# 第三章 分组密码与高级数据加密标准

杨礼珍

课件下载Email：yanglizhen_course@163.com，密码：tongjics

同济大学计算机科学与技术系, 2018

# Outline

# 本章作业

本章作业以这里列出的为准。
第三章习题3.1（注意，SPN(·)只表示为SPN网络结构，不是数学函数），3.2，3.3，3.7
作业b3：如果AES算法没有列混合运算，请给出一个比穷举搜索更有效的攻击算法。
第三章思考题：课本习题3.4、3.5（需提交代码）、3.8

# 现代密码的加密方式

- **对称加密体制**—容易从加密密钥计算出解密密钥，一般加密密钥和解密密钥一致，加密密钥和解密密钥都需要保密，因此也称为私钥密码体制。
  - **流密码**：由种子密钥产生密钥流，密钥流与明文流作用产生密文流，在第1.1.7节简单介绍过。
  - **分组密码**：明文以分组为单位进行加密，当今绝大部分分组密码都是乘积密码（见上一节），本章内容。
- **非对称密码体制**—从加密密钥计算出解密密钥是困难的，加密密钥是公开的，而解密密钥是保密的，因此也称为公钥密码体制，将在第五、六章介绍。

# 现代密码的加密方式

- **对称加密体制**—容易从加密密钥计算出解密密钥，一般加密密钥和解密密钥一致，加密密钥和解密密钥都需要保密，因此也称为私钥密码体制。
  - **流密码：**由种子密钥产生密钥流，密钥流与明文流作用产生密文流，在第1.1.7节简单介绍过。
  - **分组密码：**明文以分组为单位进行加密，当今绝大部分分组密码都是乘积密码（见上一节），本章内容。
- **非对称密码体制**—从加密密钥计算出解密密钥是困难的，加密密钥是公开的，而解密密钥是保密的，因此也称为公钥密码体制，将在第五、六章介绍。

# 现代密码的加密方式

- **对称加密体制**—容易从加密密钥计算出解密密钥，一般加密密钥和解密密钥一致，加密密钥和解密密钥都需要保密，因此也称为私钥密码体制。
  - **流密码：**由种子密钥产生密钥流，密钥流与明文流作用产生密文流，在第1.1.7节简单介绍过。
  - **分组密码：**明文以分组为单位进行加密，当今绝大部分分组密码都是乘积密码（见上一节），本章内容。
- **非对称密码体制**—从加密密钥计算出解密密钥是困难的，加密密钥是公开的，而解密密钥是保密的，因此也称为公钥密码体制，将在第五、六章介绍。

# 现代密码的加密方式

- **对称加密体制**—容易从加密密钥计算出解密密钥，一般加密密钥和解密密钥一致，加密密钥和解密密钥都需要保密，因此也称为私钥密码体制。
  - **流密码：**由种子密钥产生密钥流，密钥流与明文流作用产生密文流，在第1.1.7节简单介绍过。
  - **分组密码：**明文以分组为单位进行加密，当今绝大部分分组密码都是乘积密码（见上一节），本章内容。
- **非对称密码体制**—从加密密钥计算出解密密钥是困难的，加密密钥是公开的，而解密密钥是保密的，因此也称为公钥密码体制，将在第五、六章介绍。

# 分组密码的基本术语

**分组长度** 明文分组长度（长度=比特数），和密文分组长度一样

**种子密钥** 分组密码的密钥也称为种子密钥，以区别于轮密钥。

**密钥长度** 种子密钥的长度，不一定等于分组长度

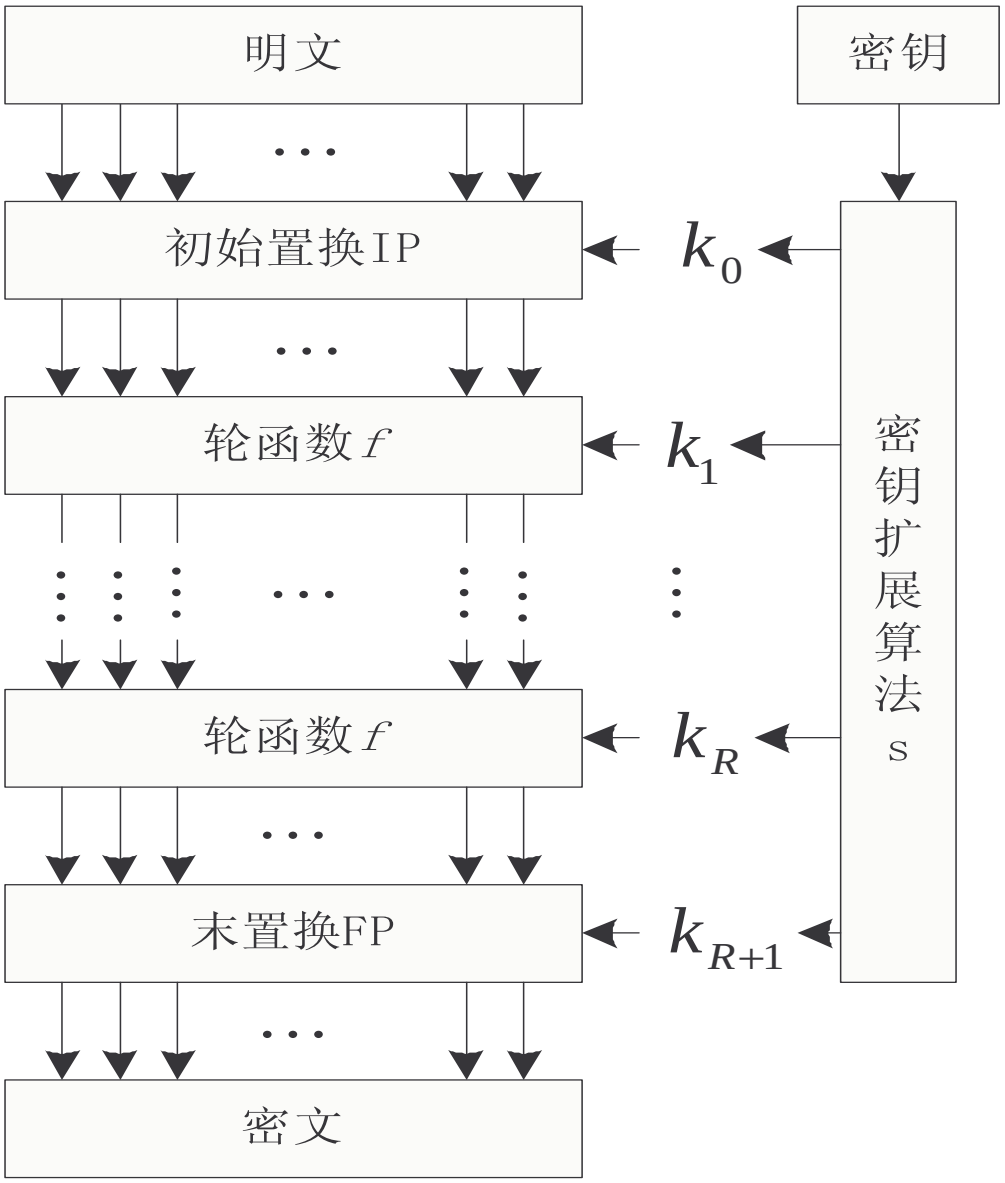
**轮函数**

**轮密钥** 轮密钥的长度不一定等于密钥长度

**密钥编排算法(方案)，或密码扩展算法(方案)** 种子密钥由密钥编排方案扩展成若干个轮密钥，作为轮函数的输入。

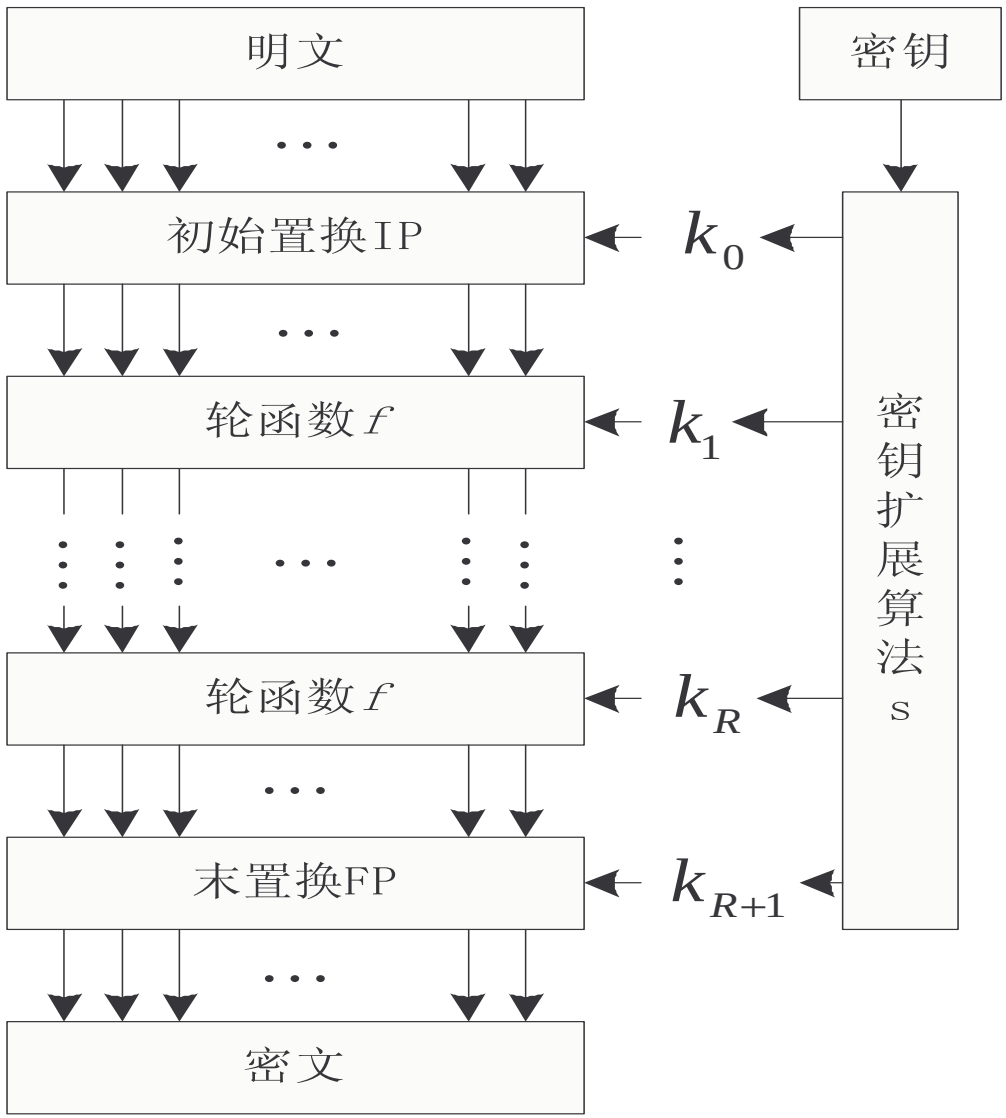
**迭代次数**

# 分组密码的一般形式



# 分组密码的一般形式

**解密函数：**加密函数的逆函数，因此解密函数的运算过程和加密函数相反，轮函数是加密函数的轮函数的逆，轮密钥与加密函数的轮密钥顺序相反。



# 分组密码的一般形式

备注：以上给出的是分组密码的一般形式，不是每个分组加密都严格遵循以上一般形式。

# 本章内容

# 迭代密码的两种类型

根据轮函数的形式，分为两种类型：

- Feistel型密码：代表密码是DES（将在第3.5节介绍）
- 代换-置换网络(SPN)：代表密码是AES（将在第3.6节介绍）

# 迭代密码的两种类型

根据轮函数的形式，分为两种类型：

- Feistel型密码：代表密码是DES（将在第3.5节介绍）
- 代换-置换网络(SPN)：代表密码是AES（将在第3.6节介绍）

# 代换-置换网络的一般形式

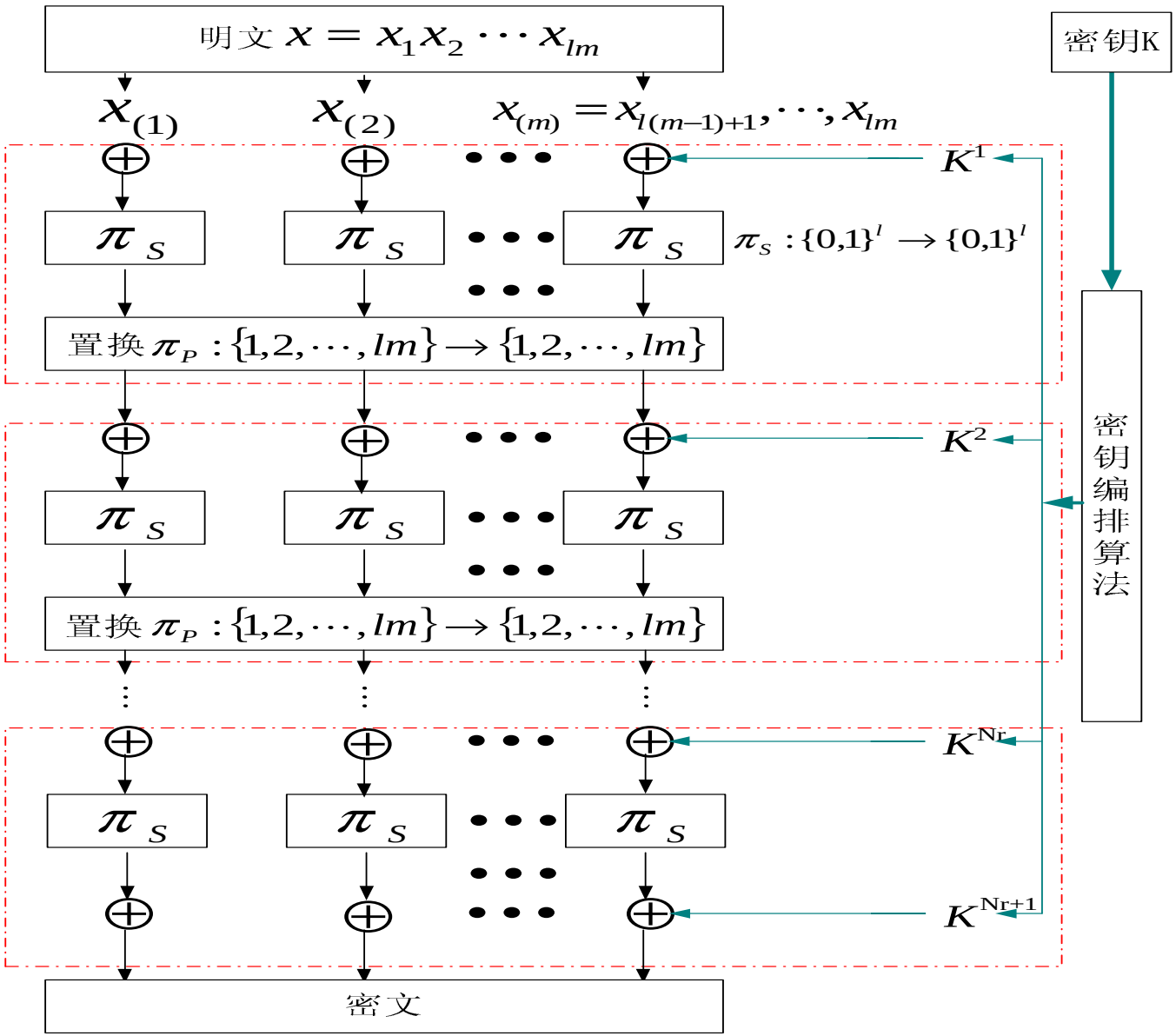
代换-置换网络来自Shannon的扩散-混淆的设计思想：

- 扩散：将明文中一个比特的影响扩散到密文中很多比特，从. 而将明文的统计结构隐藏起来。$\pi_P$起到扩散作用。
- 混淆：采用数据变换，使密文的统计特性和明文的统计特性之间的关系更为复杂。$\pi_S$起到混淆作用。

# 代换-置换网络的一般形式

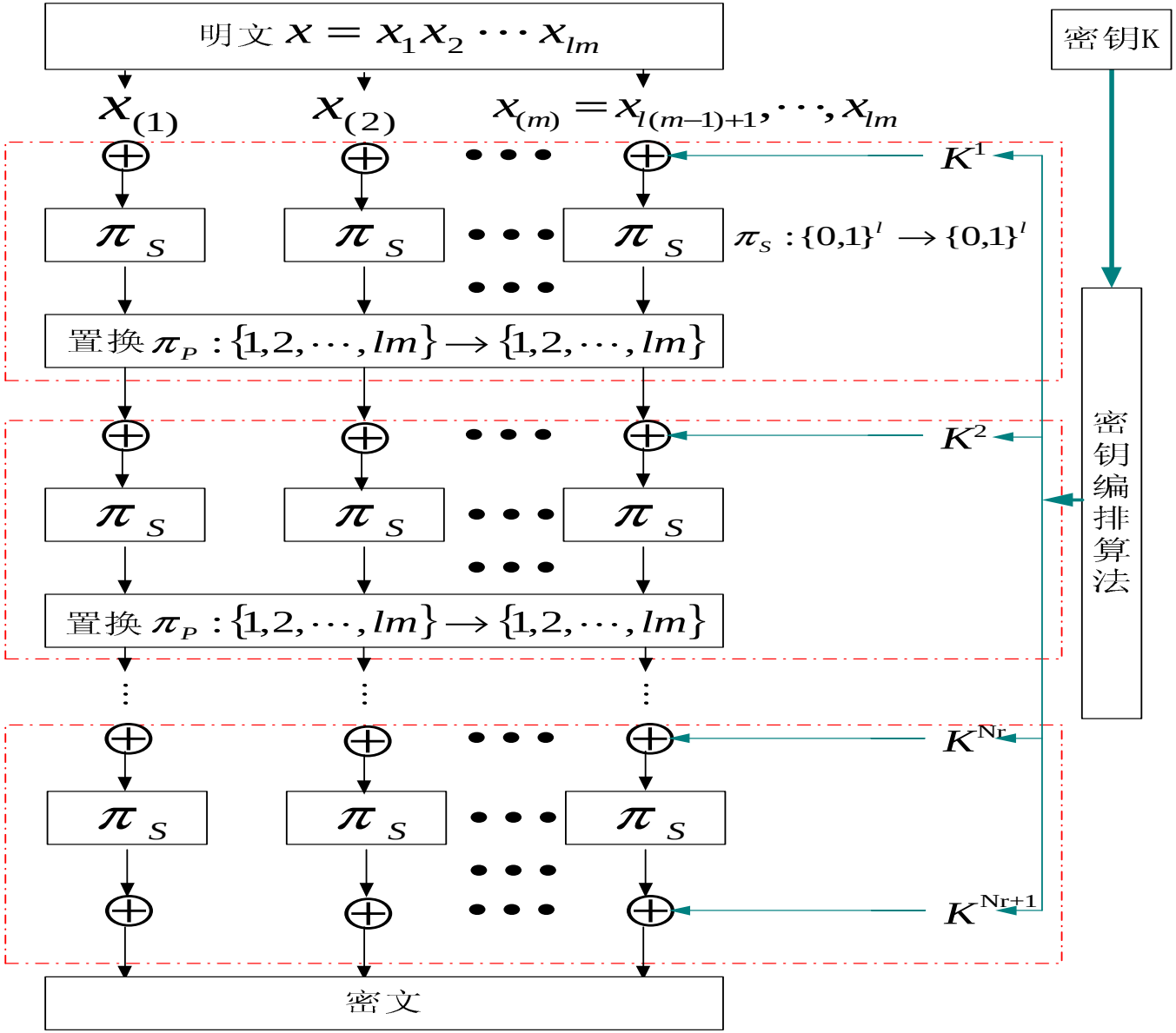
$\pi_S$：$\{0,1\}^l$自身上的双射，非线性运算，代换层，S盒。

$\pi_P$：$\{1,2,\ldots,lm\}$上的置换，线性运算，置换层。



# 代换-置换网络的一般形式

**解密函数：**轮函数顺序与加密函数相反，过程相反，$S$盒是$\pi_S$的逆函数，置换是$\pi_P$的逆函数。思考练习3.1。



# 例3.1

参数定义： $l = m = 4 = N_r = 4$

$S$盒$\pi_S$定义：输入$z$和输出$\pi_S(z)$都以十六进制表示，即

$$0 \leftrightarrow \{0,0,0,0\}, 1 \leftrightarrow \{0,0,0,1\}, \cdots, 9 \leftrightarrow \{1,0,0,1\}$$
$$A \leftrightarrow \{1,0,1,0\}, \cdots F \leftrightarrow \{1,1,1,1\}$$

| $z$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_S(z)$ | E | 4 | D | 1 | 2 | F | B | 8 | 3 | A | 6 | C | 5 | 9 | 0 | 7 |

