现代密码学

第十八讲 SP网络

信息与软件工程学院

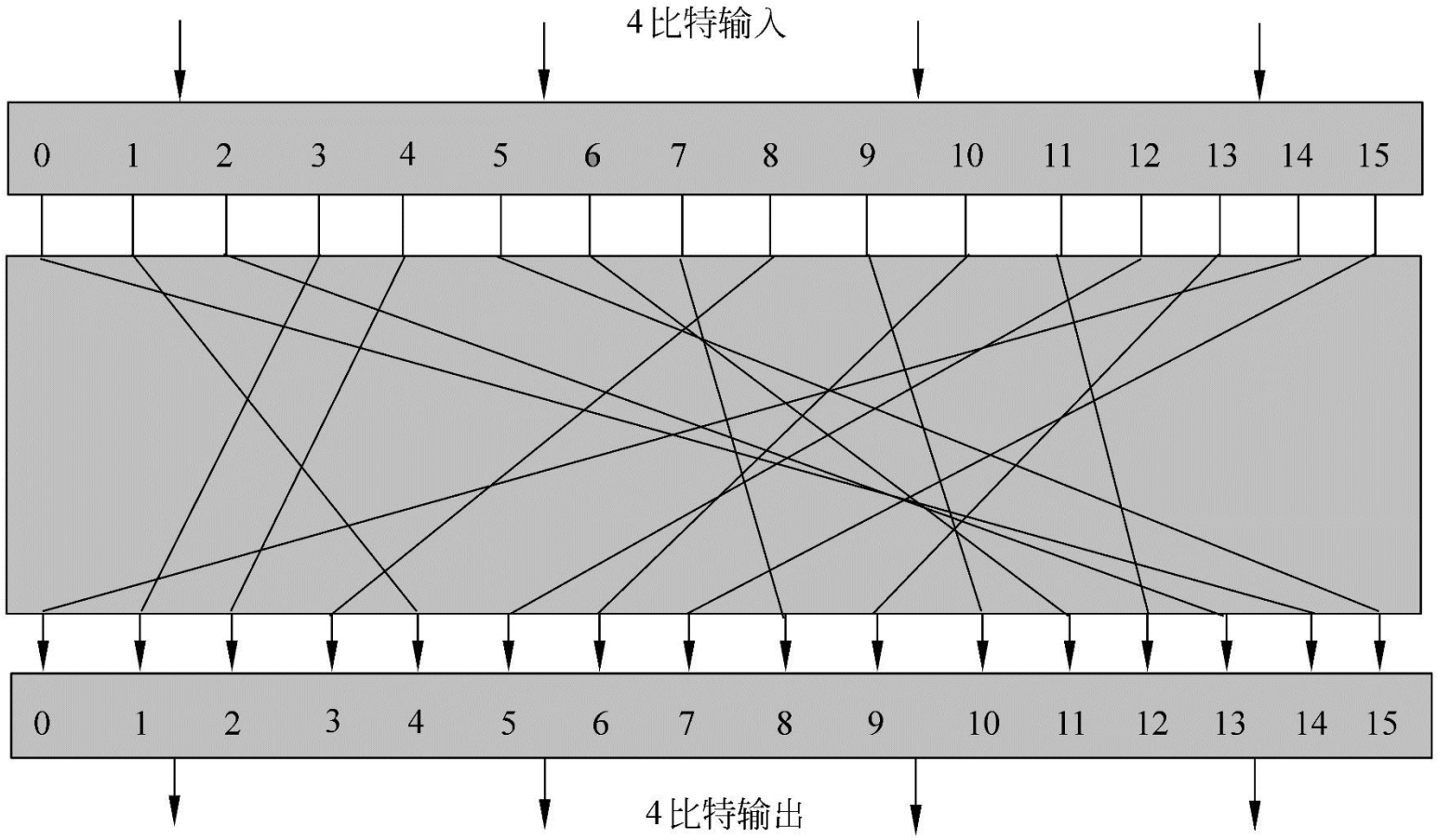
第十八讲 SP网络

代换的定义

•如果明文和密文的分组长都为n比特，则明文的每一个分组都有2^n个可能的取值。为使加密运算可逆（使解密运算可行），明文的每一个分组都应产生惟一的一个密文分组，这样的变换是可逆的，称明文分组到密文分组的可逆变换为代换。

•不同可逆变换的个数有$2^n!$个。

代换结构


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

代换表

明文	密文	明文	密文
0000	1101	1000	1010
0001	0101	1001	1000
0010	0001	1010	1011
0011	0110	1011	1110
0100	1001	1100	0111
0101	1111	1101	0100
0110	0010	1110	1100
0111	0011	1111	0000

正向代换

密文	明文	密文	明文
0000	1111	1000	1001
0001	0010	1001	0100
0010	0110	1010	1000
0011	0111	1011	1010
0100	1101	1100	1110
0101	0001	1101	0000
0110	0011	1110	1011
0111	1100	1111	0101

反向代换

代换的弱点

- 如果分组长度太小，如n=4，系统则等价于古典的代换密码，容易通过对明文的统计分析而被攻破
  - 这个弱点不是代换结构固有的，只是因为分组长度太小
  - 如果分组长度n足够大，而且从明文到密文可有任意可逆的代换，那么明文的统计特性将被隐藏而使以上的攻击不能奏效。

