



# 现代密码学

## 第十九讲 Feistel密码结构

信息与软件工程学院



## 第十九讲 Feistel结构

---



## Feistel密码的思想

- **乘积密码**指顺序地执行两个或多个基本密码系统，使得最后结果的密码强度高于每个基本密码系统产生的结果。
- Feistel还提出了实现代换和置换的方法。其思想实际上是Shannon提出的利用乘积密码实现混淆和扩散思想的具体应用。

## Feistel密码实现的参数

Feistel网络的实现与以下参数和特性有关：

- ① 分组大小：分组越大则安全性越高，但加密速度就越慢。 > 安全性↑ 牺牲速度
- ② 密钥大小：密钥越长则安全性越高，但加密速度就越慢。
- ③ 轮数：单轮结构远不足以保证安全性，但多轮结构可提供足够的安全性。  
典型地，轮数取为16。
- ④ 子密钥产生算法：该算法的复杂性越大，则密码分析的困难性就越大。
- ⑤ 轮函数：轮函数的复杂性越大，密码分析的困难性也越大。

## 设计Feistel密码的两个要求

在设计Feistel网络时，还有以下两个方面需要考虑：

- ① **快速的软件实现**：在很多情况中，算法是被镶嵌在应用程序中，因而无法用硬件实现。此时算法的**执行速度**是考虑的关键。
- ② **算法容易分析**：如果算法能被无疑义地解释清楚，就可容易地分析算法抵抗攻击的能力，有助于设计高强度的算法。





## 第十九讲 Feistel结构

---



# Feistel加密结构

分左右,  $n$ 轮迭代, 合并

➤ 输入是分组长为 $2w$ 的明文和一个密钥 $K$ 。将每组明文分成左右两半 $L_0$ 和 $R_0$ , 在进行完 $n$ 轮迭代后, 左右两半再合并到一起以产生密文分组。第 $i$ 轮迭代的输入为前一轮输出的函数:

$$L_i = R_{i-1} \quad \text{左右输出}$$

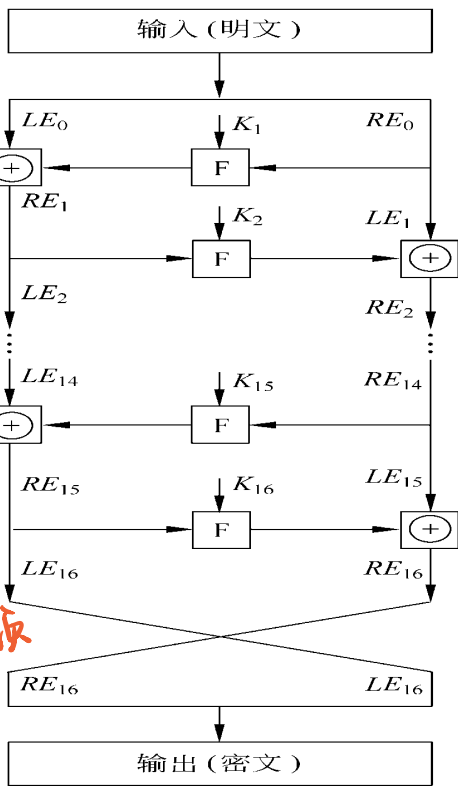
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \quad \text{左右} \oplus \quad \text{左右} \oplus \text{密钥为输入函数}$$

➤ 其中 $K_i$ 是第 $i$ 轮用的子密钥, 由加密密钥 $K$ 得到。一般地, 各轮子密钥彼此不同而且与 $K$ 也不同。

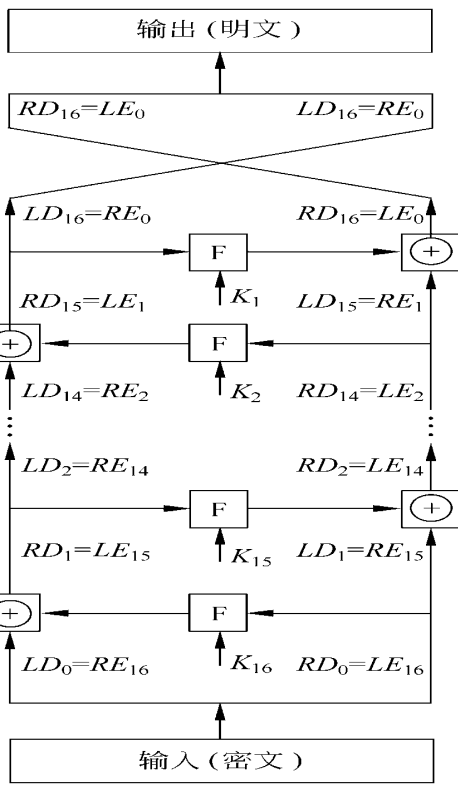
## Feistel解密结构

- Feistel解密过程本质上和加密过程是一样的，算法使用密文作为输入
- 但使用子密钥 $K_i$ 的次序与加密过程相反，即第1轮使用 $K_n$ ，第2轮使用 $K_{n-1}$ ，.....，最后一轮使用 $K_1$ 。这一特性保证了解密和加密可采用同一算法。





最后一轮时  
左右两边再交换  
后输出



Feistel加解密过程

## Feistel密码解密的正确性

在加密过程中:  $LE_{16} = RE_{15}$

(最后一轮)

$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

在解密过程中

(第一轮)  $LD_1 = RD_0 = LE_{16} = RE_{15}$

$$\begin{aligned} RD_1 &= LD_0 \oplus F(RD_0, K_{16}) = RE_{16} \oplus F(RE_{15}, K_{16}) \\ &= [LE_{15} \oplus F(RE_{15}, K_{16})] \oplus F(RE_{15}, K_{16}) \\ &= LE_{15} \end{aligned}$$

所以解密过程第1轮的输出为 $LE_{15} \parallel RE_{15}$ , 等于加密过程第16轮输入左右两半交换后的结果。

## Feistel密码解密的正确性（续）

容易证明这种对应关系在16轮中每轮都成立。一般地，加密过程的第*i*轮有

$$LE_i = RE_{i-1}$$

$$RE_i = LE_{i-1} \oplus F(RE_{i-1}, K_i)$$

因此

$$RE_{i-1} = LE_i$$

$$LE_{i-1} = RE_i \oplus F(RE_{i-1}, K_i) = RE_i \oplus F(LE_i, K_i)$$



感谢聆听!

xynie@uestc.edu.cn