置换$\pi_P$定义：

$$\pi_P(i+4j) = 4i + j - 3 \quad \pi_P(16) = 16, \quad 0 \leq j \leq 3$$

| $z$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_P(z)$ | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 | 15 | 4 | 8 | 12 | 16 |

密钥编排算法定义：

$$32\text{比特密钥}K = K_1||K_2||K_3||K_4||K_5||K_6||K_7||K_8$$

轮密钥：

$$K^1 = K_1||K_2||K_3||K_4 \quad K^2 = K_2||K_3||K_4||K_5 \quad K^3 = K_3||K_4||K_5||K_6$$
$$K^4 = K_4||K_5||K_6||K_7 \quad K^5 = K_5||K_6||K_7||K_8$$

# 例3.1

参数定义： $l = m = 4 = N_r = 4$

$S$盒$\pi_S$定义：输入$z$和输出$\pi_S(z)$都以十六进制表示，即

$$0 \leftrightarrow \{0,0,0,0\}, 1 \leftrightarrow \{0,0,0,1\}, \cdots, 9 \leftrightarrow \{1,0,0,1\}$$
$$A \leftrightarrow \{1,0,1,0\}, \cdots F \leftrightarrow \{1,1,1,1\}$$

| $z$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_S(z)$ | E | 4 | D | 1 | 2 | F | B | 8 | 3 | A | 6 | C | 5 | 9 | 0 | 7 |

置换$\pi_P$定义：

$$\pi_P(i+4j) = 4i + j - 3 \quad \pi_P(16) = 16, \quad 0 \leq j \leq 3$$

| $z$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_P(z)$ | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 | 15 | 4 | 8 | 12 | 16 |

密钥编排算法定义：

$$32\text{比特密钥}K = K_1||K_2||K_3||K_4||K_5||K_6||K_7||K_8$$

轮密钥：

$$K^1 = K_1||K_2||K_3||K_4 \quad K^2 = K_2||K_3||K_4||K_5 \quad K^3 = K_3||K_4||K_5||K_6$$
$$K^4 = K_4||K_5||K_6||K_7 \quad K^5 = K_5||K_6||K_7||K_8$$

# 例3.1

参数定义： $l = m = 4 = N_r = 4$

$S$盒$\pi_S$定义：输入$z$和输出$\pi_S(z)$都以十六进制表示，即

$$0 \leftrightarrow \{0,0,0,0\}, 1 \leftrightarrow \{0,0,0,1\}, \cdots, 9 \leftrightarrow \{1,0,0,1\}$$
$$A \leftrightarrow \{1,0,1,0\}, \cdots F \leftrightarrow \{1,1,1,1\}$$

| $z$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_S(z)$ | E | 4 | D | 1 | 2 | F | B | 8 | 3 | A | 6 | C | 5 | 9 | 0 | 7 |

置换$\pi_P$定义：

$$\pi_P(i+4j) = 4i + j - 3 \quad \pi_P(16) = 16, \quad 0 \le j \le 3$$

| $z$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_P(z)$ | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 | 15 | 4 | 8 | 12 | 16 |

密钥编排算法定义：

$$32\text{比特密钥}K = K_1||K_2||K_3||K_4||K_5||K_6||K_7||K_8$$

轮密钥：

$$K^1 = K_1||K_2||K_3||K_4 \quad K^2 = K_2||K_3||K_4||K_5 \quad K^3 = K_3||K_4||K_5||K_6$$
$$K^4 = K_4||K_5||K_6||K_7 \quad K^5 = K_5||K_6||K_7||K_8$$

# 例3.1

参数定义： $l = m = 4 = N_r = 4$

$S$盒$\pi_S$定义：输入$z$和输出$\pi_S(z)$都以十六进制表示，即

$$0 \leftrightarrow \{0,0,0,0\}, 1 \leftrightarrow \{0,0,0,1\}, \cdots, 9 \leftrightarrow \{1,0,0,1\}$$
$$A \leftrightarrow \{1,0,1,0\}, \cdots F \leftrightarrow \{1,1,1,1\}$$

| $z$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_S(z)$ | E | 4 | D | 1 | 2 | F | B | 8 | 3 | A | 6 | C | 5 | 9 | 0 | 7 |

置换$\pi_P$定义：

$$\pi_P(i+4j) = 4i + j - 3 \quad \pi_P(16) = 16, \quad 0 \le j \le 3$$

| $z$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\pi_P(z)$ | 1 | 5 | 9 | 13 | 2 | 6 | 10 | 14 | 3 | 7 | 11 | 15 | 4 | 8 | 12 | 16 |

密钥编排算法定义：

$$32\text{比特密钥}K = K_1||K_2||K_3||K_4||K_5||K_6||K_7||K_8$$

轮密钥：

$$K^1 = K_1||K_2||K_3||K_4 \quad K^2 = K_2||K_3||K_4||K_5 \quad K^3 = K_3||K_4||K_5||K_6$$
$$K^4 = K_4||K_5||K_6||K_7 \quad K^5 = K_5||K_6||K_7||K_8$$

# 例3.1

**输入：**明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

# 例3.1

输入：明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

加密过程：

$$
\begin{array}{lllll}
x & & = & 0010\ 0110\ 1011\ 0111 & \\
K^1 & & = & 0011\ 1010\ 1001\ 0100 & \\
u^1 & = x \oplus K^1 & = & 0001\ 1100\ 0010\ 0011 & = 1\ C\ 2\ 3 \\
v^1 & = \pi_S(u^1) & = & 0100\ 0101\ 1101\ 0001 & = 4\ 5\ D\ 1 \\
w^1 & = \pi_P(v^1) & = & 0010\ 1110\ 0000\ 0111 & \\
 & & \vdots & & \\
w^3 & & = & 1110\ 0100\ 0110\ 1110 & \\
K^4 & & = & 0100\ 1101\ 0110\ 0011 & \\
u^4 & = w^3 \oplus K^4 & = & 1010\ 1001\ 0000\ 1101 & = A\ 9\ 0\ B \\
v^4 & = \pi_S(u^4) & = & 0110\ 1010\ 1110\ 1001 & = 6\ A\ E\ C \\
K^5 & & = & 1101\ 0110\ 0011\ 1111 & \\
y & = v^4 \oplus K^5 & = & 1011\ 1100\ 1101\ 0110 &
\end{array}
$$

# 例3.1

输入：明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

加密过程：

$$
\begin{array}{lllll}
x & & = & 0010\ 0110\ 1011\ 0111 & \\
K^1 & & = & 0011\ 1010\ 1001\ 0100 & \\
u^1 & = x \oplus K^1 & = & 0001\ 1100\ 0010\ 0011 & = 1\ C\ 2\ 3 \\
v^1 & = \pi_S(u^1) & = & 0100\ 0101\ 1101\ 0001 & = 4\ 5\ D\ 1 \\
w^1 & = \pi_P(v^1) & = & 0010\ 1110\ 0000\ 0111 & \\
 & & \vdots & & \\
w^3 & & = & 1110\ 0100\ 0110\ 1110 & \\
K^4 & & = & 0100\ 1101\ 0110\ 0011 & \\
u^4 & = w^3 \oplus K^4 & = & 1010\ 1001\ 0000\ 1101 & = A\ 9\ 0\ B \\
v^4 & = \pi_S(u^4) & = & 0110\ 1010\ 1110\ 1001 & = 6\ A\ E\ C \\
K^5 & & = & 1101\ 0110\ 0011\ 1111 & \\
y & = v^4 \oplus K^5 & = & 1011\ 1100\ 1101\ 0110 &
\end{array}
$$

# 例3.1

输入：明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

加密过程：

$$
\begin{array}{lllll}
x & & = & 0010\ 0110\ 1011\ 0111 & \\
K^1 & & = & 0011\ 1010\ 1001\ 0100 & \\
u^1 & = x \oplus K^1 & = & 0001\ 1100\ 0010\ 0011 & = 1\ C\ 2\ 3 \\
v^1 & = \pi_S(u^1) & = & 0100\ 0101\ 1101\ 0001 & = 4\ 5\ D\ 1 \\
w^1 & = \pi_P(v^1) & = & 0010\ 1110\ 0000\ 0111 & \\
 & & \vdots & & \\
w^3 & & = & 1110\ 0100\ 0110\ 1110 & \\
K^4 & & = & 0100\ 1101\ 0110\ 0011 & \\
u^4 & = w^3 \oplus K^4 & = & 1010\ 1001\ 0000\ 1101 & = A\ 9\ 0\ B \\
v^4 & = \pi_S(u^4) & = & 0110\ 1010\ 1110\ 1001 & = 6\ A\ E\ C \\
K^5 & & = & 1101\ 0110\ 0011\ 1111 & \\
y & = v^4 \oplus K^5 & = & 1011\ 1100\ 1101\ 0110 &
\end{array}
$$

# 例3.1

输入：明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

加密过程：

$$
\begin{array}{lllll}
x & & = & 0010\ 0110\ 1011\ 0111 & \\
K^1 & & = & 0011\ 1010\ 1001\ 0100 & \\
u^1 & = x \oplus K^1 & = & 0001\ 1100\ 0010\ 0011 & = 1\ C\ 2\ 3 \\
v^1 & = \pi_S(u^1) & = & 0100\ 0101\ 1101\ 0001 & = 4\ 5\ D\ 1 \\
w^1 & = \pi_P(v^1) & = & 0010\ 1110\ 0000\ 0111 & \\
 & & \vdots & & \\
w^3 & & = & 1110\ 0100\ 0110\ 1110 & \\
K^4 & & = & 0100\ 1101\ 0110\ 0011 & \\
u^4 & = w^3 \oplus K^4 & = & 1010\ 1001\ 0000\ 1101 & = A\ 9\ 0\ B \\
v^4 & = \pi_S(u^4) & = & 0110\ 1010\ 1110\ 1001 & = 6\ A\ E\ C \\
K^5 & & = & 1101\ 0110\ 0011\ 1111 & \\
y & = v^4 \oplus K^5 & = & 1011\ 1100\ 1101\ 0110 &
\end{array}
$$

# 例3.1

输入：明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

加密过程：

$$
\begin{array}{lllll}
x & & = & 0010\ 0110\ 1011\ 0111 & \\
K^1 & & = & 0011\ 1010\ 1001\ 0100 & \\
u^1 & = x \oplus K^1 & = & 0001\ 1100\ 0010\ 0011 & = 1\ C\ 2\ 3 \\
v^1 & = \pi_S(u^1) & = & 0100\ 0101\ 1101\ 0001 & = 4\ 5\ D\ 1 \\
w^1 & = \pi_P(v^1) & = & 0010\ 1110\ 0000\ 0111 & \\
 & & \vdots & & \\
w^3 & & = & 1110\ 0100\ 0110\ 1110 & \\
K^4 & & = & 0100\ 1101\ 0110\ 0011 & \\
u^4 & = w^3 \oplus K^4 & = & 1010\ 1001\ 0000\ 1101 & = A\ 9\ 0\ B \\
v^4 & = \pi_S(u^4) & = & 0110\ 1010\ 1110\ 1001 & = 6\ A\ E\ C \\
K^5 & & = & 1101\ 0110\ 0011\ 1111 & \\
y & = v^4 \oplus K^5 & = & 1011\ 1100\ 1101\ 0110 &
\end{array}
$$

# 例3.1

输入：明文：$x = 0010\ 0110\ 1011\ 0111$

密钥：$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$

加密过程：

$$
\begin{array}{lllll}
x & & = & 0010\ 0110\ 1011\ 0111 & \\
K^1 & & = & 0011\ 1010\ 1001\ 0100 & \\
u^1 & = x \oplus K^1 & = & 0001\ 1100\ 0010\ 0011 & = 1\ C\ 2\ 3 \\
v^1 & = \pi_S(u^1) & = & 0100\ 0101\ 1101\ 0001 & = 4\ 5\ D\ 1 \\
w^1 & = \pi_P(v^1) & = & 0010\ 1110\ 0000\ 0111 & \\
 & & \vdots & & \\
w^3 & & = & 1110\ 0100\ 0110\ 1110 & \\
K^4 & & = & 0100\ 1101\ 0110\ 0011 & \\
u^4 & = w^3 \oplus K^4 & = & 1010\ 1001\ 0000\ 1101 & = A\ 9\ 0\ B \\
v^4 & = \pi_S(u^4) & = & 0110\ 1010\ 1110\ 1001 & = 6\ A\ E\ C \\
K^5 & & = & 1101\ 0110\ 0011\ 1111 & \\
y & = v^4 \oplus K^5 & = & 1011\ 1100\ 1101\ 0110 &
\end{array}
$$

# 代换-置换网络特点和变体

## SPN的特点是简单有效：

- $S$盒$\pi_S$可以以查表方式实现，$\pi_S : \{0,1\}^l \to \{0,1\}^l$所需的存储空间是$l2^l$。
- $S$盒$\pi_S$的作用是把明文和密钥局部混淆，是非线性运算，$\pi_P$起全局扩散作用，是线性运算。

# 代换-置换网络特点和变体

## SPN的特点是简单有效：

- $S$盒$\pi_S$可以以查表方式实现，$\pi_S : \{0,1\}^l \to \{0,1\}^l$所需的存储空间是$l2^l$。
- $S$盒$\pi_S$的作用是把明文和密钥局部混淆，是非线性运算，$\pi_P$起全局扩散作用，是线性运算。

# 代换-置换网络特点和变体

## SPN的特点是简单有效：

- $S$盒$\pi_S$可以以查表方式实现，$\pi_S : \{0,1\}^l \to \{0,1\}^l$所需的存储空间是$l2^l$。
- $S$盒$\pi_S$的作用是把明文和密钥局部混淆，是非线性运算，$\pi_P$起全局扩散作用，是线性运算。

## SPN的变体：

- 使用多个$S$盒$\pi_S$，如AES中使用了8个不同的$S$盒。
- 每一轮中包含一个可逆的线性运算，该线性变换要么代替置换$\pi_P$，要么作为$\pi_P$的补充。

# 代换-置换网络特点和变体

## SPN的特点是简单有效：

- $S$盒$\pi_S$可以以查表方式实现，$\pi_S : \{0,1\}^l \to \{0,1\}^l$所需的存储空间是$l2^l$。
- $S$盒$\pi_S$的作用是把明文和密钥局部混淆，是非线性运算，$\pi_P$起全局扩散作用，是线性运算。

## SPN的变体：

- 使用多个$S$盒$\pi_S$，如AES中使用了8个不同的$S$盒。
- 每一轮中包含一个可逆的线性运算，该线性变换要么代替置换$\pi_P$，要么作为$\pi_P$的补充。

# 3.2节的作业

练习3.1

# 线性密码分析原理

符号说明：

- $X[i_1, i_2, \ldots, i_d]$表示比特向量$X$的第$i_1, i_2, \ldots, i_d$比特的异或，即

$$X[i_1, i_2, \ldots, i_d] = X[i_1] \oplus X[i_2] \oplus \ldots X[i_d]$$

- $X$表示分组密码的明文输入，$W^i(i = 1, \ldots, N^r + 1)$表示第$i$轮输出，或第$i + 1$轮输入，那么密文$Y = W^{N^r+1}$。

# 线性密码分析原理

线性密码分析是已知明文分析。

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] = 0 \quad \text{成立概率} p \neq 1/2$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] = 0 \quad \text{成立概率} p \neq 1/2$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$X[i_1, i_2, \ldots, i_a] \oplus W^{Nr}[z_1, z_2, \ldots, z_f] = 0 \quad \text{成立概率} p \neq 1/2$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] = 0 \quad \text{成立概率} p \neq 1/2$$

$$\Uparrow$$

$$\pi_S(y \oplus K^{N_r+1}[n_1, n_2, \ldots, n_m]) \Leftarrow \text{猜测} K^{N_r+1}[n_1, n_2, \ldots, n_m]$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$X[i_1, i_2, \ldots, i_a] \oplus W^1[j_1, j_2, \ldots, j_b] = K^1[s_1, s_2, \ldots, s_u] \quad \text{第一轮线性逼近概率} p_1$$

$$W^1[j_1, j_2, \ldots, j_b] \oplus W^2[l_1, l_2, \ldots, l_c] = K^2[t_1, t_2, \ldots, t_v] \quad \text{第二轮线性逼近概率} p_2$$

$$W^2[l_1, l_2, \ldots, l_c] \oplus W^3[k_1, k_2, \ldots, k_d] = K^3[g_1, g_2, \ldots, g_w] \quad \text{第三轮线性逼近概率} p_3$$

$$\vdots$$

$$W^{N_r-1}[r_1, r_2, \ldots, r_e] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] = K^{N_r}[f_1, f_2, \ldots, f_h] \quad \text{第} N_r - 1 \text{轮逼近概率} p_{N_r-1}$$

$$X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] = 0 \quad \text{成立概率} p \neq 1/2$$

$$\Uparrow$$

$$\pi_S(y \oplus K^{N_r+1}[n_1, n_2, \ldots, n_m]) \Leftarrow \quad \text{猜测} K^{N_r+1}[n_1, n_2, \ldots, n_m]$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$
\begin{array}{rcll}
X[i_1, i_2, \ldots, i_a] \oplus W^1[j_1, j_2, \ldots, j_b] & = & K^1[s_1, s_2, \ldots, s_u] & \text{第一轮线性逼近概率} p_1 \\
\oplus & & & \\
W^1[j_1, j_2, \ldots, j_b] \oplus W^2[l_1, l_2, \ldots, l_c] & = & K^2[t_1, t_2, \ldots, t_v] & \text{第二轮线性逼近概率} p_2 \\
\oplus & & & \\
W^2[l_1, l_2, \ldots, l_c] \oplus W^3[k_1, k_2, \ldots, k_d] & = & K^3[g_1, g_2, \ldots, g_w] & \text{第三轮线性逼近概率} p_3 \\
\oplus & & & \\
\vdots & & & \\
\oplus & & & \\
W^{N_r-1}[r_1, r_2, \ldots, r_e] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] & = & K^{N_r}[f_1, f_2, \ldots, f_h] & \text{第} N_r - 1 \text{轮逼近概率} p_{N_r-1} \\
\Downarrow & & & \\
X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] & = & K^1[s_1 \ldots s_u] \ldots K^{N_r}[f_1 \ldots f_h] & \\
\Uparrow & & & \\
\pi_S(y \oplus K^{N_r+1}[n_1, n_2, \ldots, n_m]) & \Leftarrow & & \text{猜测} K^{N_r+1}[n_1, n_2, \ldots, n_m]
\end{array}
$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$
\begin{array}{rcll}
X[i_1, i_2, \ldots, i_a] \oplus W^1[j_1, j_2, \ldots, j_b] & = & K^1[s_1, s_2, \ldots, s_u] & \text{第一轮线性逼近概率} p_1 \\
\oplus & & & \\
W^1[j_1, j_2, \ldots, j_b] \oplus W^2[l_1, l_2, \ldots, l_c] & = & K^2[t_1, t_2, \ldots, t_v] & \text{第二轮线性逼近概率} p_2 \\
\oplus & & & \\
W^2[l_1, l_2, \ldots, l_c] \oplus W^3[k_1, k_2, \ldots, k_d] & = & K^3[g_1, g_2, \ldots, g_w] & \text{第三轮线性逼近概率} p_3 \\
\oplus & & & \\
\vdots & & & \\
\oplus & & & \\
W^{N_r-1}[r_1, r_2, \ldots, r_e] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] & = & K^{N_r}[f_1, f_2, \ldots, f_h] & \text{第} N_r - 1 \text{轮逼近概率} p_{N_r-1} \\
\Downarrow & & & \text{假定每一轮逼近独立} \\
X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] & = & K^1[s_1 \ldots s_u] \ldots K^{N_r}[f_1 \ldots f_h] & \text{根据堆积引理计算概率} p \\
\Uparrow & & & \\
\pi_S(y \oplus K^{N_r+1}[n_1, n_2, \ldots, n_m]) & \Leftarrow & & \text{猜测} K^{N_r+1}[n_1, n_2, \ldots, n_m]
\end{array}
$$

