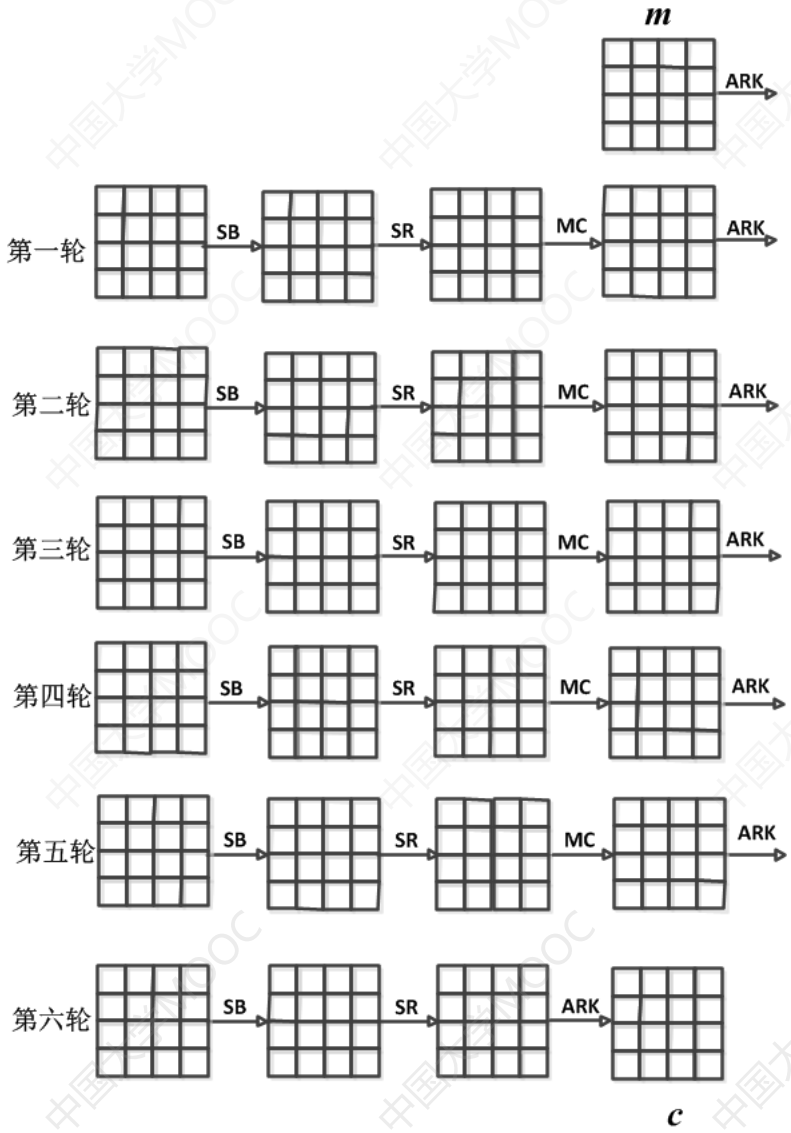
6轮AES-128 的不可能差分攻击

西安邮电大学

2021/6/20

6轮AES的加密流程



状态

0	4	8	12	0
1	5	9	13	1
2	6	10	14	2
3	7	11	15	3
0	1	2	3	

不可能差分攻击

- 思想：基于寻找到的不可能差分特征，排除那些导致满足该特征的候选密钥，最终恢复出正确密钥的一种攻击方法。
- 其中：不可能差分特征↔概率为0的差分特征

6轮AES-128的不可能差分攻击

- 攻击步骤

第一步 构造4轮AES-128的不可能差分特征。

第二步 通过排除错误密钥进行6轮AES-128的密钥恢复。

6轮AES-128的不可能差分攻击

- 攻击步骤

第一步 构造4轮AES-128的不可能差分特征。

第二步 通过排除错误密钥进行6轮AES-128的密钥恢复。

- 差分：设x，$x^*\in\{0，1\}^n$，则x和x^*的差分定义为$x\oplus x^*$。

4轮AES-128的不可能差分特征

定理：若给定一个明文对，其差分只有第0个字节为非0，那么经过4轮AES加密之后，密文对的差分在第（3，6，9，12）字节不可能为0。

注意：最后一轮没有MC变换。

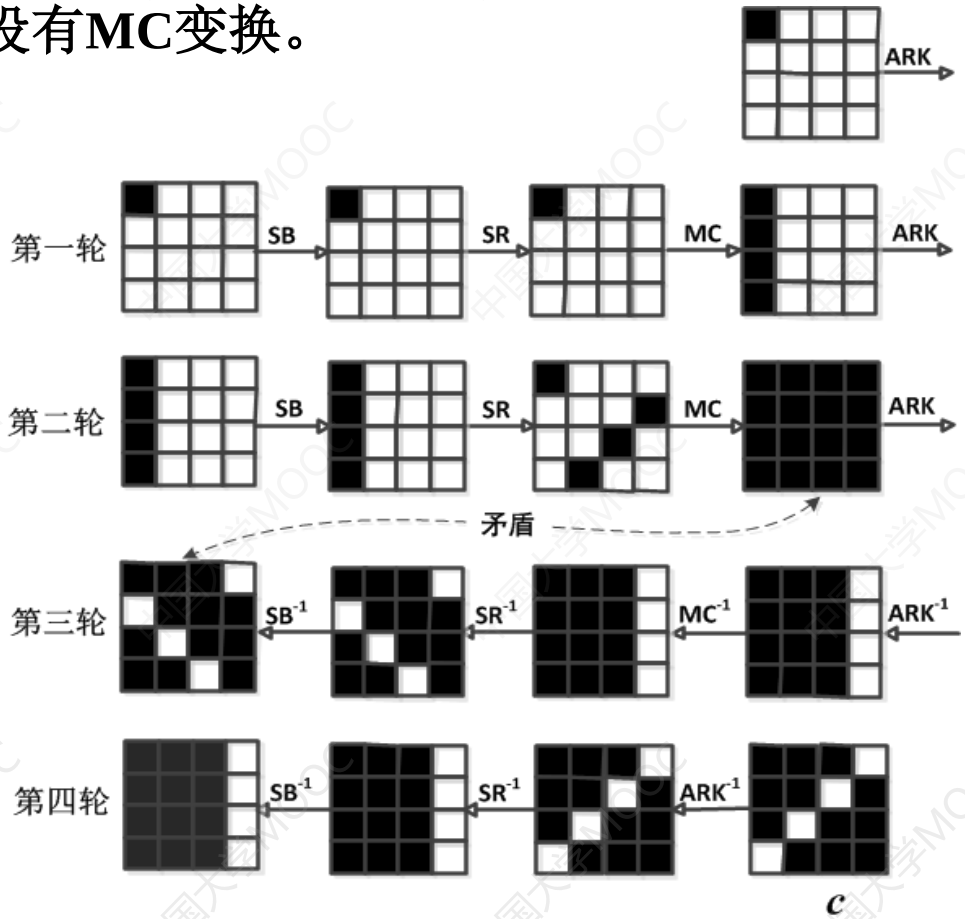


图　4轮AES的不可能差分特征

6轮AES-128的不可能差分攻击

- 攻击步骤

第一步 构造4轮AES-128的不可能差分特征。

第二步 通过排除错误密钥进行6轮AES-128的密钥恢复。

