第 2 章：分组密码体制

2.3 DES 的安全性

赵俊舟

junzhou.zhao@xjtu.edu.cn

2025 年 3 月 5 日

目录

目录

密钥长度问题

- 56 位密钥有 $2^{56} \approx 7.2 \times 10^{16} = 7.2$ 亿亿之多。
- 穷举搜索（brute force search）似乎很困难，20 世纪 70 年代估计要 $1000 \sim 2000$ 年。
- 技术进步使穷举搜索成为可能：
- 1997 年 1 月 29 日，RSA 公司发起破译 RC4、RC5、MD2、MD5，以及 DES 的活动，破译 DES 奖励 $10,000$ 美金。明文是：Strong cryptography makes the world a safer place。结果仅搜索了 24.6% 的密钥空间便得到结果，耗时 96 天。
- 1998 年在一台专用机（“DES 破译机”）上只要三天时间即可！
- 1999 年在超级计算机上只要 22 小时！
- 现在只需要 10 小时！

DES 的内部结构问题

- 密码分析者有可能利用 DES 算法本身的特征进行攻击。
- S 盒的设计标准被列为官方机密，并没有公开。
- NSA 有可能利用这些内部机密在没有密钥的情况下解密。
- 但是迄今为止并没有发现 S 盒存在致命弱点。

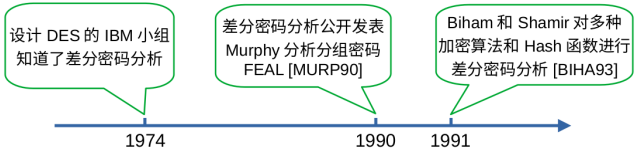
计时攻击

- 通过观察算法对多种密文解密所需的时间，来获取关于密钥或明文的信息。
- 计时攻击所利用的信息是加密或解密算法对于不同输入所花的时间有着细微的差别。
- 例如利用计时攻击分析密钥的汉明权重，即二进制串中 1 的个数。
- 目前为止，计时攻击还不可能成功攻击 DES。

目录

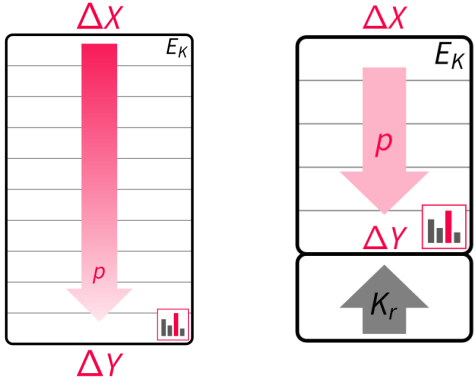
差分密码分析（Differential Cryptanalysis）

- 差分密码分析属于选择明文攻击。通过分析明文对的差分（即异或）对结果密文对的差分的影响，确定最有可能的密钥。
- 1990 年，Murphy、Biham 和 Shamir 首次提出用差分密码分析攻击分组密码和散列函数。
- 研究表明，若有 2^{47} 个选择明文，用差分分析就可以在 2^{47} 次加密运算内成功攻击 DES。但是要拥有 2^{47} 个选择明文的条件使得这种方法只具有理论上的意义。
- DES 在设计之初已经考虑了抵抗差分密码分析。在设计 S 盒和置换 P 时已经做了充分考虑。

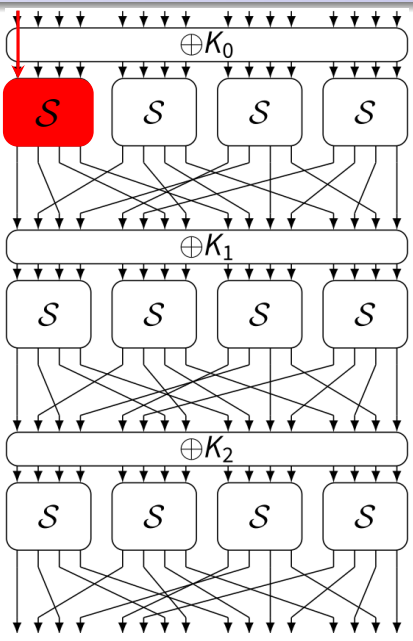


差分密码分析的主要思想

- 考虑输入差分为 ΔX 的一对明文；
- 跟踪这对明文经过每轮处理后的变化；
- 根据输出的差分推测每一轮处理所使用的子密钥。



差分密码分析的主要思想

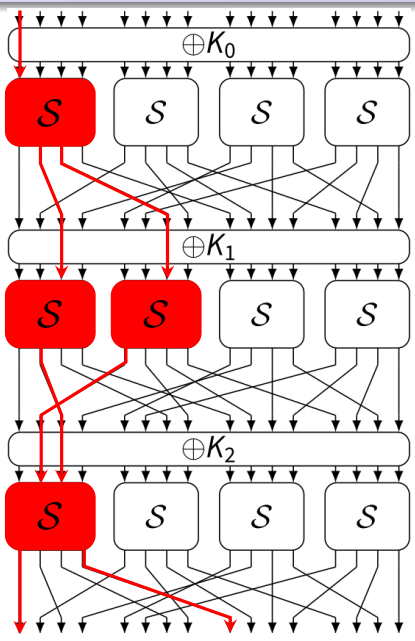


- 将 DES 简化为左图所示的运算，只包含 DES 的关键运算。
- 一次轮函数运算可以看作输入与该轮子密钥异或后再经过 S 盒替换。
- 输入异或不受子密钥影响：考虑一对输入 x 和 x'，则