# 线性密码分析原理

线性密码分析是已知明文分析。**原理：**

符号说明：$X[i_1, i_2, \ldots, i_a]$表示$X$的第$i_1, i_2, \ldots, i_a$比特的异或，其它依此类推。

$$
\begin{array}{rcll}
X[i_1, i_2, \ldots, i_a] \oplus W^1[j_1, j_2, \ldots, j_b] & = & K^1[s_1, s_2, \ldots, s_u] & \text{第一轮线性逼近概率} p_1 \\
\oplus & & & \\
W^1[j_1, j_2, \ldots, j_b] \oplus W^2[l_1, l_2, \ldots, l_c] & = & K^2[t_1, t_2, \ldots, t_v] & \text{第二轮线性逼近概率} p_2 \\
\oplus & & & \\
W^2[l_1, l_2, \ldots, l_c] \oplus W^3[k_1, k_2, \ldots, k_d] & = & K^3[g_1, g_2, \ldots, g_w] & \text{第三轮线性逼近概率} p_3 \\
\oplus & & & \\
\vdots & & & \\
\oplus & & & \\
W^{N_r-1}[r_1, r_2, \ldots, r_e] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] & = & K^{N_r}[f_1, f_2, \ldots, f_h] & \text{第} N_r - 1 \text{轮逼近概率} p_{N_r-1} \\
\Downarrow & & & \text{假定每一轮逼近独立} \\
X[i_1, i_2, \ldots, i_a] \oplus W^{N_r}[z_1, z_2, \ldots, z_f] & = & K^1[s_1 \ldots s_u] \ldots K^{N_r}[f_1 \ldots f_h] & \text{根据堆积引理计算概率} p \\
\Uparrow & & & \\
\pi_S(y \oplus K^{N_r+1}[n_1, n_2, \ldots, n_m]) & \Leftarrow & & \text{猜测} K^{N_r+1}[n_1, n_2, \ldots, n_m]
\end{array}
$$

单轮的线性逼近概率由非线性的$S$盒决定，因此线性分析的关键是求$S$盒的线性逼近。

# 堆积引理

**偏差：**设随机变量$X$取值为$\{0,1\}$，而且$Pr[X=0]=p$，则随机变量$X$的偏差定义为$\varepsilon = p - 1/2$。

## Lemma

（堆积引理）设$X_1, X_2, \ldots, X_k$是$k$个独立的随机变量，而且$P[X_i = 0] = p_i$，$P[X_i = 1] = 1 - p_i$，则

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_k = 0] = 1/2 + 2^{k-1} \prod_{i=1}^{k} (p_i - 1/2)$$

若$X_i (1 \le i \le k)$的偏差为$\varepsilon_i$，则$X_1 \oplus X_2 \oplus \ldots \oplus X_k$的偏差为

$$\varepsilon = 2^{k-1} \prod_{i=1}^{k} \varepsilon_i$$

## 堆积引理

**偏差：**设随机变量$X$取值为$\{0,1\}$，而且$Pr[X=0]=p$，则随机变量$X$的偏差定义为$\varepsilon = p - 1/2$。

### Lemma

（堆积引理）设$X_1, X_2, \ldots, X_k$是$k$个独立的随机变量，而且$P[X_i=0]=p_i$，$P[X_i=1]=1-p_i$，则

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_k = 0] = 1/2 + 2^{k-1}\prod_{i=1}^{k}(p_i - 1/2)$$

若$X_i(1 \le i \le k)$的偏差为$\varepsilon_i$，则$X_1 \oplus X_2 \oplus \ldots \oplus X_k$的偏差为

$$\varepsilon = 2^{k-1}\prod_{i=1}^{k}\varepsilon_i$$

# 堆积引理

**偏差：**设随机变量$X$取值为$\{0,1\}$，而且$Pr[X=0]=p$，则随机变量$X$的偏差定义为$\varepsilon = p - 1/2$。

## Lemma

（堆积引理）设$X_1, X_2, \ldots, X_k$是$k$个独立的随机变量，而且$P[X_i=0]=p_i$，$P[X_i=1]=1-p_i$，则

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_k = 0] = 1/2 + 2^{k-1}\prod_{i=1}^{k}(p_i - 1/2)$$

若$X_i(1 \le i \le k)$的偏差为$\varepsilon_i$，则$X_1 \oplus X_2 \oplus \ldots \oplus X_k$的偏差为

$$\varepsilon = 2^{k-1}\prod_{i=1}^{k}\varepsilon_i$$

# 堆积引理

**偏差：**设随机变量$X$取值为$\{0,1\}$，而且$Pr[X=0]=p$，则随机变量$X$的偏差定义为$\varepsilon = p - 1/2$。

## Lemma

（堆积引理）设$X_1, X_2, \ldots, X_k$是$k$个独立的随机变量，而且$P[X_i=0]=p_i$，$P[X_i=1]=1-p_i$，则

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_k = 0] = 1/2 + 2^{k-1}\prod_{i=1}^{k}(p_i - 1/2)$$

若$X_i(1 \le i \le k)$的偏差为$\varepsilon_i$，则$X_1 \oplus X_2 \oplus \ldots \oplus X_k$的偏差为

$$\varepsilon = 2^{k-1}\prod_{i=1}^{k}\varepsilon_i$$

## 堆积引理的证明

对$k$应用数学归纳法。

## 堆积引理的证明

对$k$应用数学归纳法。

(1)$k = 1$是显然成立。

# 堆积引理的证明

对$k$应用数学归纳法。
(1)$k = 1$是显然成立。
(2)假设$k = l$时成立，即有

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] = 1/2 + 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2)$$

# 堆积引理的证明

对$k$应用数学归纳法。
(1)$k = 1$是显然成立。
(2)假设$k = l$时成立，即有

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] = 1/2 + 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2)$$

当$k = l + 1$时有

$$\begin{aligned} P[X_1 \oplus X_2 \oplus \ldots \oplus X_{l+1} = 0] &= P[X_{l+1} = 0]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0 | X_{l+1} = 0] + \\ & \quad P[X_{l+1} = 1]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 1 | X_{l+1} = 1] \\ &= P[X_{l+1} = 0]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] + \\ & \quad P[X_{l+1} = 1]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 1] \end{aligned}$$

# 堆积引理的证明

对$k$应用数学归纳法。
(1)$k = 1$是显然成立。
(2)假设$k = l$时成立，即有

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] = 1/2 + 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2)$$

当$k = l + 1$时有

$$\begin{aligned}
P[X_1 \oplus X_2 \oplus \ldots \oplus X_{l+1} = 0] &= P[X_{l+1} = 0]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0 | X_{l+1} = 0] + \\
&\quad P[X_{l+1} = 1]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 1 | X_{l+1} = 1] \\
&= P[X_{l+1} = 0]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] + \\
&\quad P[X_{l+1} = 1]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 1] \\
&= p_{l+1} \left( 1/2 + 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2) \right) + \\
&\quad (1 - p_{l+1}) \left( 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2) - 1/2 \right)
\end{aligned}$$

# 堆积引理的证明

对$k$应用数学归纳法。
(1)$k = 1$是显然成立。
(2)假设$k = l$时成立，即有

$$P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] = 1/2 + 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2)$$

当$k = l + 1$时有

$$\begin{aligned}
P[X_1 \oplus X_2 \oplus \ldots \oplus X_{l+1} = 0] &= P[X_{l+1} = 0]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0 | X_{l+1} = 0] + \\
&\quad P[X_{l+1} = 1]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 1 | X_{l+1} = 1] \\
&= P[X_{l+1} = 0]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 0] + \\
&\quad P[X_{l+1} = 1]P[X_1 \oplus X_2 \oplus \ldots \oplus X_l = 1] \\
&= p_{l+1} \left( 1/2 + 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2) \right) + \\
&\quad (1 - p_{l+1}) \left( 2^{l-1} \prod_{i=1}^{l} (p_i - 1/2) - 1/2 \right) \\
&= 1/2 + 2^{l} \prod_{i=1}^{l+1} (p_i - 1/2)
\end{aligned}$$

# 堆积引理的推论

**Corollary**

设$X_1, X_2, \ldots, X_k$是$k$个独立的随机变量，若对某个$j$，$X_j$的偏差$\varepsilon_j = 0$，则随机变量$X_1 \oplus X_2 \oplus \ldots \oplus X_k$的偏差$\varepsilon = 0$。

# 堆积引理的推论

**Corollary**

设$X_1, X_2, \ldots, X_k$是$k$个独立的随机变量，若对某个$j$，$X_j$的偏差$\varepsilon_j = 0$，则随机变量$X_1 \oplus X_2 \oplus \ldots \oplus X_k$的偏差$\varepsilon = 0$。

# 堆积引理成立的条件

堆积引理只在$X_1, X_2, \ldots, X_k$统计独立情况下才成立，否则不一定成立。

**Example**

设$X_1, X_2, X_3$的偏差分别为$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1/4$，由堆积引理得到$\varepsilon_{1,2} = \varepsilon_{1,3} = \varepsilon_{2,3} = 1/8$。

$$X_1 \oplus X_3 = (X_1 \oplus X_2) \oplus (X_2 \oplus X_3)$$

如果随机变量$(X_1 \oplus X_2)$和$X_2 \oplus X_3$统计独立，根据堆积引理计算得到

$$\varepsilon_{1,3} = 2(1/8)^2 = 1/32 \neq 1/8$$

因此$X_1 \oplus X_2$和$X_2 \oplus X_3$统计不独立，不能由堆积引理给出正确答案。

思考练习3.9：证明$X_1 \oplus X_2$和$X_2 \oplus X_3$统计独立当且仅当$\varepsilon_1 = \varepsilon_3 = 0$或$\varepsilon_2 = \pm 1/2$。

# 堆积引理成立的条件

堆积引理只在$X_1, X_2, \ldots, X_k$统计独立情况下才成立，否则不一定成立。

**Example**

设$X_1, X_2, X_3$的偏差分别为$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1/4$，由堆积引理得到$\varepsilon_{1,2} = \varepsilon_{1,3} = \varepsilon_{2,3} = 1/8$。

$$X_1 \oplus X_3 = (X_1 \oplus X_2) \oplus (X_2 \oplus X_3)$$

如果随机变量$(X_1 \oplus X_2)$和$X_2 \oplus X_3$统计独立，根据堆积引理计算得到

$$\varepsilon_{1,3} = 2(1/8)^2 = 1/32 \neq 1/8$$

因此$X_1 \oplus X_2$和$X_2 \oplus X_3$统计不独立，不能由堆积引理给出正确答案。

思考练习3.9：证明$X_1 \oplus X_2$和$X_2 \oplus X_3$统计独立当且仅当$\varepsilon_1 = \varepsilon_3 = 0$或$\varepsilon_2 = \pm 1/2$。

# 堆积引理成立的条件

堆积引理只在$X_1, X_2, \ldots, X_k$统计独立情况下才成立，否则不一定成立。

**Example**

设$X_1, X_2, X_3$的偏差分别为$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1/4$，由堆积引理得到$\varepsilon_{1,2} = \varepsilon_{1,3} = \varepsilon_{2,3} = 1/8$。

$$X_1 \oplus X_3 = (X_1 \oplus X_2) \oplus (X_2 \oplus X_3)$$

如果随机变量$(X_1 \oplus X_2)$和$X_2 \oplus X_3$统计独立，根据堆积引理计算得到

$$\varepsilon_{1,3} = 2(1/8)^2 = 1/32 \neq 1/8$$

因此$X_1 \oplus X_2$和$X_2 \oplus X_3$统计不独立，不能由堆积引理给出正确答案。

思考练习3.9：证明$X_1 \oplus X_2$和$X_2 \oplus X_3$统计独立当且仅当$\varepsilon_1 = \varepsilon_3 = 0$或$\varepsilon_2 = \pm 1/2$。

# 堆积引理成立的条件

堆积引理只在$X_1, X_2, \ldots, X_k$统计独立情况下才成立，否则不一定成立。

**Example**

设$X_1, X_2, X_3$的偏差分别为$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1/4$，由堆积引理得到$\varepsilon_{1,2} = \varepsilon_{1,3} = \varepsilon_{2,3} = 1/8$。

$$X_1 \oplus X_3 = (X_1 \oplus X_2) \oplus (X_2 \oplus X_3)$$

如果随机变量$(X_1 \oplus X_2)$和$X_2 \oplus X_3$统计独立，根据堆积引理计算得到

$$\varepsilon_{1,3} = 2(1/8)^2 = 1/32 \neq 1/8$$

因此$X_1 \oplus X_2$和$X_2 \oplus X_3$统计不独立，不能由堆积引理给出正确答案。

思考练习3.9：证明$X_1 \oplus X_2$和$X_2 \oplus X_3$统计独立当且仅当$\varepsilon_1 = \varepsilon_3 = 0$或$\varepsilon_2 = \pm 1/2$。

# 堆积引理成立的条件

堆积引理只在$X_1, X_2, \ldots, X_k$统计独立情况下才成立，否则不一定成立。

**Example**

设$X_1, X_2, X_3$的偏差分别为$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1/4$，由堆积引理得到$\varepsilon_{1,2} = \varepsilon_{1,3} = \varepsilon_{2,3} = 1/8$。

$$X_1 \oplus X_3 = (X_1 \oplus X_2) \oplus (X_2 \oplus X_3)$$

如果随机变量$(X_1 \oplus X_2)$和$X_2 \oplus X_3$统计独立，根据堆积引理计算得到

$$\varepsilon_{1,3} = 2(1/8)^2 = 1/32 \neq 1/8$$

因此$X_1 \oplus X_2$和$X_2 \oplus X_3$统计不独立，不能由堆积引理给出正确答案。

思考练习3.9：证明$X_1 \oplus X_2$和$X_2 \oplus X_3$统计独立当且仅当$\varepsilon_1 = \varepsilon_3 = 0$或$\varepsilon_2 = \pm 1/2$。

# 堆积引理成立的条件

堆积引理只在$X_1, X_2, \ldots, X_k$统计独立情况下才成立，否则不一定成立。

**Example**

设$X_1, X_2, X_3$的偏差分别为$\varepsilon_1 = \varepsilon_2 = \varepsilon_3 = 1/4$，由堆积引理得到$\varepsilon_{1,2} = \varepsilon_{1,3} = \varepsilon_{2,3} = 1/8$。

$$X_1 \oplus X_3 = (X_1 \oplus X_2) \oplus (X_2 \oplus X_3)$$

如果随机变量$(X_1 \oplus X_2)$和$X_2 \oplus X_3$统计独立，根据堆积引理计算得到

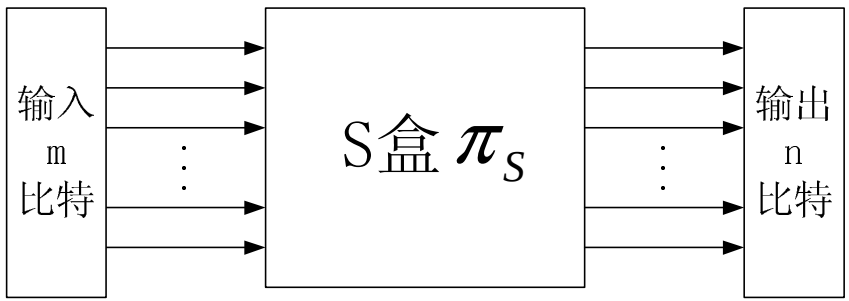
$$\varepsilon_{1,3} = 2(1/8)^2 = 1/32 \neq 1/8$$

因此$X_1 \oplus X_2$和$X_2 \oplus X_3$统计不独立，不能由堆积引理给出正确答案。

思考练习3.9：证明$X_1 \oplus X_2$和$X_2 \oplus X_3$统计独立当且仅当$\varepsilon_1 = \varepsilon_3 = 0$或$\varepsilon_2 = \pm 1/2$。

# S盒的线性逼近

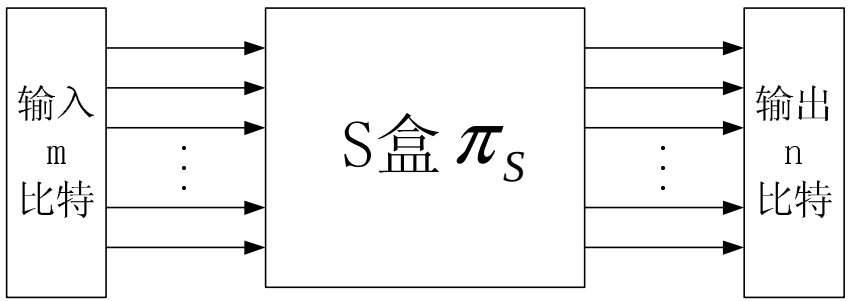
考虑$S$盒$\pi_S : \{0,1\}^m \to \{0,1\}^n$。




**定义：** 随机变量$\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m)$表示$m$重输入，
随机变量$\mathbf{Y} = (\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n)$表示$n$重输出。
**假定：** $\mathbf{X}_i (1 \le i \le m), \mathbf{Y}_j (1 \le j \le n)$独立同分布，均取值于$\{0,1\}$，而且偏差为0。
**计算：** 随机变量$a_1\mathbf{X}_1 \oplus \ldots \oplus a_m\mathbf{X}_m \oplus b_1\mathbf{Y}_1 \oplus \ldots \oplus b_n\mathbf{Y}_n$的偏差值。