6轮AES的密钥恢复

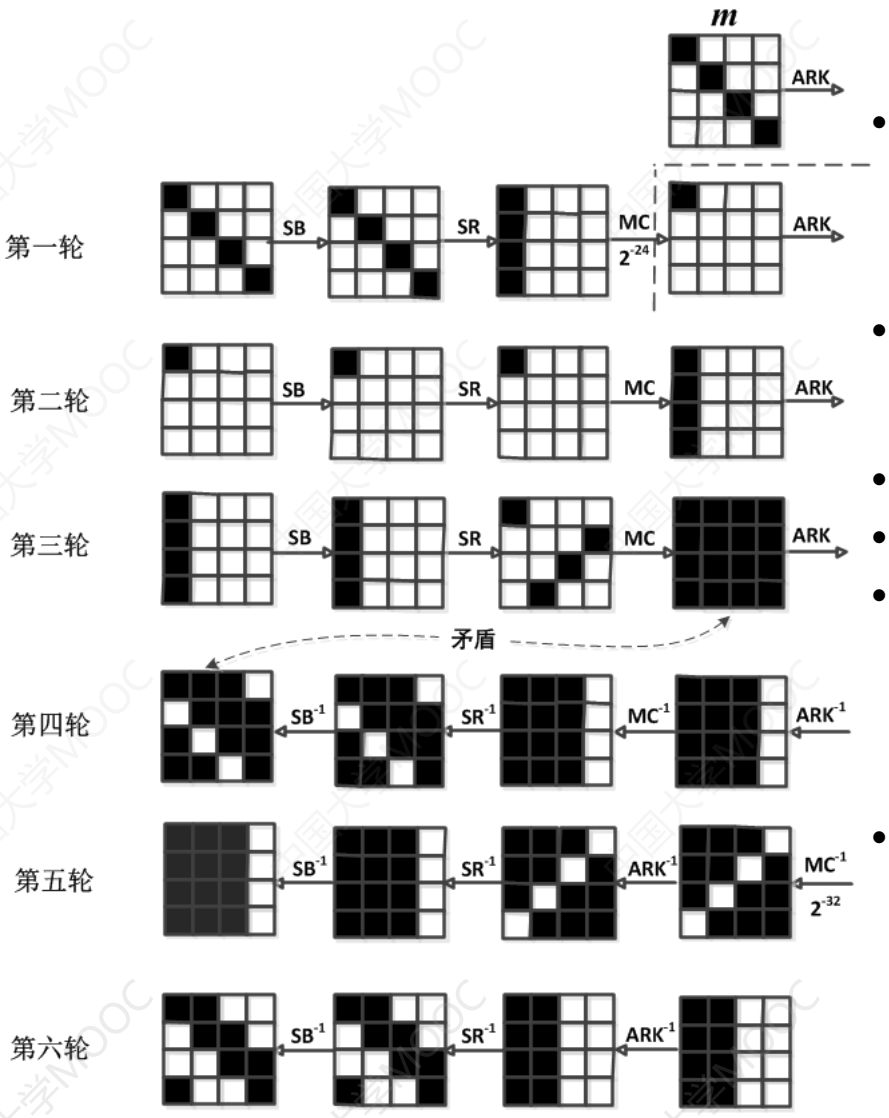


图　6轮AES-128的不可能差分攻击

- **Step1**：定义一种明文结构：明文在主对角线的4个字节取值任意，其余字节取值固定。一种明文结构包含2^{32}个明文，可以形成$2\times2^{32}\times(2^{32}-1)\times1/2\approx2^{63}$个明文对。
- **Step2**：选择$2^{63.5}$个明文结构进行加密，共得到$2^{63.5}\times2^{32}=2^{95.5}$个密文，形成$2^{63.5}\times2^{63}=2^{126.5}$个密文对。保留满足密文对的差分在Col（2，3）为0的对，其余丢弃。剩余
- $2^{126.5}\times2^{-64}=2^{62.5}$个对。
- **Step3**：猜测子密钥k_6中Col（0，1）。对剩余的每个密文对,依次经过ARK^{-1}，SR^{-1}，BS^{-1}和MC^{-1}，此时若它们的差分满足在第（3，6，9，12）个字节差分为0，则保留这样的对。剩余$2^{62.5}\times2^{-32}=2^{30.5}$个对。
- **Step4**：猜测白化密钥k_0中第（0，5，10，15）个字节。对剩余明文对进行部分加密，即依次经过变换ARK，BS，SR，MC。此时，如果存在一个明文对其第0列差分仅仅在第0个字节为非0（概率为2^{-24}），猜测的密钥是错误的，排除掉。