$$(x \oplus k) \oplus (x' \oplus k) = x \oplus x'$$

- 当差分输入到一个 S 盒时，可以利用 S 盒的差分特性进行分析。

差分密码分析的主要思想

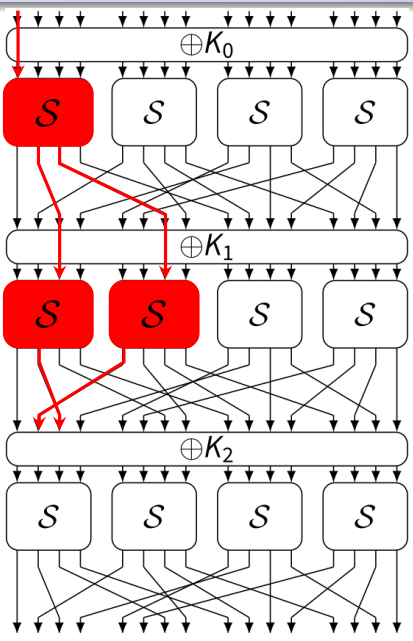


- 考虑具有相同输入差分的所有输入对：$\{(x, x') | x \oplus x' = \delta\}$
- 统计 S 盒相应的输出对的差分，会发现输出差分的分布往往不均匀。
- 例如，当输入差分为 1011 时，S_1 盒的输出差分分布为

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2

- 从而可以计算出从某个输入差分产生某个输出差分的概率。

差分密码分析的攻击过程



- 搜集尽可能多的明密文对 $(x, y), (x', y')$ 且满足 $x \oplus x' = \delta$；
- 对于每对输入明文，计算出倒数第二轮的输出差分及其对应的传递概率；
- 枚举最后一轮的所有可能密钥，对于每对输出密文用密钥解密，得到最后一轮的输入对；
- 若该输入对的差分等于上一步计算出的输出差分，则该密钥计数加一；
- 根据每个密钥的计数值，输出计数值最大的密钥为该轮的子密钥。

线性密码分析 I

- 1993 年提出的一种统计攻击方法，通过寻找 DES 变换的线性近似来进行攻击。
- 可以在有 2^{43} 个已知明文的情况下破译 DES 密钥，但仍然只具有理论意义。
- 令明文分组为 $P[1], \ldots, P[n]$，密文分组为 $C[1], \ldots, C[n]$，密钥为 $K[1], \ldots, K[m]$。定义 $A[i, j, \ldots, k] \triangleq A[i] \oplus A[j] \oplus \ldots \oplus A[k]$。
- 线性密码分析的目标是找到如下有效线性方程：

$$P[\alpha_1, \alpha_2, \ldots, \alpha_a] \oplus C[\beta_1, \beta_2, \ldots, \beta_b] = K[\gamma_1, \gamma_2, \ldots, \gamma_c]$$

其中 $1 \leq a, b \leq n, 1 \leq c \leq m, \alpha, \beta$ 和 γ 等表示固定的唯一的比特位置。

线性密码分析 II

- 要求方程以概率 $p \neq 0.5$ 成立，p 离 0.5 越远，方程越有效。
- 对于大量的明文密文对，计算方程左边的值，如果结果中有一半以上为 0，则假定 $K[\gamma_1, \gamma_2, \ldots, \gamma_c] = 0$；如果大多为 1，则假定 $K[\gamma_1, \gamma_2, \ldots, \gamma_c] = 1$。

目录

S 盒的设计准则：增加扰乱性

- 输出比特不应太接近输入比特的一个线性函数；
- 每一行应该包括所有 16 种比特组合；
- 两个输入相差一个比特，输出必须相差两个比特；
- 如果两个输入刚好在两个中间比特上不同，输出必须在至少两个比特上不同；
- 两个输入前两位不同而最后两位相同，两个输出必须不同；
- 具有非零 6 比特差值的输入，32 对中有不超过 8 对输出相同。

置换 P 的设计准则：增加扩散性

- 第 i 次循环时每个 S 盒输出的四个比特被分布开，以便其中两个影响下一循环的中间比特，两个影响两端的比特；
- 每个 S 盒输出的四个比特影响下一循环的 6 个不同的 S 盒，并且任何两个都不会影响同一个 S 盒；
- 如果 S_j 的一个输出比特影响下一循环 S_k 的中间比特，则 S_k 的一个输出比特就不能影响 S_j 的一个中间比特。

其他设计准则

- 迭代轮数：迭代次数越多则进行密码分析的难度就越大，选择准则是要使已知的密码分析工作量大于简单的穷举密钥搜索的工作量。
- 轮函数 F：提供扰乱作用，要求强非线性，良好的雪崩性质。
- 密钥扩展算法：选择子密钥时要使得推测各子密钥和由此推出主密钥难度尽可能大，保证密钥/密文的严格雪崩效应准则和位独立准则。

小结

1. DES 加密强度
2. 差分分析和线性分析
3. 分组密码的设计原理