# S盒的线性逼近

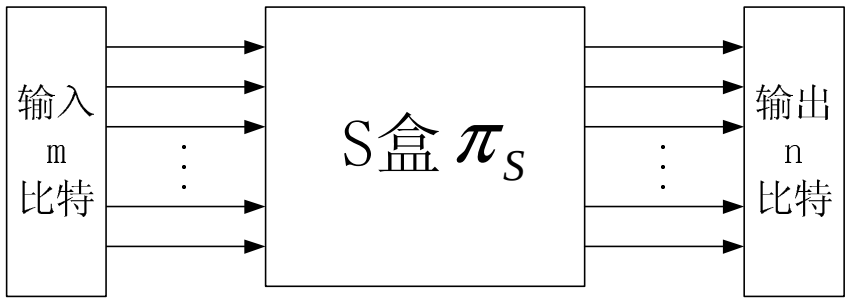
考虑$S$盒$\pi_S : \{0,1\}^m \to \{0,1\}^n$。




**定义：** 随机变量$\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m)$表示$m$重输入，
随机变量$\mathbf{Y} = (\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n)$表示$n$重输出。
**假定：** $\mathbf{X}_i (1 \le i \le m), \mathbf{Y}_j (1 \le j \le n)$独立同分布，均取值于$\{0,1\}$，而且偏差为0。
**计算：** 随机变量$a_1\mathbf{X}_1 \oplus \ldots \oplus a_m\mathbf{X}_m \oplus b_1\mathbf{Y}_1 \oplus \ldots \oplus b_n\mathbf{Y}_n$的偏差值。

# S盒的线性逼近

考虑$S$盒$\pi_S : \{0,1\}^m \to \{0,1\}^n$。




**定义：** 随机变量$\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m)$表示$m$重输入，
随机变量$\mathbf{Y} = (\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_n)$表示$n$重输出。
**假定：** $\mathbf{X}_i (1 \le i \le m), \mathbf{Y}_j (1 \le j \le n)$独立同分布，均取值于$\{0,1\}$，而且偏差为0。
**计算：** 随机变量$a_1\mathbf{X}_1 \oplus \ldots \oplus a_m\mathbf{X}_m \oplus b_1\mathbf{Y}_1 \oplus \ldots \oplus b_n\mathbf{Y}_n$的偏差值。

# S盒的线性逼近

首先求概率

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

# S盒的线性逼近

首先求概率

根据全概率公式：

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

$$= \sum_{(\bigoplus_{i=1}^{m} a_i x_i) \oplus (\bigoplus_{j=1}^{n} b_j y_j) = 0} P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m) \cdot P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$$

## S盒的线性逼近

计算概率$P(\mathbf{Y}_j = y_j, 1 \leq j \leq n, \mathbf{X}_i = x_i, 1 \leq i \leq m)$

$P(\mathbf{Y}_j = y_j, 1 \leq j \leq n | \mathbf{X}_i = x_i, 1 \leq i \leq m)$

## S盒的线性逼近

计算概率$P(\mathbf{Y}_j = y_j, 1 \leq j \leq n, \mathbf{X}_i = x_i, 1 \leq i \leq m)$

$$P(\mathbf{Y}_j = y_j, 1 \leq j \leq n | \mathbf{X}_i = x_i, 1 \leq i \leq m)$$

分两种情况讨论：

## S盒的线性逼近

计算概率$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m)$$

分两种情况讨论：

情况一：$(y_1, \ldots, y_n) \neq \pi_S(x_1, \ldots, x_m)$,

情况二：$(y_1, \ldots, y_n) = \pi_S(x_1, \ldots, x_m)$,

## S盒的线性逼近

计算概率$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m)$$

分两种情况讨论：

**情况一：** $(y_1, \ldots, y_n) \neq \pi_S(x_1, \ldots, x_m)$，有

$$P(\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m, \mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n) = 0$$

**情况二：** $(y_1, \ldots, y_n) = \pi_S(x_1, \ldots, x_m)$，

## S盒的线性逼近

计算概率$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$

$P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m)$

分两种情况讨论：

情况一：$(y_1, \ldots, y_n) \neq \pi_S(x_1, \ldots, x_m)$，有

$$P(\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m, \mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n) = 0$$

情况二：$(y_1, \ldots, y_n) = \pi_S(x_1, \ldots, x_m)$，有

$$P(\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m, \mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n)$$
$$= P(\mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m) = 2^{-m}$$

并且

$$P(\mathbf{Y}_1 = y_1, \ldots, \mathbf{Y}_n = y_n | \mathbf{X}_1 = x_1, \ldots, \mathbf{X}_m = x_m) = 1$$

# S盒的线性逼近

## 继续刚才的计算

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

$$= \sum_{(\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j) = 0} P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m) \cdot$$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$$

# S盒的线性逼近

继续刚才的计算

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

$$= \sum_{(\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j) = 0} P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m) \cdot$$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$$

# S盒的线性逼近

继续刚才的计算

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

$$= \sum_{(\oplus_{i=1}^{m} a_i x_i)\oplus(\oplus_{j=1}^{n} b_j y_j)=0} P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m) \cdot$$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$$

$$= \frac{|\{x_1, \ldots, x_m, y_1, \ldots, y_m : (y_1, \ldots, y_m) = \pi_S(x_1, \ldots, x_m), (\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j) = 0\}|}{2^m}$$

# S盒的线性逼近

继续刚才的计算

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

$$= \sum_{(\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j) = 0} P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m) \cdot$$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$$

$$= \frac{|\{x_1, \ldots, x_m, y_1, \ldots, y_m : (y_1, \ldots, y_m) = \pi_S(x_1, \ldots, x_m), (\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j) = 0\}|}{2^m}$$

记

$$N_L = |\{x_1, \ldots, x_m, y_1, \ldots, y_m : (y_1, \ldots, y_m) = \pi_S(x_1, \ldots, x_m), (\bigoplus_{i=1}^{m} a_i x_i) \oplus (\bigoplus_{j=1}^{n} b_j y_j) = 0\}|$$

# S盒的线性逼近

## 继续刚才的计算

$$P((\bigoplus_{i=m} a_i \mathbf{X}_i) \oplus (\bigoplus_{j=1}^{n} b_j \mathbf{Y}_j) = 0)$$

$$= \sum_{(\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j)=0} P(\mathbf{Y}_j = y_j, 1 \le j \le n | \mathbf{X}_i = x_i, 1 \le i \le m) \cdot$$

$$P(\mathbf{Y}_j = y_j, 1 \le j \le n, \mathbf{X}_i = x_i, 1 \le i \le m)$$

$$= \frac{|\{x_1, \ldots, x_m, y_1, \ldots, y_m : (y_1, \ldots, y_m) = \pi_S(x_1, \ldots, x_m), (\oplus_{i=1}^{m} a_i x_i) \oplus (\oplus_{j=1}^{n} b_j y_j) = 0\}|}{2^m}$$

记

$$N_L = |\{x_1, \ldots, x_m, y_1, \ldots, y_m : (y_1, \ldots, y_m) = \pi_S(x_1, \ldots, x_m), (\bigoplus_{i=1}^{m} a_i x_i) \oplus (\bigoplus_{j=1}^{n} b_j y_j) = 0\}|$$

那么偏差为$N_L/2^m - 1/2$。

# S盒的线性逼近–例3.2

**问题：**考虑例3.1中的$S$盒，$\pi_S$：$\{0,1\}^4 \to \{0,1\}^4$如右图所示。
求$\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_4$的偏差。

| $\mathbf{X}_1$ | $\mathbf{X}_2$ | $\mathbf{X}_3$ | $\mathbf{X}_4$ | $\mathbf{Y}_1$ | $\mathbf{Y}_2$ | $\mathbf{Y}_3$ | $\mathbf{Y}_4$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |

# S盒的线性逼近–例3.2

**问题：**考虑例3.1中的$S$盒，$\pi_S$：$\{0,1\}^4 \to \{0,1\}^4$如右图所示。

求$\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_4$的偏差。

$N_L$ = 满足$x_3 \oplus x_4 \oplus y_1 \oplus y_4 = 0$的输入输出对的数量

| $\mathbf{X}_1$ | $\mathbf{X}_2$ | $\mathbf{X}_3$ | $\mathbf{X}_4$ | $\mathbf{Y}_1$ | $\mathbf{Y}_2$ | $\mathbf{Y}_3$ | $\mathbf{Y}_4$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |

# S盒的线性逼近–例3.2

**问题：**考虑例3.1中的$S$盒，$\pi_S$：$\{0,1\}^4 \to \{0,1\}^4$如右图所示。

求$\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_4$的偏差。

$N_L =$ 满足$x_3 \oplus x_4 \oplus y_1 \oplus y_4 = 0$的输入输出对的数量

| $\mathbf{X}_1$ | $\mathbf{X}_2$ | $\mathbf{X}_3$ | $\mathbf{X}_4$ | $\mathbf{Y}_1$ | $\mathbf{Y}_2$ | $\mathbf{Y}_3$ | $\mathbf{Y}_4$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |

# S盒的线性逼近–例3.2

**问题：**考虑例3.1中的$S$盒，$\pi_S$：$\{0,1\}^4 \to \{0,1\}^4$如右图所示。

求$\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_4$的偏差。

$N_L$ = 满足$x_3 \oplus x_4 \oplus y_1 \oplus y_4 = 0$的输入输出对的数量=2

| $\mathbf{X}_1$ | $\mathbf{X}_2$ | $\mathbf{X}_3$ | $\mathbf{X}_4$ | $\mathbf{Y}_1$ | $\mathbf{Y}_2$ | $\mathbf{Y}_3$ | $\mathbf{Y}_4$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |

# S盒的线性逼近–例3.2

**问题：**考虑例3.1中的$S$盒，$\pi_S$：$\{0,1\}^4 \to \{0,1\}^4$如右图所示。

求$\mathbf{X}_3 \oplus \mathbf{X}_4 \oplus \mathbf{Y}_1 \oplus \mathbf{Y}_4$的偏差。

$N_L =$ 满足$x_3 \oplus x_4 \oplus y_1 \oplus y_4 = 0$的输入输出对的数量=2

因此偏差$= N_L/16 - 1/2 = 2/16 - 1/2 = -3/8$

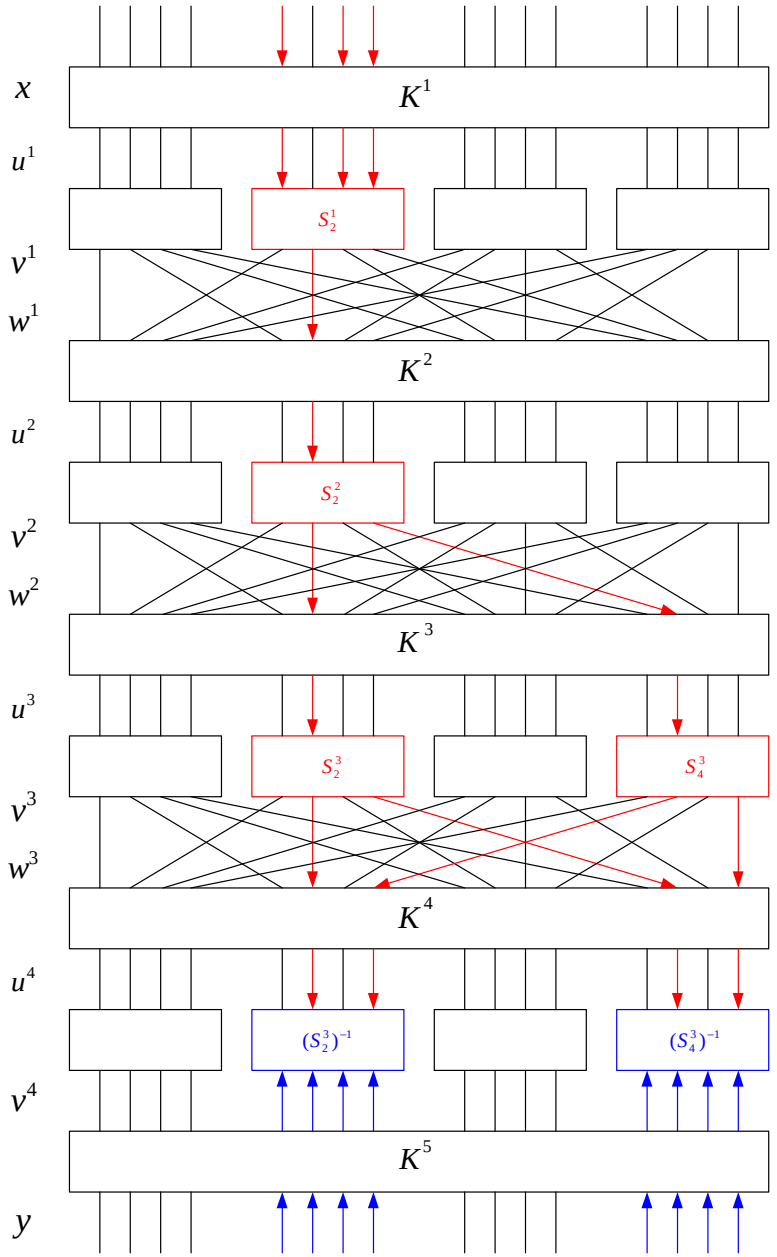
| $\mathbf{X}_1$ | $\mathbf{X}_2$ | $\mathbf{X}_3$ | $\mathbf{X}_4$ | $\mathbf{Y}_1$ | $\mathbf{Y}_2$ | $\mathbf{Y}_3$ | $\mathbf{Y}_4$ |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |

包含所有$N_L$的值表称为线性逼近表。例3.1的$S$盒的线性逼近表见课本图3.2，由所有$N_L$值能求出所有输入输出的线性组合的偏差。

3.3.2节习题：练习3.12*，3.14(a)。

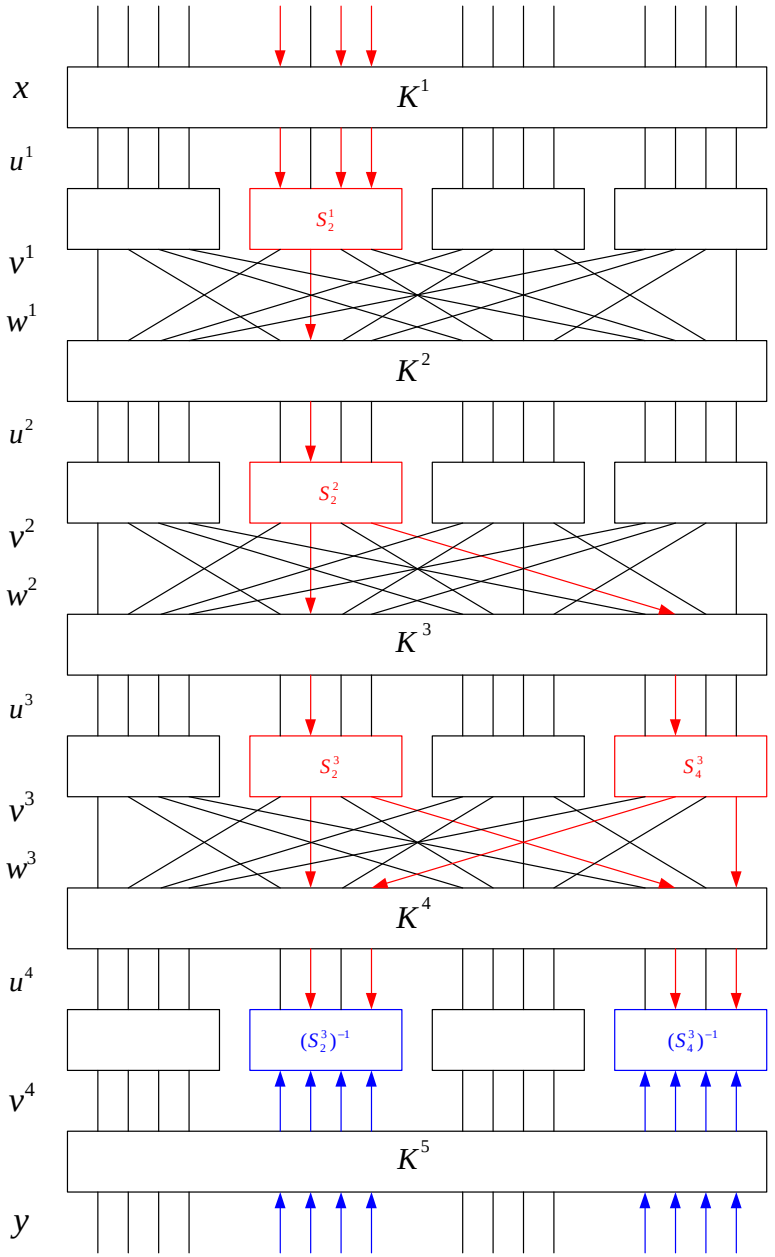
# 对例3.1的线性密码分析

| $S$盒 | 随机变量 | 偏差 |
|---|---|---|
| $S_2^1$ | $\mathbf{T}_1 = \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1$ | $1/4$ |
| $S_2^2$ | $\mathbf{T}_2 = \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2$ | $-1/4$ |
| $S_2^3$ | $\mathbf{T}_3 = \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3$ | $-1/4$ |
| $S_4^3$ | $\mathbf{T}_4 = \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3$ | $-1/4$ |



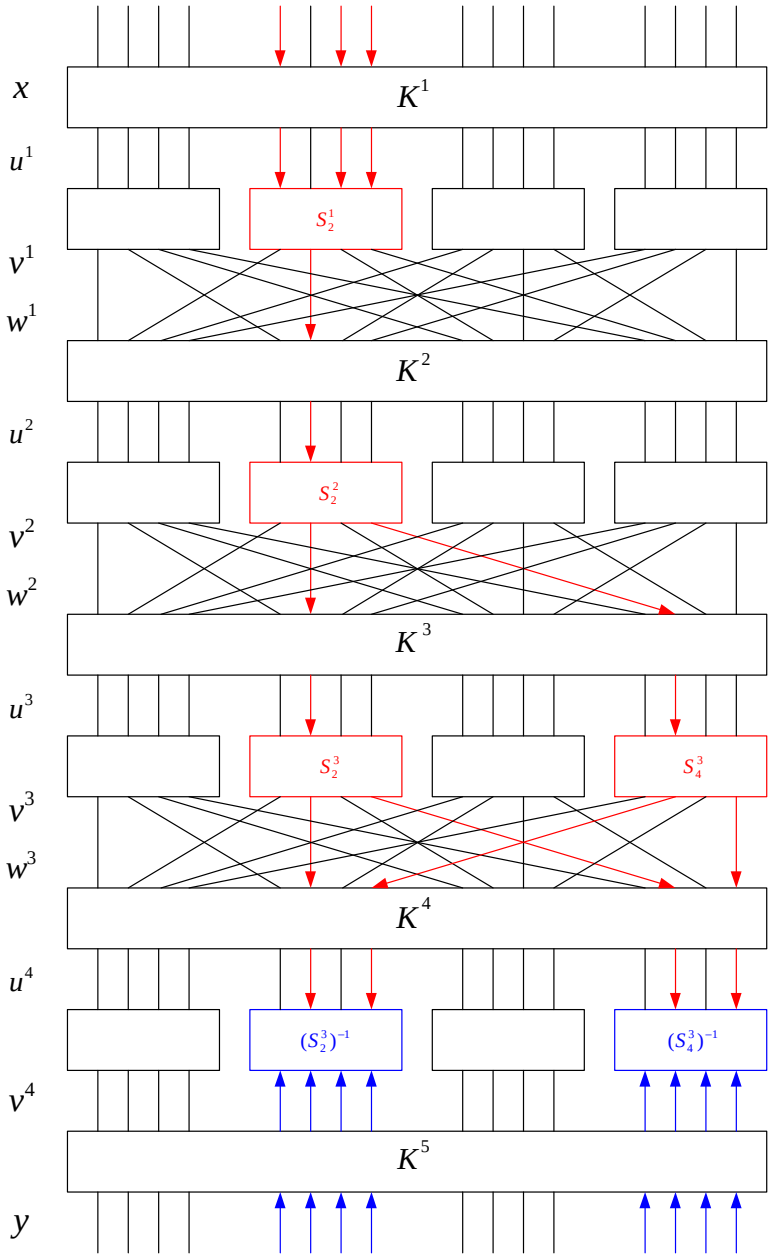
# 对例3.1的线性密码分析

| $S$盒 | 随机变量 | 偏差 |
|---|---|---|
| $S_2^1$ | $\mathbf{T}_1 = \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1$ | $1/4$ |
| $S_2^2$ | $\mathbf{T}_2 = \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2$ | $-1/4$ |
| $S_2^3$ | $\mathbf{T}_3 = \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3$ | $-1/4$ |
| $S_4^3$ | $\mathbf{T}_4 = \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3$ | $-1/4$ |