- **Step5**：穷举搜索k_6中Col（2，3）的子密钥获得最终的主密钥。

6轮AES-128的密钥恢复

Step3的时间复杂度：

$2^{64}\times 2\times 2^{62.5}\times 1/2\times 1/6\approx 2^{123.9}$（6轮AES-128加密）

Step4的时间复杂度：

$$2^{64}\times 2^{32}\times 2\times\{1+(1-2^{-24})+\cdots(1-2^{-24})^{i-1}+\cdots(1-2^{-24})^{2^{30.5}-1}\}\times 1/4\times 1/6$$

$\approx 2^{116.4}$（6轮AES-128加密）

Step4剩余错误子密钥$k_6[col(0,1)]\|k_0[0,5,10,15]$的概率：

$$2^{64}\times 2^{32}\times(1-2^{-24})^{2^{30.5}}$$

$$\approx 2^{64}\times 2^{32}\times e^{-2^{6.5}}$$

$$=2^{-34.6}$$

Step5的时间复杂度：

$1\times 2^{64}=2^{64}$（6轮AES-128加密）

6轮AES-128不可能差分攻击

- 结论： 6轮AES-128理论上被攻破

  数据复杂度：$2^{95.5}$个选择明文

  时间复杂度： $2^{123.9}$个6轮AES-128的加密

思考

- 改进上述6轮AES-128的不可能差分攻击，降低攻击的复杂度。
- 进行7轮AES-128的不可能差分攻击。