代换的弱点（续）

- 从实现的角度来看，分组长度很大的可逆代换结构是不实际的
  - 仍以4比特的代换表为例，该表定义了n=4时从明文到密文的一个可逆映射，其中第2列是每个明文分组对应的密文分组的值，可用来定义这个可逆映射。
  - 从本质上来说，第2列是从所有可能映射中决定某一特定映射的密钥
  - 密钥需要64比特
- 一般地，对n比特的代换结构，密钥的大小是$n\times 2^n$比特。如对64比特的分组，密钥大小应是$64\times 2^{64}=2^{70}\approx 10^{21}$比特，因此难以处理。

第十八讲 SP网络

- 代换概述
- SP网络

SP网络

- 在Shannon 1949 的文章中，介绍了替代-置换网络的思想即SP网络
  - 这种思想形成了现代密码的基础
  - SP网络是替代-置换乘积密码的现代形式
- SP网络是基于下列两种最基本的密码运算：
  - 替代（ Substitution ）
  - 置换（ Permutation ）

代换网络

- 代换是输入集A到输出A'上的双射变换：

$$f_k: A \rightarrow A'$$

式中，k是控制输入变量，在密码学中则为密钥。

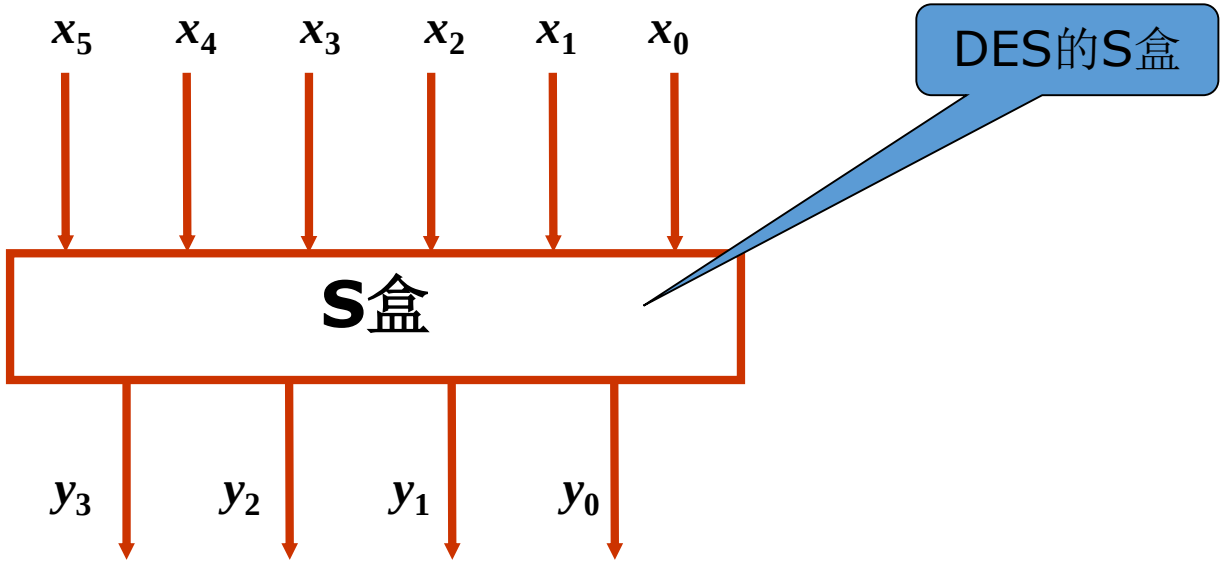
- 实现代换f_k的网络称作代换网络
  - 双射条件保证在给定k下可从密文惟一地恢复出原明文
- 代换f_k的集合：　$S=\{f_k|k\in K\}$
- 如果网络可以实现所有可能的$2^n!$个代换，则称其为全代换网络
  - 全代换网络密钥个数必须满足条件：$\#\{k\}\geq 2^n!$

代换网络

- 密码设计中需要先定义代换集S，而后还需定义解密变换集，即逆代换网络S^{-1}，它以密文y作为输入矢量，其输出为恢复的明文矢量x。
- 要实现全代换网络并不容易。因此实用中常常利用一些简单的基本代换，通过组合实现较复杂的、元素个数较多的代换集。
- 实用密码体制的集合S中的元素个数都远小于$2^n!$。

代换盒(S盒)

在密码设计中，可选$n=r\cdot n_0$，其中r和n_0都为正整数，将设计n个变量的代换网络化为设计r个较小的子代换网络，而每个子代换网络只有n_0个输入变量。称每个子代换网络为代换盒(Substitution Box)



S盒的设计准则

迄今为止，有关方面未曾完全公开有关DES的S盒的设计准则。Branstead等曾披露过下述准则：

- P1 S盒的输出都不是其输入的线性或仿射函数。
- P2 改变S盒的一个输入比特，其输出至少有两比特产生变化，即近一半产生变化。
- P3 当S盒的任一输入位保持不变，其它5位输入变化时(共有2^5 =32种情况)，输出数字中的0和1的总数近于相等。

这三点使DES的S盒能够实现较好的混淆。

感 谢 聆 听!

xynie@uestc.edu.cn