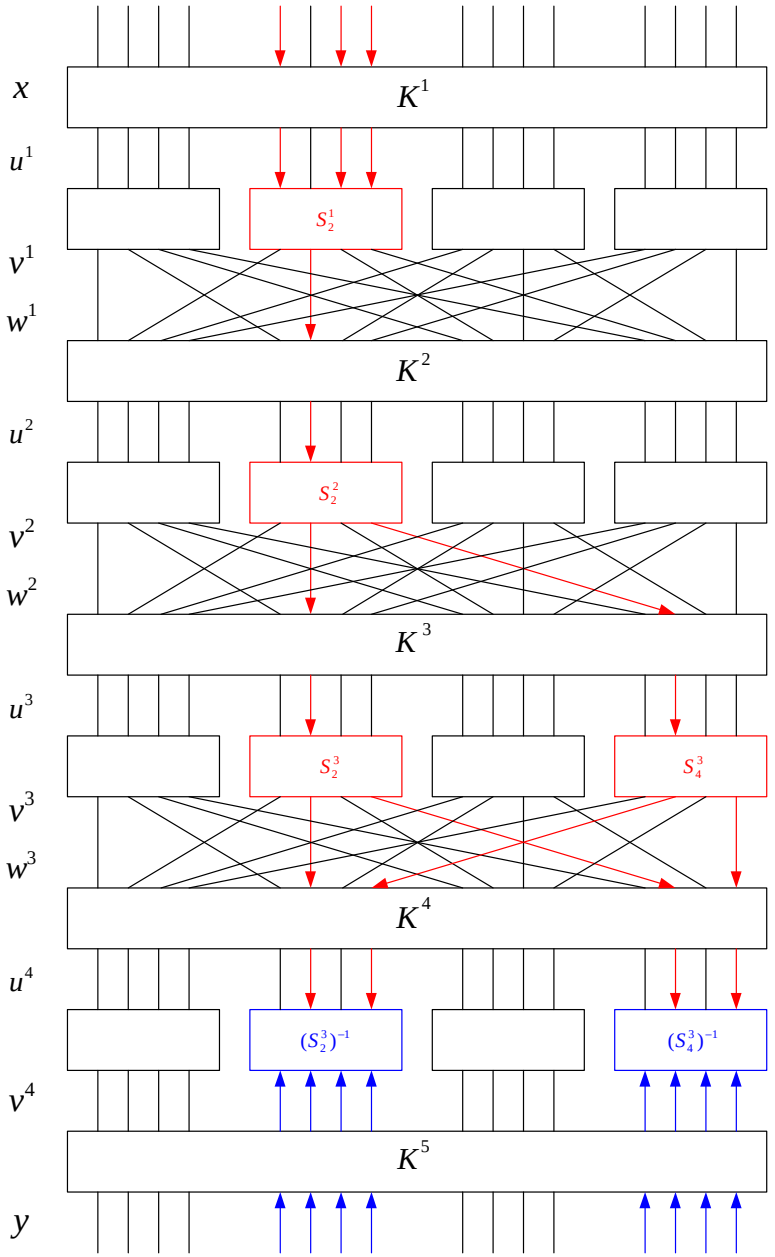
# 对例3.1的线性密码分析

| $S$盒 | 随机变量 | 偏差 |
|---|---|---|
| $S_2^1$ | $\mathbf{T}_1 = \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1$ | $1/4$ |
| $S_2^2$ | $\mathbf{T}_2 = \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2$ | $-1/4$ |
| $S_2^3$ | $\mathbf{T}_3 = \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3$ | $-1/4$ |
| $S_4^3$ | $\mathbf{T}_4 = \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3$ | $-1/4$ |



# 对例3.1的线性密码分析

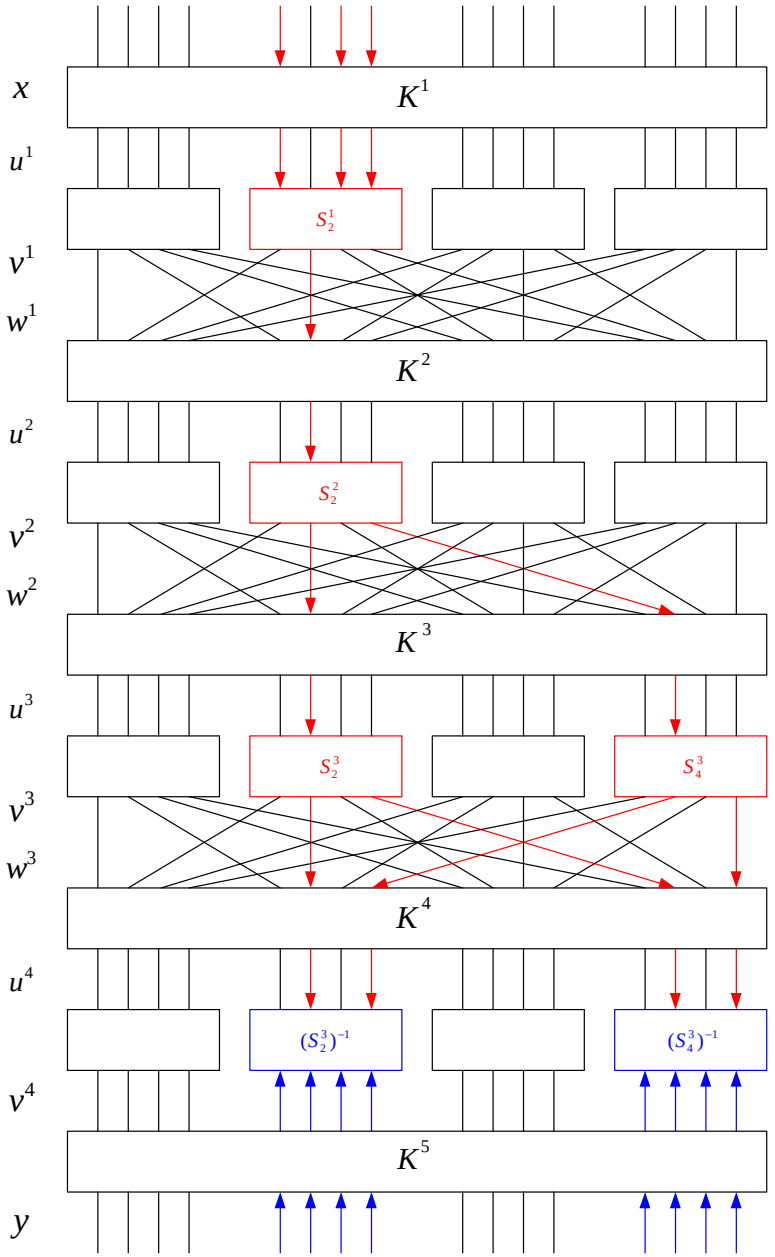
| $S$盒 | 随机变量 | 偏差 |
|---|---|---|
| $S_2^1$ | $\mathbf{T}_1 = \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1$ | $1/4$ |
| $S_2^2$ | $\mathbf{T}_2 = \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2$ | $-1/4$ |
| $S_2^3$ | $\mathbf{T}_3 = \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3$ | $-1/4$ |
| $S_4^3$ | $\mathbf{T}_4 = \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3$ | $-1/4$ |



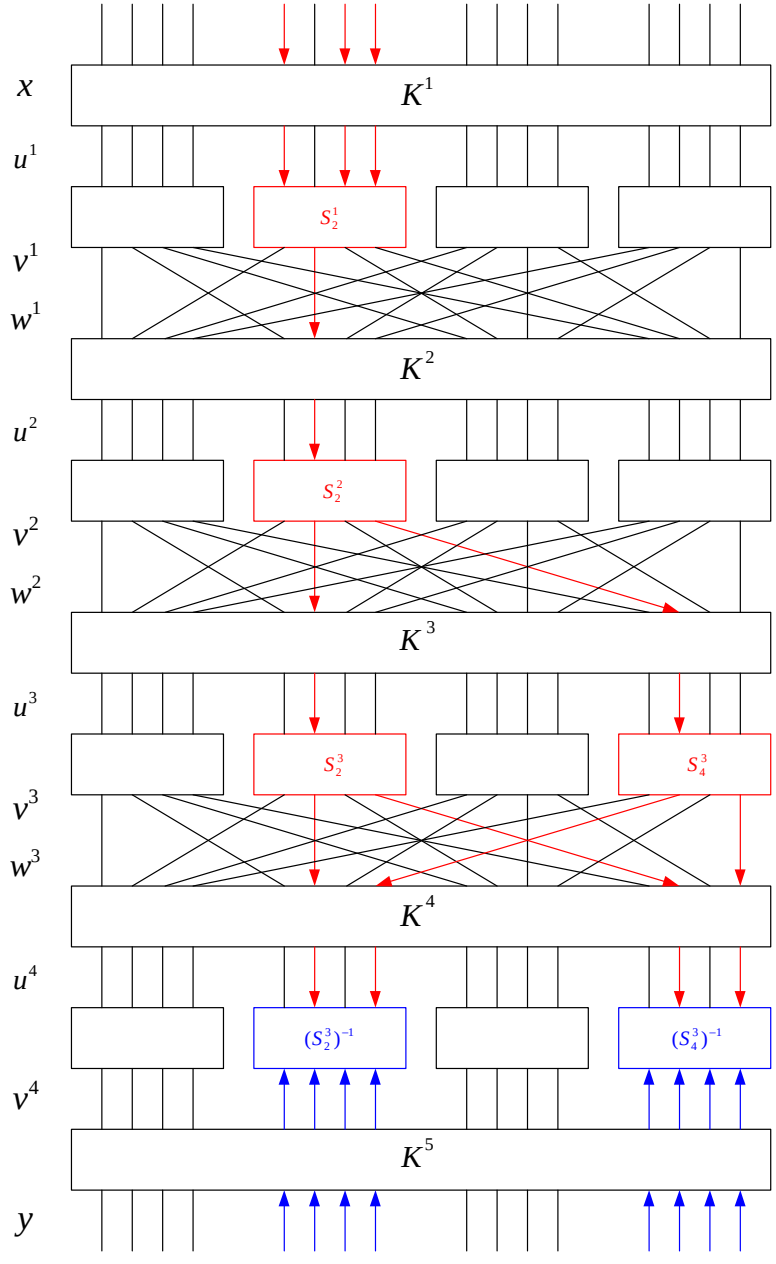
# 对例3.1的线性密码分析

| $S$盒 | 随机变量 | 偏差 |
|---|---|---|
| $S_2^1$ | $\mathbf{T}_1 = \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1$ | $1/4$ |
| $S_2^2$ | $\mathbf{T}_2 = \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2$ | $-1/4$ |
| $S_2^3$ | $\mathbf{T}_3 = \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3$ | $-1/4$ |
| $S_4^3$ | $\mathbf{T}_4 = \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3$ | $-1/4$ |

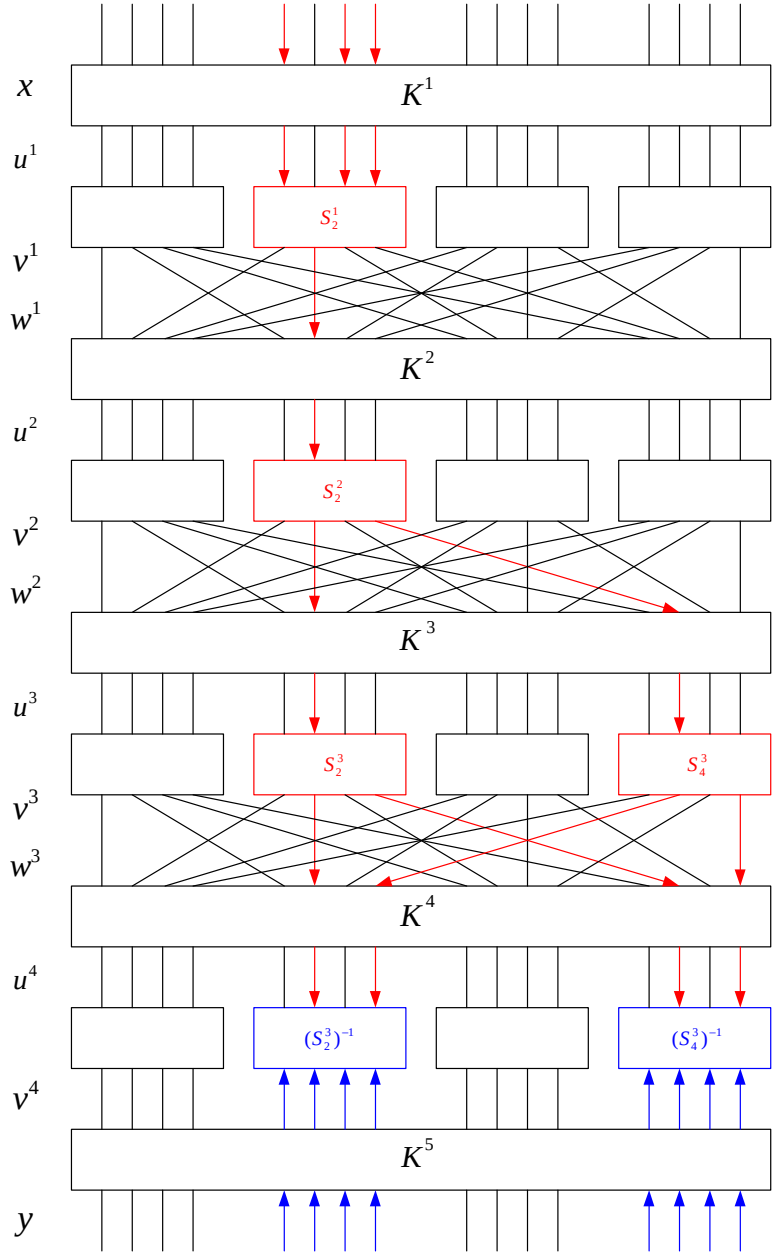
$\mathbf{T}_1 \oplus \mathbf{T}_2 \oplus \mathbf{T}_3 \oplus \mathbf{T}_4$的偏差$=2^3(1/4)(-1/4)^3 = -1/32$



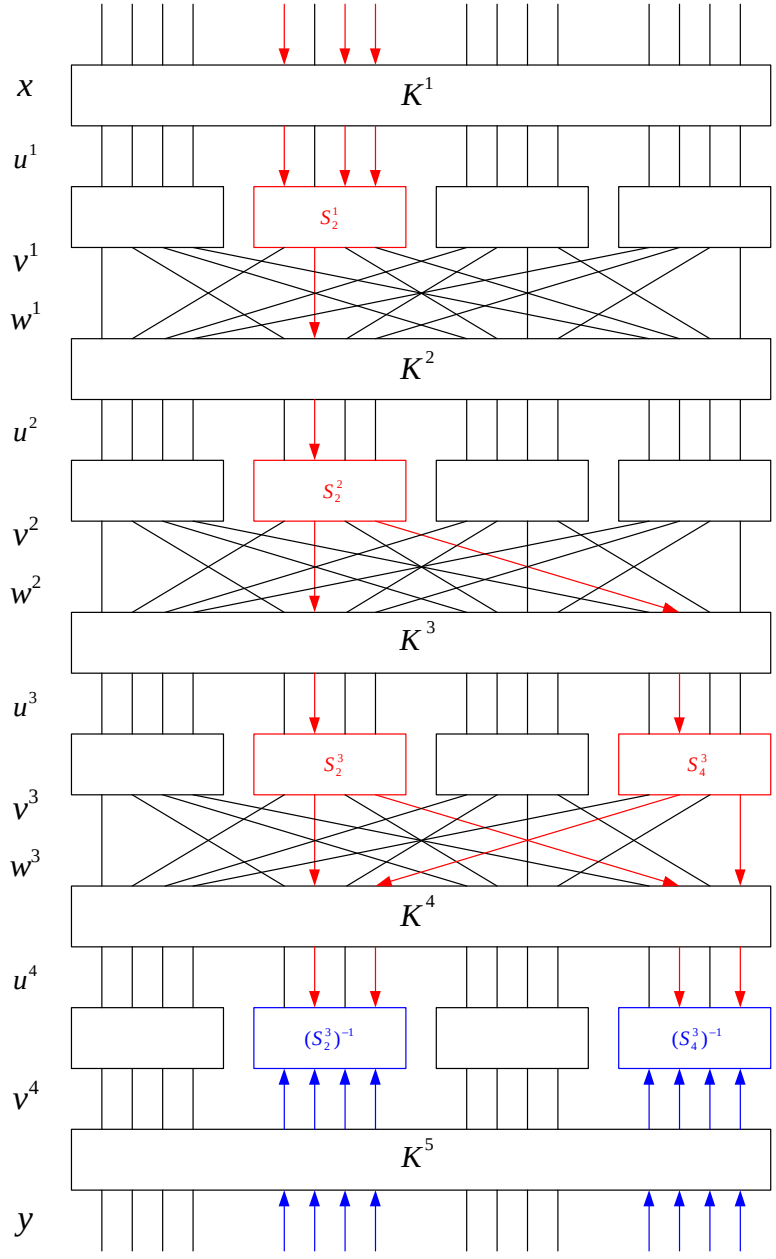
$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
&= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
&= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
&= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3
\end{aligned}
$$



