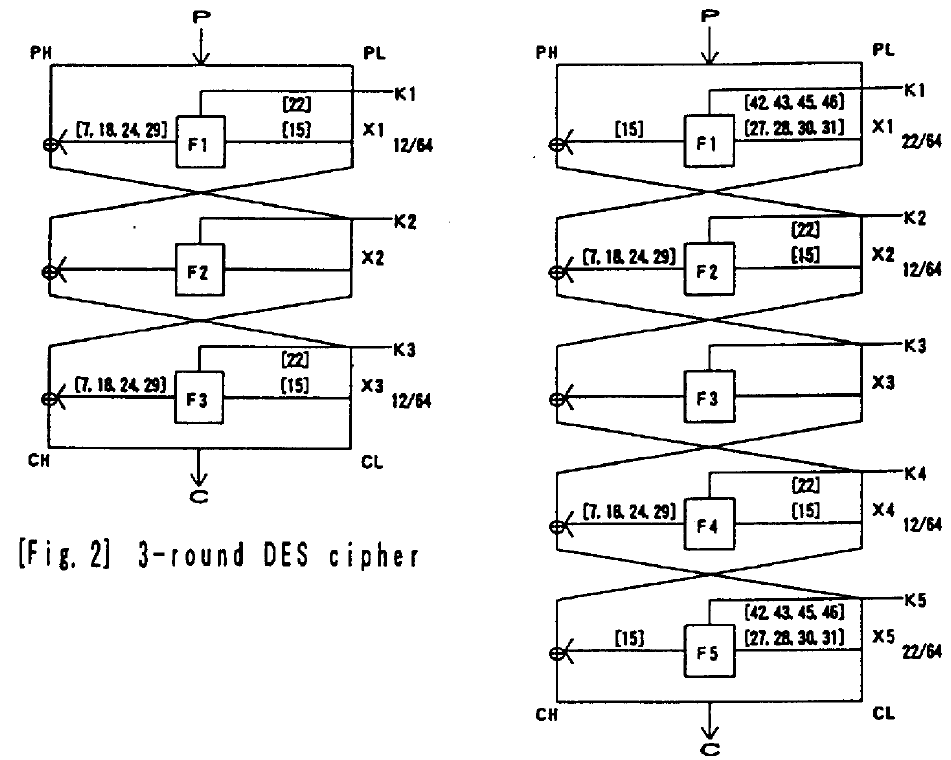
Whirlpool算法描述：<https://link.springer.com/article/10.1007/s00145-013-9166-5>（攻击论文，可参考其中算法描述）

分组密码W采用SPN结构，其一轮运算类似AES，输入为64个字节，设SB为按字节过同一个8进8出的S盒，将S盒看做伪随机置换（双射）；SC为按列的字节循环移位，第*j*列循环下移*j*个字节；MC为行混合运算，分支数为9；AK看做异或常数。

尝试寻找不可能差分。



1. 仿照以下3轮DES算法（左图，不考虑初始IP置换和最后的IP逆置换，最后一轮左右不交换）的迭代线性近似式，结合S盒的线性分布表（任一S盒均可），手动推导一条新的3轮迭代差分路线（与以下示例不同的），并计算相应概率。
2. 在2）新找到的近似式的基础上，仿照右图，构造5轮线性近似式，并计算相应概率。
3. 在3）的基础上，利用Matsui算法2（课上讲），给出6轮DES算法的密钥恢复攻击（**仅恢复第6轮的部分轮密钥即可**），重复100次实验，每次实验任取，测试成功率（可能低于50%）。其中，相应的密文值可通过调用群文件中的可执行程序来实现（1-5组用程序des\_enc1；6-10组用程序des\_enc2；11-15组用程序des\_enc3；16-20组用程序des\_enc4）。



1. 提交日期：2023-10-22

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。