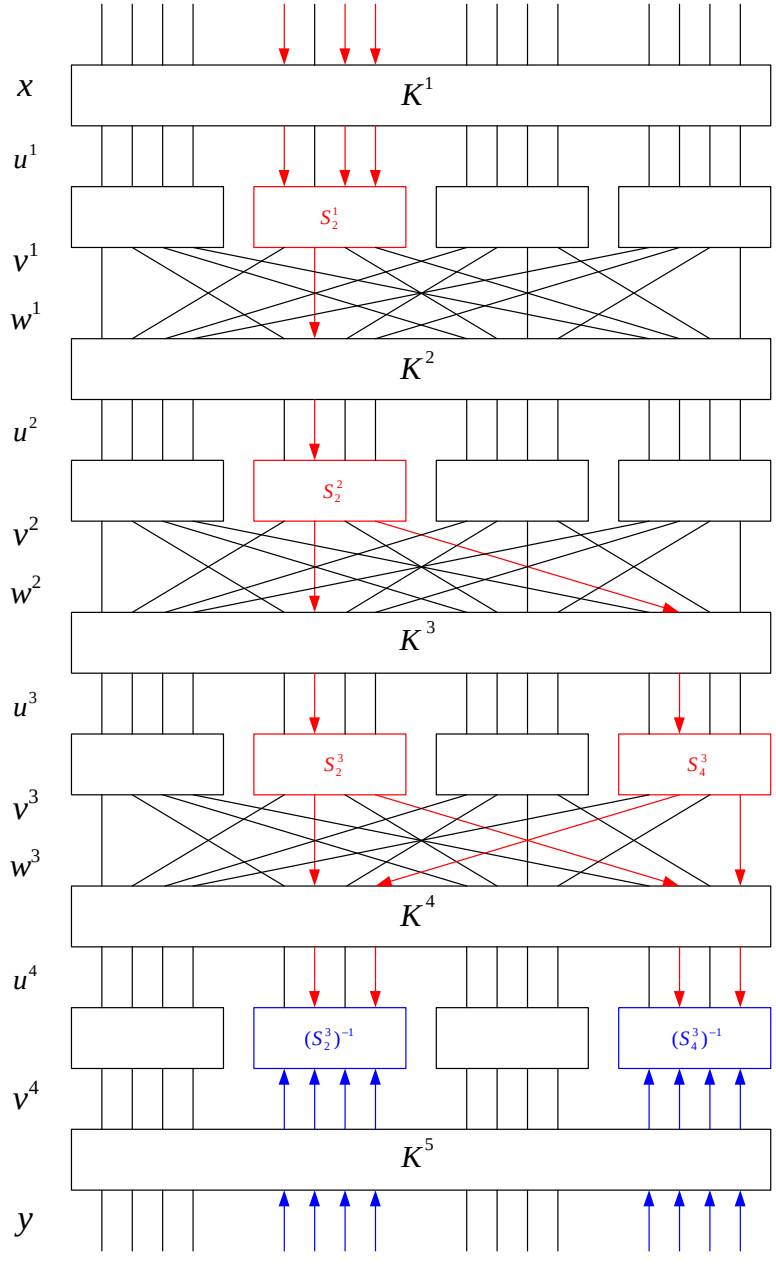
$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
&= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
&= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
&= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3
\end{aligned}
$$



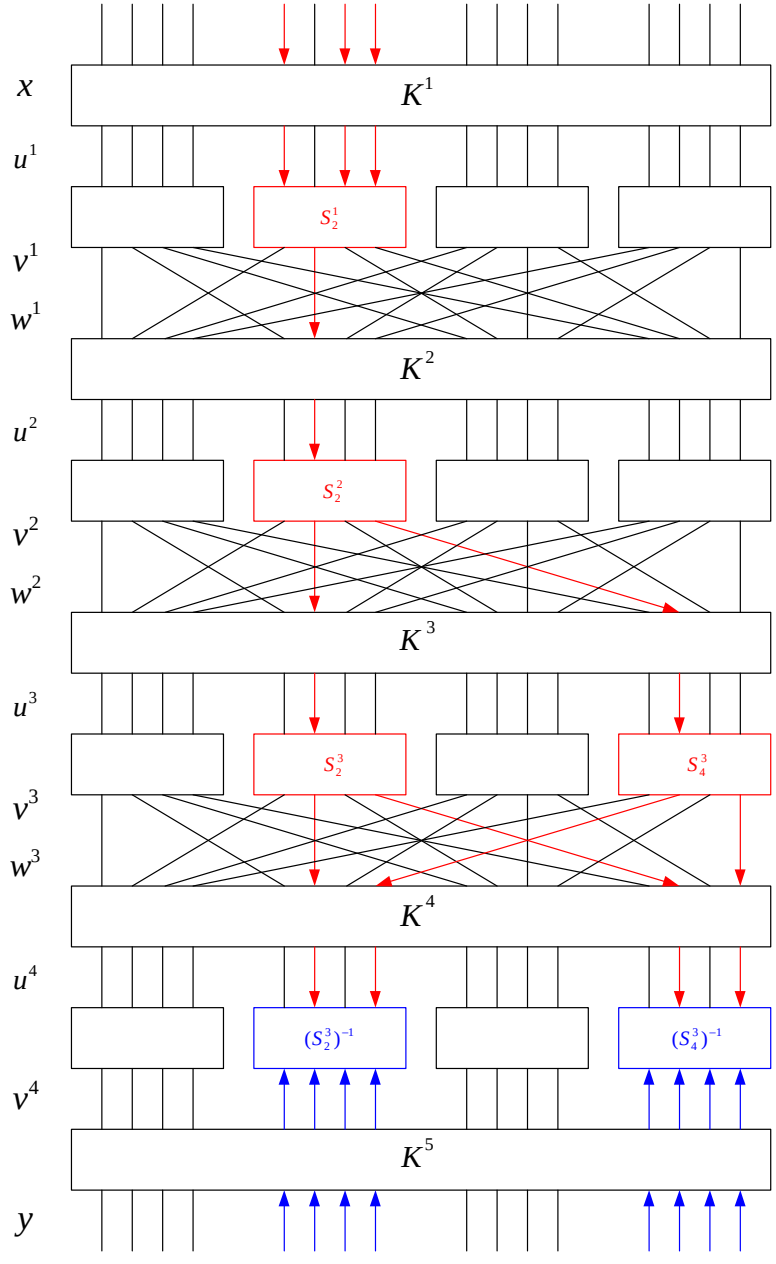
$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
&= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
&= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
&= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3
\end{aligned}
$$



$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
&= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
&= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
&= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3
\end{aligned}
$$



$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
\oplus \quad &= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\oplus \quad &= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\oplus \quad &= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
\oplus \quad &= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
\Downarrow & \\
& \mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
& \mathbf{K}_5^1 \oplus \oplus \mathbf{K}_7^1 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_{14}^3
\end{aligned}
$$



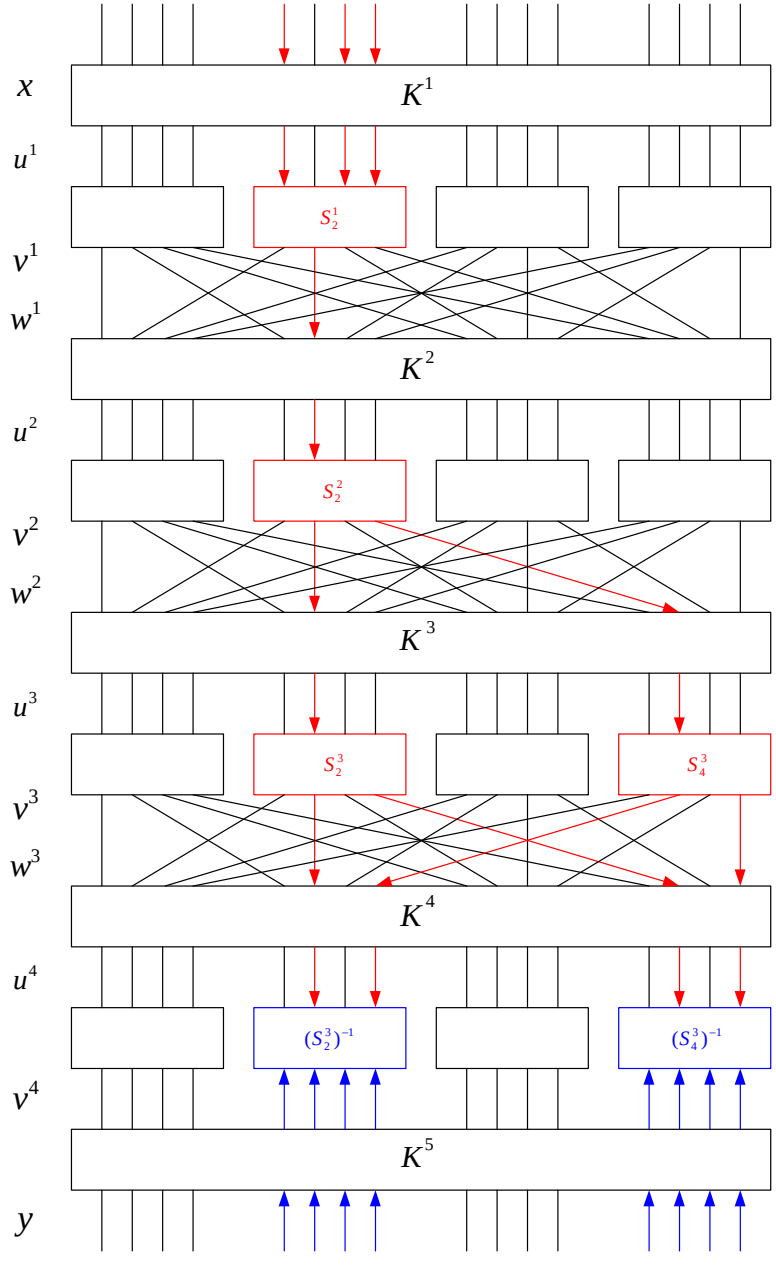
$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
\oplus &= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\oplus &= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\oplus &= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
\oplus &= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&\Downarrow \\
&\mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&\mathbf{K}_5^1 \oplus \oplus \mathbf{K}_7^1 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_{14}^3
\end{aligned}
$$

代入 $\mathbf{V}_6^3 = \mathbf{U}_6^4 \oplus \mathbf{K}_8^4 \quad \mathbf{V}_8^3 = \mathbf{U}_{14}^4 \oplus \mathbf{K}_{14}^4$

$\mathbf{V}_{14}^3 = \mathbf{U}_8^4 \oplus \mathbf{K}_8^4 \quad \mathbf{V}_{16}^3 = \mathbf{U}_{16}^4 \oplus \mathbf{K}_{16}^4$

$\Downarrow$

$$
\begin{aligned}
&\mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{U}_6^4 \oplus \mathbf{U}_8^4 \oplus \mathbf{U}_{14}^4 \oplus \mathbf{U}_{16}^4 \\
&\oplus \mathbf{K}_5^1 \oplus \mathbf{K}_7^1 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{K}_{14}^3 \oplus \\
&\mathbf{K}_6^4 \oplus \mathbf{K}_8^4 \oplus \mathbf{K}_{14}^4 \oplus \mathbf{K}_{16}^4
\end{aligned}
$$



$$
\begin{aligned}
\mathbf{T}_1 &= \mathbf{U}_5^1 \oplus \mathbf{U}_7^1 \oplus \mathbf{U}_8^1 \oplus \mathbf{V}_6^1 \\
\oplus &= \mathbf{X}_5 \oplus \mathbf{K}_5^1 \oplus \mathbf{X}_7 \oplus \mathbf{K}_7^1 \oplus \mathbf{X}_8 \oplus \mathbf{K}_8^1 \oplus \mathbf{V}_6^1 \\
\mathbf{T}_2 &= \mathbf{U}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\oplus &= \mathbf{V}_6^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{V}_6^2 \oplus \mathbf{V}_8^2 \\
\mathbf{T}_3 &= \mathbf{U}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\oplus &= \mathbf{V}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \\
\mathbf{T}_4 &= \mathbf{U}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
\oplus &= \mathbf{V}_8^2 \oplus \mathbf{K}_{14}^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&\Downarrow \\
&\mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{V}_6^3 \oplus \mathbf{V}_8^3 \oplus \mathbf{V}_{14}^3 \oplus \mathbf{V}_{16}^3 \\
&\mathbf{K}_5^1 \oplus \oplus \mathbf{K}_7^1 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_{14}^3
\end{aligned}
$$

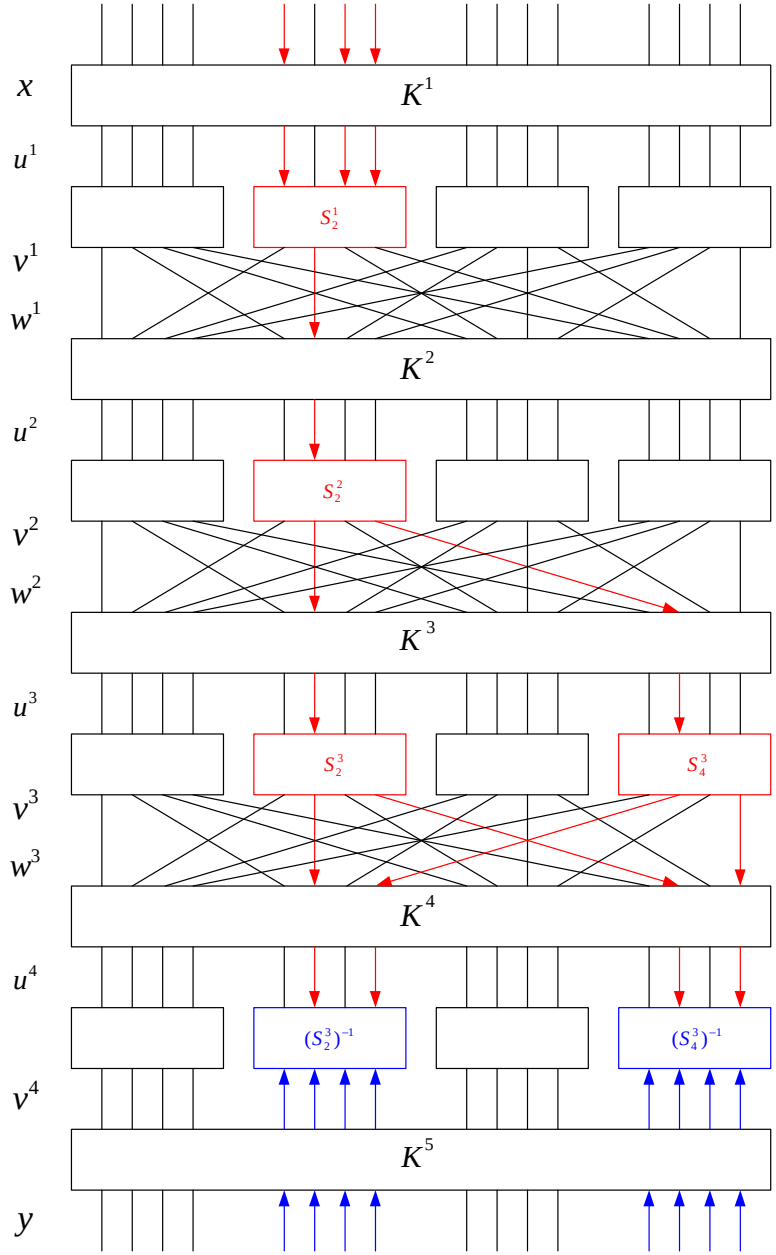
代入 $\mathbf{V}_6^3 = \mathbf{U}_6^4 \oplus \mathbf{K}_8^4 \quad \mathbf{V}_8^3 = \mathbf{U}_{14}^4 \oplus \mathbf{K}_{14}^4$

$\mathbf{V}_{14}^3 = \mathbf{U}_8^4 \oplus \mathbf{K}_8^4 \quad \mathbf{V}_{16}^3 = \mathbf{U}_{16}^4 \oplus \mathbf{K}_{16}^4$

$\Downarrow$

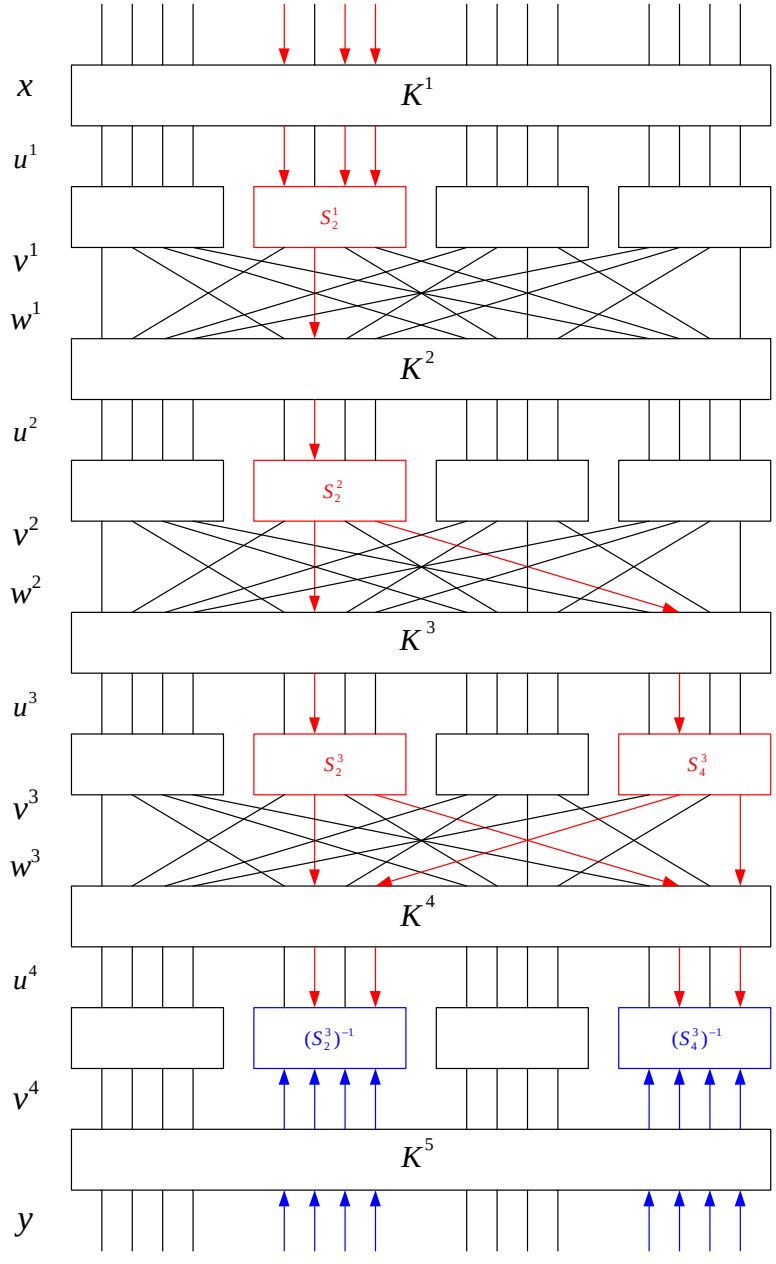
$$
\begin{aligned}
&\mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{U}_6^4 \oplus \mathbf{U}_8^4 \oplus \mathbf{U}_{14}^4 \oplus \mathbf{U}_{16}^4 \\
&\oplus \mathbf{K}_5^1 \oplus \mathbf{K}_7^1 \oplus \mathbf{K}_8^1 \oplus \mathbf{K}_6^2 \oplus \mathbf{K}_6^3 \oplus \mathbf{K}_{14}^3 \oplus \\
&\mathbf{K}_6^4 \oplus \mathbf{K}_8^4 \oplus \mathbf{K}_{14}^4 \oplus \mathbf{K}_{16}^4 \\
&\mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{U}_6^4 \oplus \mathbf{U}_8^4 \oplus \mathbf{U}_{14}^4 \oplus \mathbf{U}_{16}^4
\end{aligned}
$$

偏差= $\pm 1/32$



线性分析算法：

已知：$T \approx 8000$对明-密文

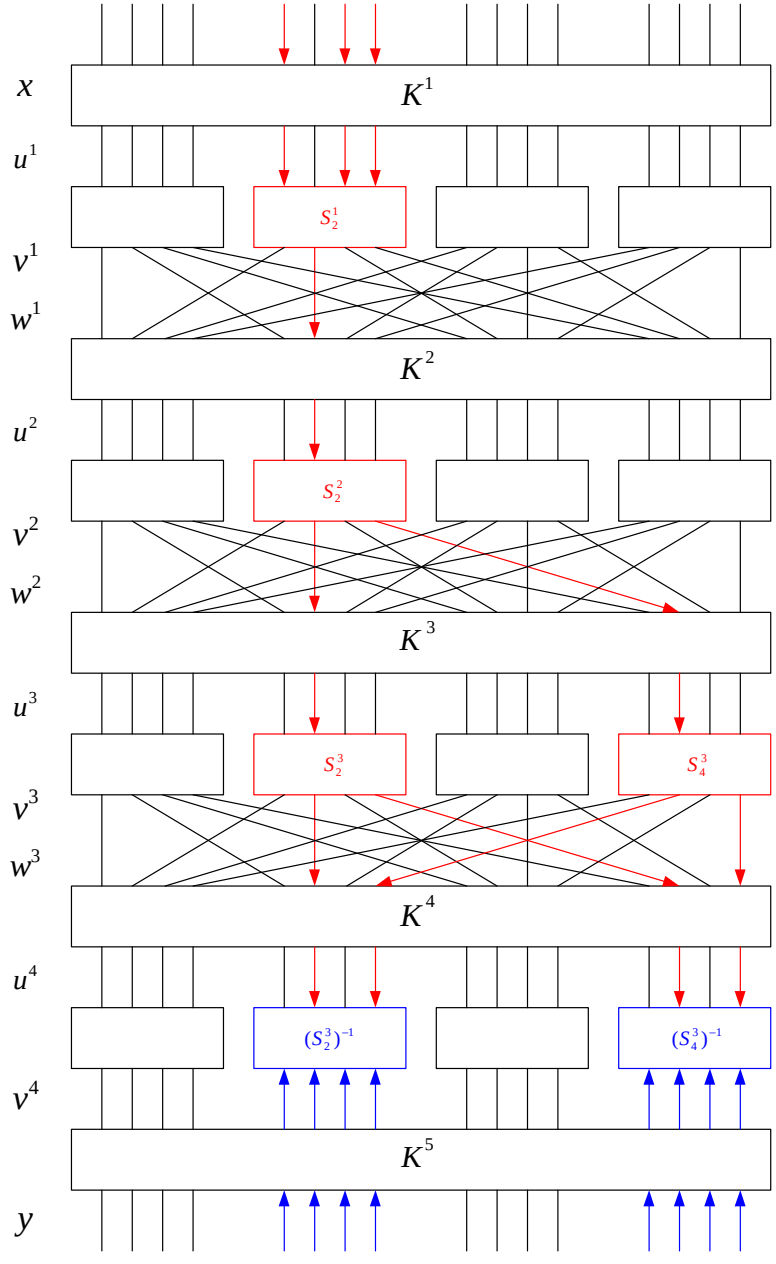



输出：$K_5^5, K_6^5, K_7^5, K_8^5$
$K_{13}^5, K_{14}^5, K_{15}^5, K_{16}^5$

线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：



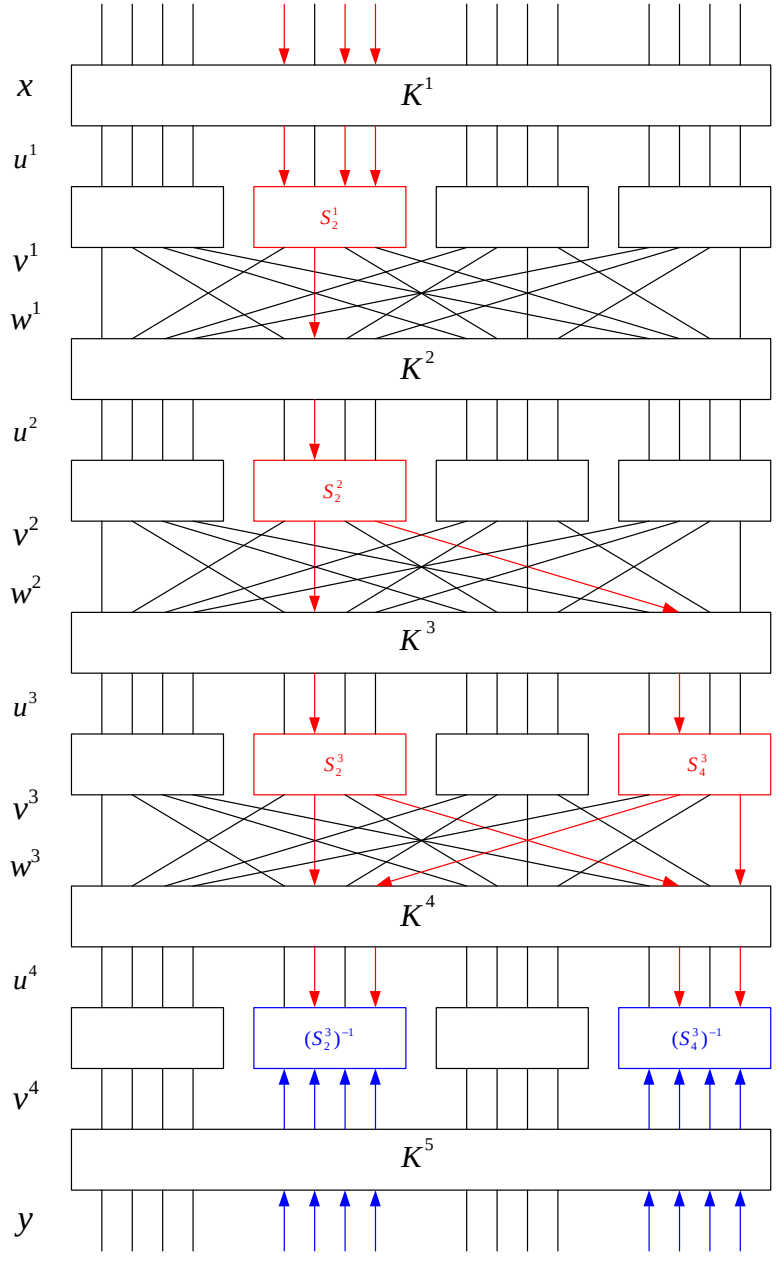

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$

线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$




输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$

线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

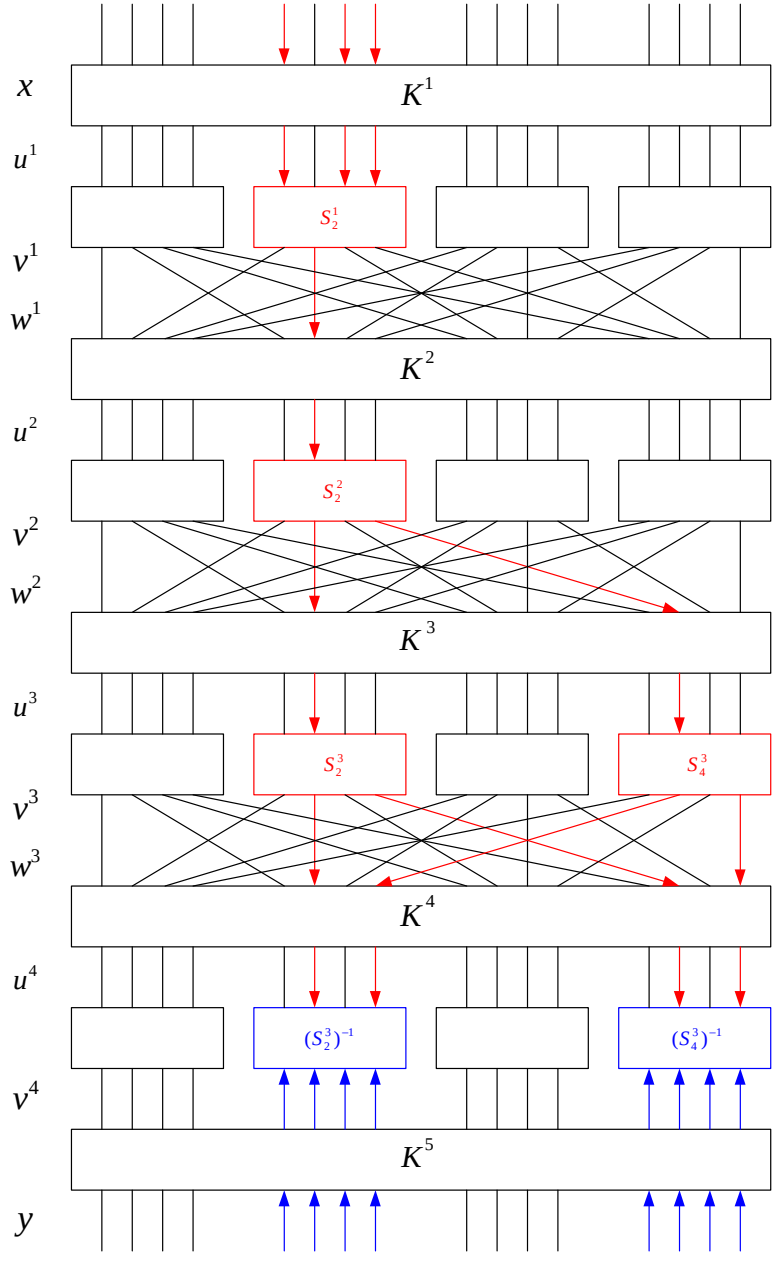
**Step 2.1**($\pi_P$) $v_2^4 \leftarrow L_1 \oplus y_2$,
$v_4^4 \leftarrow L_1 \oplus y_4$.

**Step 2.2**($\pi_S^{-1}$) $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$,
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4**(计数) 如果$z = 0$
则$Count[L_1, L_2] + +$

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$



线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

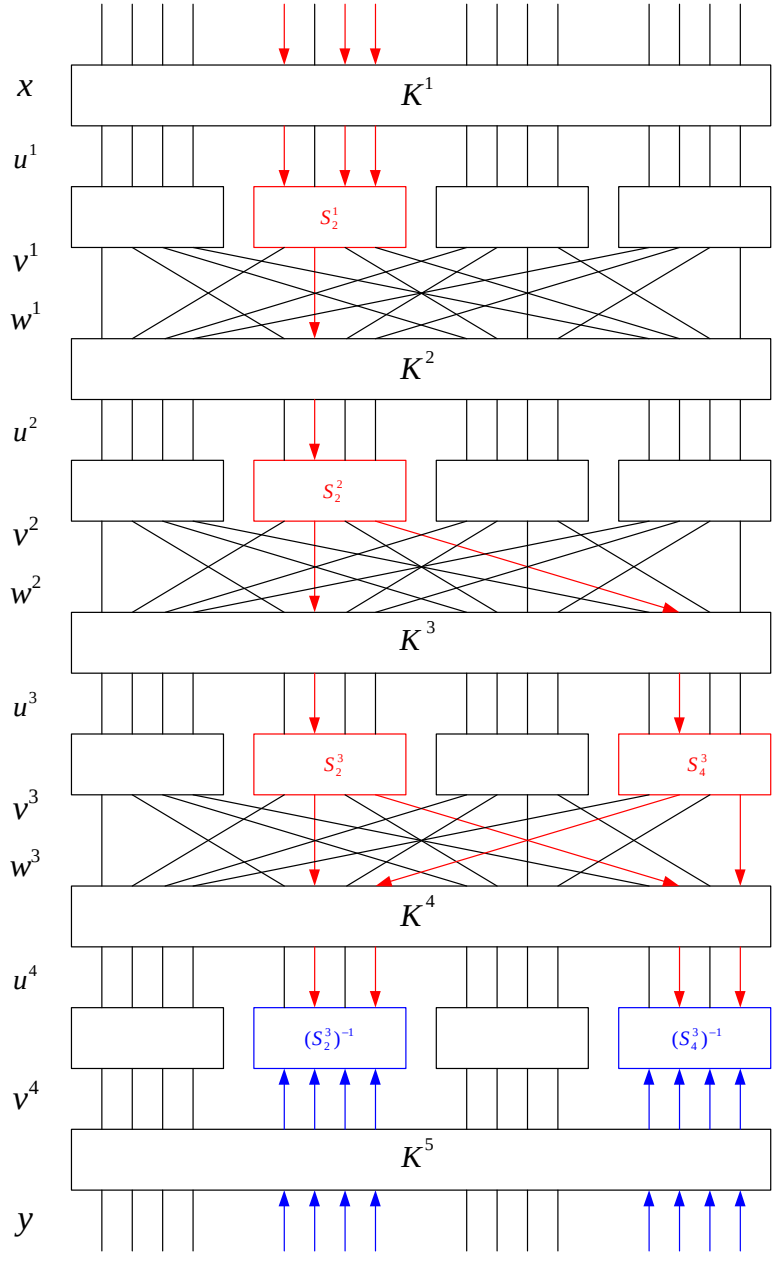
**Step 2.1**($\pi_P$) $v_2^4 \leftarrow L_1 \oplus y_2$,
$v_4^4 \leftarrow L_1 \oplus y_4$.

**Step 2.2**($\pi_S^{-1}$) $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$,
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4**(计数) 如果$z = 0$
则$Count[L_1, L_2] + +$

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$



线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

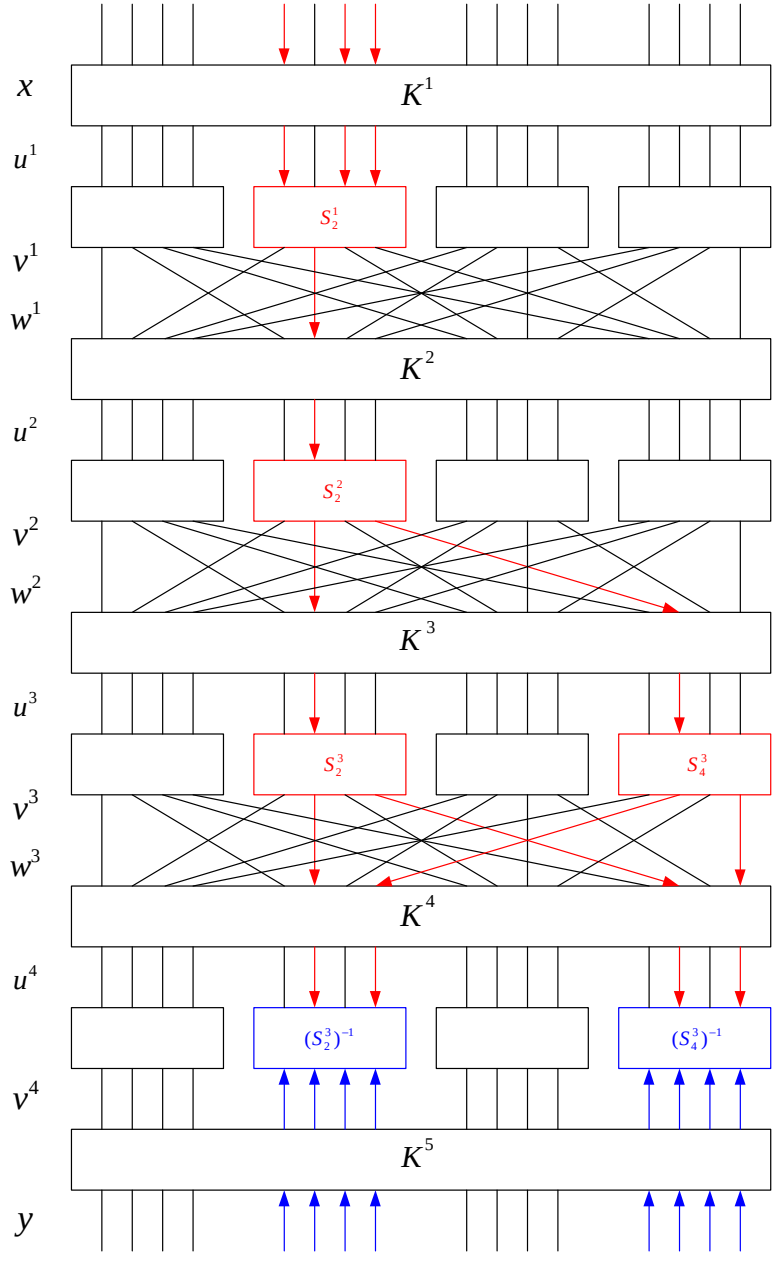
**Step 2.1**($\pi_P$) $v_2^4 \leftarrow L_1 \oplus y_2$，
$v_4^4 \leftarrow L_1 \oplus y_4$.

**Step 2.2**($\pi_S^{-1}$) $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$，
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4**(计数) 如果$z = 0$
则$Count[L_1, L_2] + +$

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$



线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

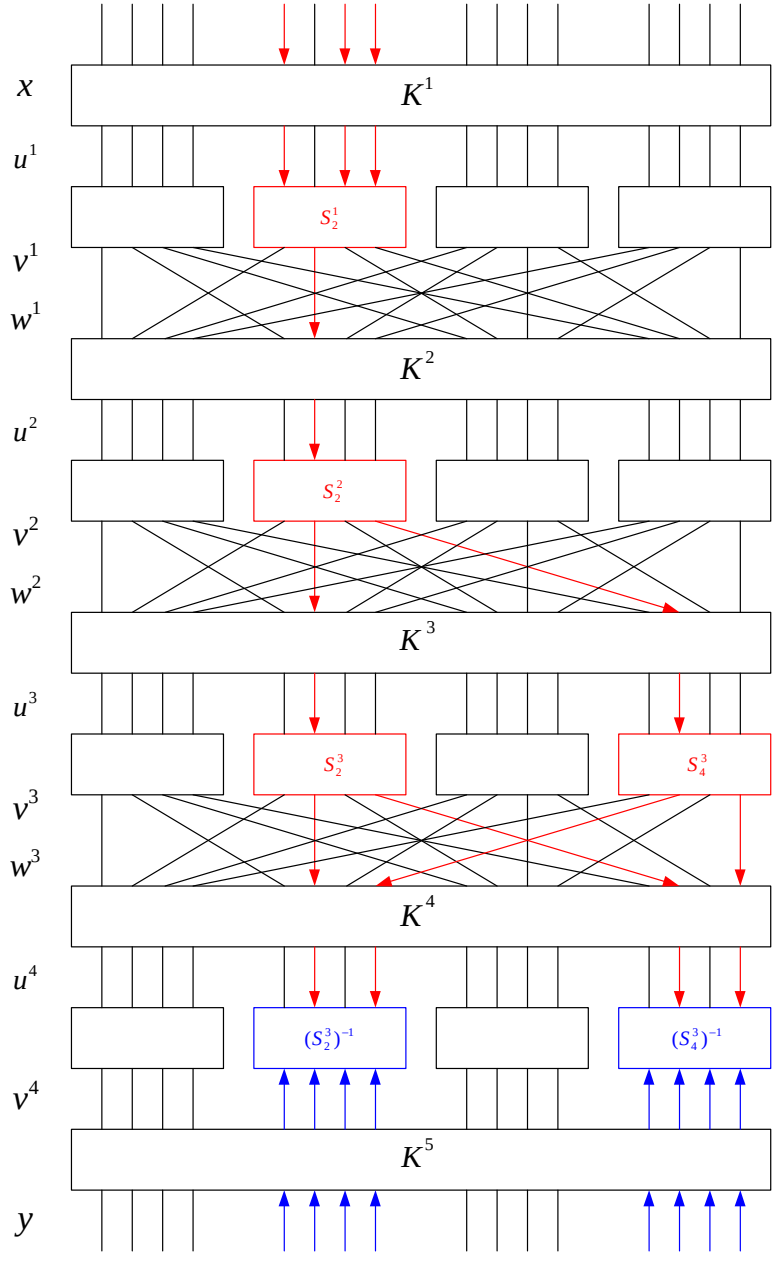
**Step 2.1**($\pi_P$) $v_2^4 \leftarrow L_1 \oplus y_2$,
$v_4^4 \leftarrow L_1 \oplus y_4$.

**Step 2.2**($\pi_S^{-1}$) $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$,
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4**(计数) 如果$z = 0$
则$Count[L_1, L_2]++$

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$



线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

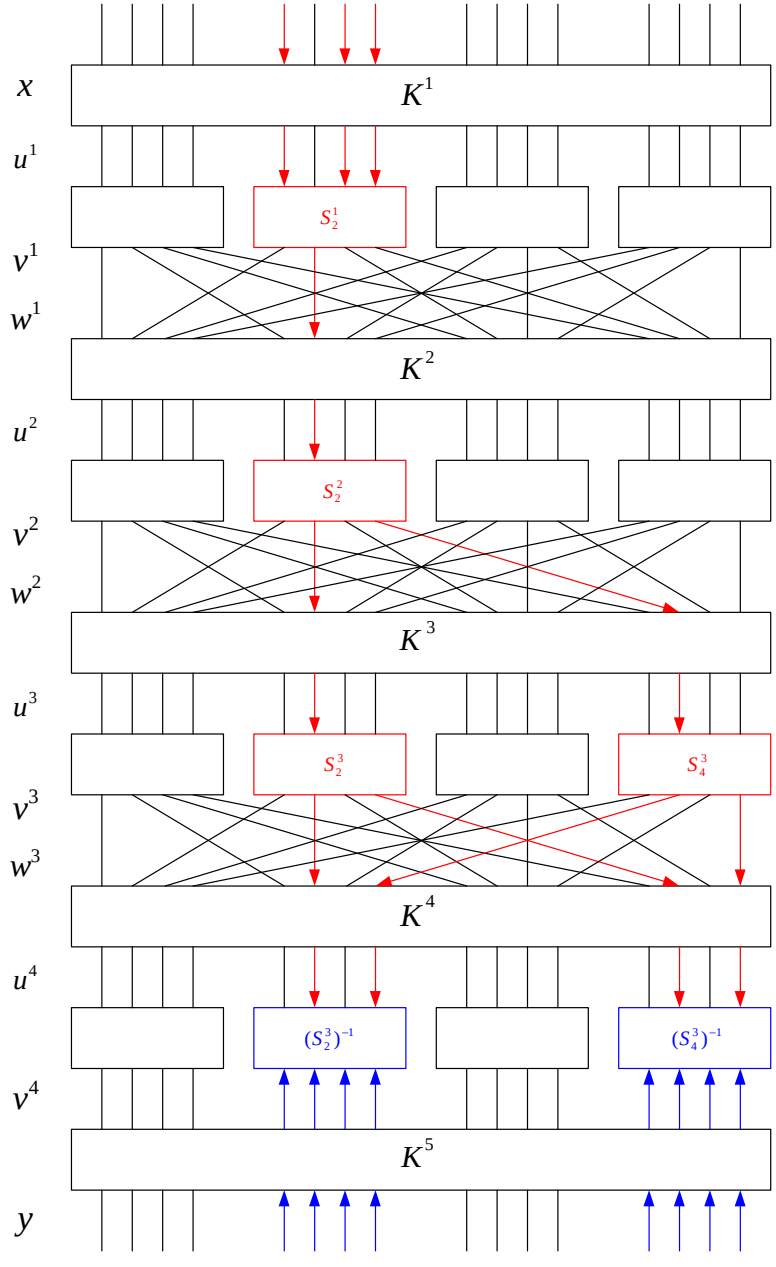
**Step 2.1**($\pi_P$) $v_2^4 \leftarrow L_1 \oplus y_2$,
$v_4^4 \leftarrow L_1 \oplus y_4$.

**Step 2.2**($\pi_S^{-1}$) $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$,
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4**(计数) 如果$z = 0$
则$Count[L_1, L_2] + +$

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$



线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

**Step 2.1($\pi_P$)** $v_2^4 \leftarrow L_1 \oplus y_2$,
$v_4^4 \leftarrow L_1 \oplus y_4$.

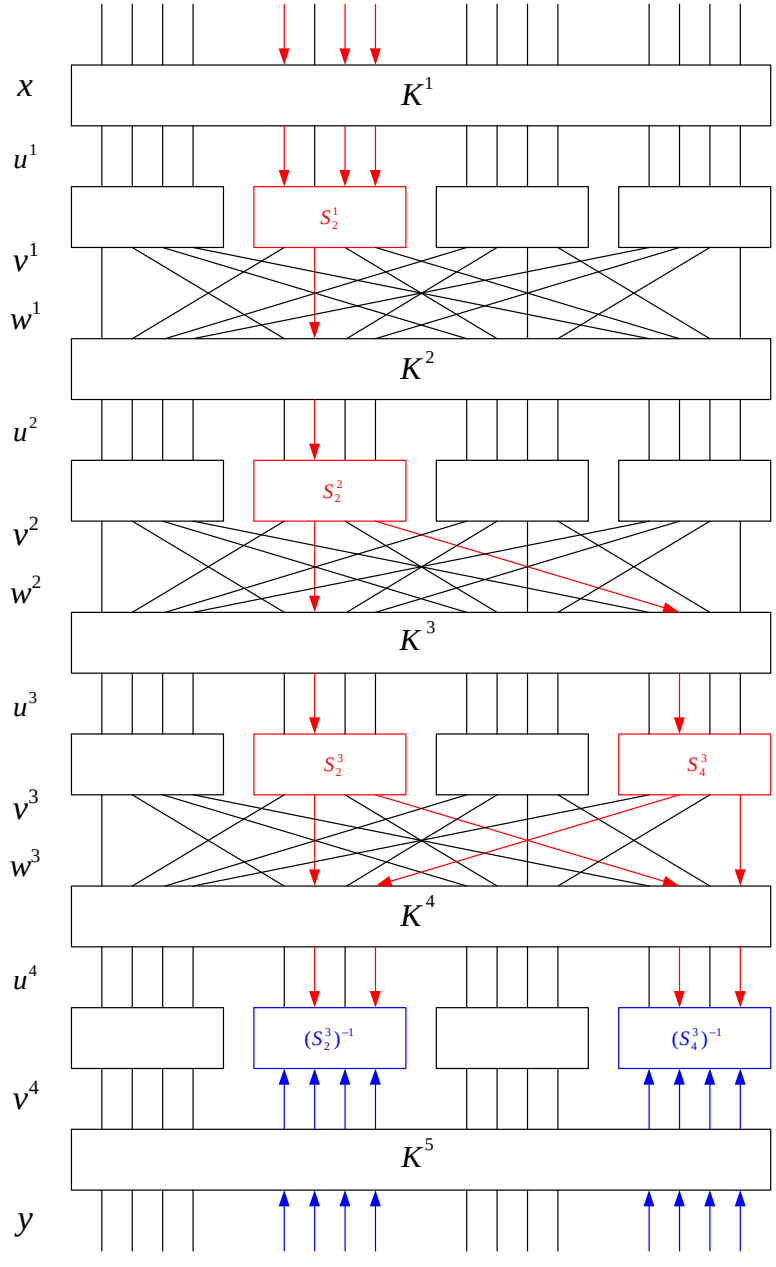
**Step 2.2($\pi_S^{-1}$)** $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$,
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4(计数)** 如果$z = 0$
则$Count[L_1, L_2] + +$

计算$(l_1, l_2)$,满足
$Count[l_1, l_2] =$
$\max |Count[L_1, L_2]/2^4 - 1/2|$

输出：$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$



线性分析算法：

已知：$T \approx 8000$对明-密文

穷搜索$\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5, \mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5$的所有可能值$\{0,1\}^8$，对每个可能值$(L_1, L_2)$如下计算：

Step 1.(清零)计数器$Count[L_1, L_2] = 0$

Step 2.每一对明-密文$(x, y)$，计算：

**Step 2.1($\pi_P$)** $v_2^4 \leftarrow L_1 \oplus y_2$,
$v_4^4 \leftarrow L_1 \oplus y_4$.

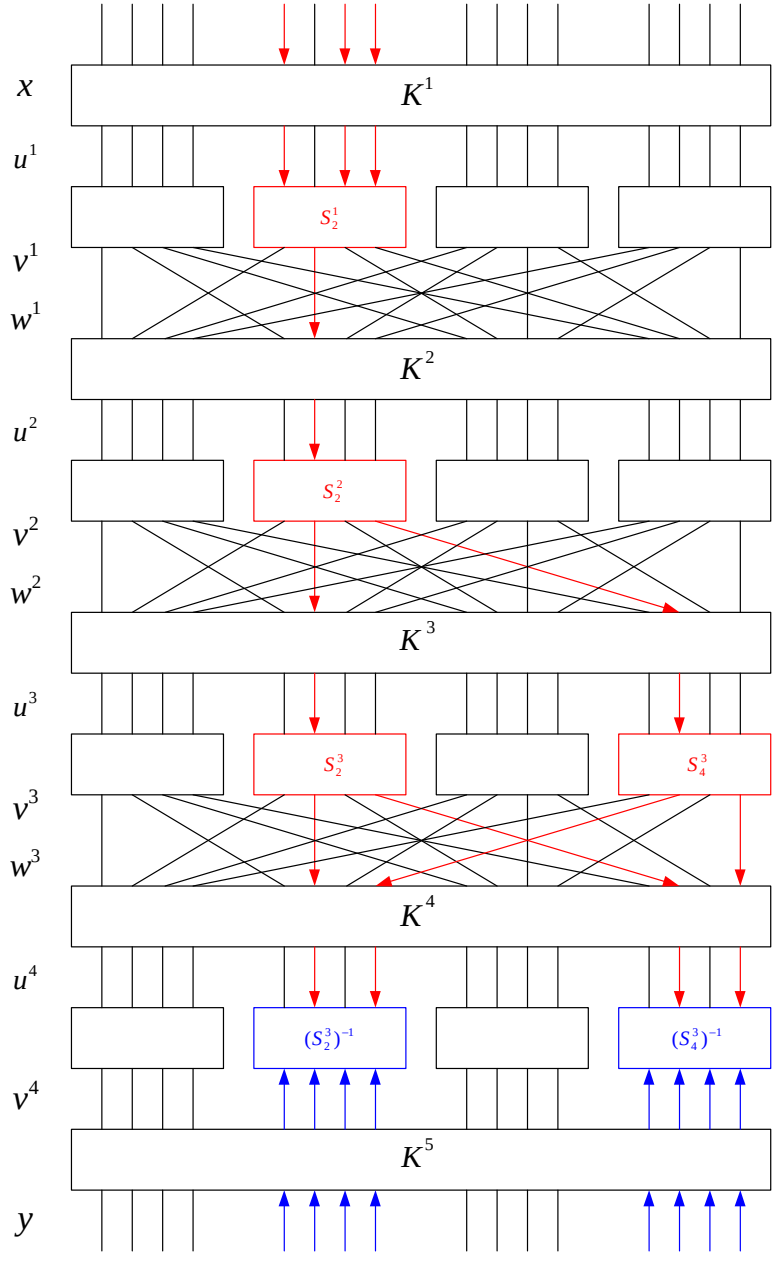
**Step 2.2($\pi_S^{-1}$)** $u_2^4 \leftarrow \pi_S^{-1}(v_{(2)^4})$,
$u_4^4 \leftarrow \pi_S^{-1}(v_{(4)^4})$.

**Step 2.3** $z \leftarrow x_5 \oplus x_7 \oplus x_8 \oplus u_6^4 \oplus u_8^4 \oplus u_{14}^4 \oplus u_{16}^4$

**Step 2.4(计数)** 如果$z = 0$
则$Count[L_1, L_2] + +$

计算$(l_1, l_2)$,满足
$Count[l_1, l_2] =$
$\max |Count[L_1, L_2]/2^4 - 1/2|$

**输出：** $\mathbf{K}_5^5, \mathbf{K}_6^5, \mathbf{K}_7^5, \mathbf{K}_8^5 = l_1$
$\mathbf{K}_{13}^5, \mathbf{K}_{14}^5, \mathbf{K}_{15}^5, \mathbf{K}_{16}^5 = l_2$



# 对例3.1的线性密码分析
## 所需明-密文数据量

如果线性分析基于的线性逼近的偏差为$\varepsilon$，则线性分析要获得成功需要的明密文对数量为：

$$c\varepsilon^{-2}$$

其中$c$为某个“小”的常数。
在例3.1中，$c \approx 8$，$\varepsilon^{-2} = 1024$，因此大约需要8000对明密文。

# 3.3节作业

练习3.9，3.12*，3.14(a)(b)(c)

# 差分密码分析

差分密码分析是选择明文分析

# 差分密码分析

差分密码分析是选择明文分析

**定义：**对两个比特串$x, x^*$，用$(')$表示它们异或，即$x' = x \oplus x^*$。

# 差分密码分析

差分密码分析是选择明文分析

**定义：**对两个比特串$x, x^*$，用$(')$表示它们异或，即$x' = x \oplus x^*$。

差分密码分析原理：

$$x' \xrightarrow{p} w'_{r-1}, \quad p > \frac{1}{2^n}, n\text{为明文分组长}$$

# 差分密码分析

差分密码分析是选择明文分析

**定义：**对两个比特串$x, x^*$，用$(')$表示它们异或，即$x' = x \oplus x^*$。

差分密码分析原理：

$$(x, x^* = x \oplus x') \Rightarrow x' \overset{p}{---\longrightarrow} w'_{r-1}, \quad p > \frac{1}{2^n}, n\text{为明文分组长}$$

$$\Uparrow$$

$$(w_{r-1}, w^*_{r-1})$$

$$\Uparrow$$

猜测$K_r$中相关的比特,经过最后轮函数的逆$g_r^{-1}$

$$\Uparrow$$

$$(y, y^*)$$

# 差分密码分析

差分密码分析是选择明文分析

**定义：**对两个比特串$x, x^*$，用$(')$表示它们异或，即$x' = x \oplus x^*$。

差分密码分析原理：

$$x' \xrightarrow{q_1} w'_1, w'_1 \xrightarrow{q_2} w'_2, \ldots, w'_{r-2} \xrightarrow{q_{r-1}} w'_{r-1}$$

$$\Downarrow$$

$$(x, x^* = x \oplus x') \Rightarrow x' \xrightarrow{p=q_1 q_2 \ldots q_{r-1}} w'_{r-1}, \quad p > \frac{1}{2^n}, n\text{为明文分组长}$$

$$\Uparrow$$

$$(w_{r-1}, w^*_{r-1})$$

$$\Uparrow$$

猜测$K_r$中相关的比特,经过最后轮函数的逆$g_r^{-1}$

$$\Uparrow$$

$$(y, y^*)$$

# S盒的输出异或分布

**定义3.1：** 设$\pi_S : \{0,1\}^m \to \{0,1\}^n$为一个$S$盒。考虑长为$m$的有序比特串对$(x, x^*)$，我们称$S$盒的输入异或为$x \oplus x^*$，输出异或为$\pi_S(x) \oplus \pi_S(x^*)$。
对任何$x' \in \{0,1\}^m$，定义集合$\Delta(x')$为包含所有具有输入异或值$x'$的有序对$(x, x^*)$，显然

$$\Delta(x') = \{(x, x \oplus x') : x \in \{0,1\}^m\}$$

$S$盒在输入异或为$x'$的情况下，我们可以计算输出异或的分布情况，如果输出异或分布不均匀，就有可能导致差分攻击。

# 例3.3:计算$S$盒的输出异或分布

考虑例3.1中的$S$盒。设输入异或$x' = 1011$，则

$\Delta(1011) = \{(0000, 1011), (0001, 1010), \ldots, (1111, 0100)\}$

| $y'$ | | | | |
|---|---|---|---|---|
| 个数 | 0000<br>0 | 0001<br>0 | 0010<br>8 | 0011<br>0 |
| $y'$ | | | | |
| 个数 | 0100<br>0 | 0101<br>2 | 0110<br>0 | 0111<br>2 |
| $y'$ | | | | |
| 个数 | 1000<br>0 | 1001<br>0 | 1010<br>0 | 1011<br>0 |
| $y'$ | | | | |
| 个数 | 1100<br>0 | 1101<br>2 | 1110<br>0 | 1111<br>2 |

| $x$ | $x^*$ | $y = \pi_S(x)$ | $y^* = \pi_S(x^*)$ | $y'$ |
|---|---|---|---|---|
| 0000 | 1011 | 1110 | 1100 | 0010 |
| 0001 | 1010 | 0100 | 0110 | 0010 |
| 0010 | 1001 | 1101 | 1010 | 0111 |
| 0011 | 1000 | 0001 | 0011 | 0010 |
| 0100 | 1111 | 0010 | 0111 | 0101 |
| 0101 | 1110 | 1111 | 0000 | 1111 |
| 0110 | 1101 | 1011 | 1001 | 0010 |
| 0111 | 1100 | 1000 | 0101 | 1101 |
| 1000 | 0011 | 0011 | 0001 | 0010 |
| 1001 | 0010 | 1010 | 1101 | 0111 |
| 1010 | 0001 | 0110 | 0100 | 0010 |
| 1011 | 0000 | 1100 | 1110 | 0010 |
| 1100 | 0111 | 0101 | 1000 | 1101 |
| 1101 | 0110 | 1001 | 1011 | 0010 |
| 1110 | 0101 | 0000 | 1111 | 1111 |
| 1111 | 0100 | 0111 | 0010 | 0101 |

# 例3.3:计算$S$盒的输出异或分布

考虑例3.1中的$S$盒。设输入异或$x' = 1011$，则

$$\Delta(1011) = \{(0000, 1011), (0001, 1010), \ldots, (1111, 0100)\}$$

| $y'$ | | | | |
|---|---|---|---|---|
| 个数 | 0000<br>0 | 0001<br>0 | 0010<br>8 | 0011<br>0 |
| $y'$ | | | | |
| 个数 | 0100<br>0 | 0101<br>2 | 0110<br>0 | 0111<br>2 |
| $y'$ | | | | |
| 个数 | 1000<br>0 | 1001<br>0 | 1010<br>0 | 1011<br>0 |
| $y'$ | | | | |
| 个数 | 1100<br>0 | 1101<br>2 | 1110<br>0 | 1111<br>2 |

| $x$ | $x^*$ | $y = \pi_S(x)$ | $y^* = \pi_S(x^*)$ | $y'$ |
|---|---|---|---|---|
| 0000 | 1011 | 1110 | 1100 | 0010 |
| 0001 | 1010 | 0100 | 0110 | 0010 |
| 0010 | 1001 | 1101 | 1010 | 0111 |
| 0011 | 1000 | 0001 | 0011 | 0010 |
| 0100 | 1111 | 0010 | 0111 | 0101 |
| 0101 | 1110 | 1111 | 0000 | 1111 |
| 0110 | 1101 | 1011 | 1001 | 0010 |
| 0111 | 1100 | 1000 | 0101 | 1101 |
| 1000 | 0011 | 0011 | 0001 | 0010 |
| 1001 | 0010 | 1010 | 1101 | 0111 |
| 1010 | 0001 | 0110 | 0100 | 0010 |
| 1011 | 0000 | 1100 | 1110 | 0010 |
| 1100 | 0111 | 0101 | 1000 | 1101 |
| 1101 | 0110 | 1001 | 1011 | 0010 |
| 1110 | 0101 | 0000 | 1111 | 1111 |
| 1111 | 0100 | 0111 | 0010 | 0101 |

# 差分分布表

更加一般的，对$S$盒$\pi_S : \{0,1\}^m \to \{0,1\}^n$，设$a'$表示输入异或，$b'$表示输出异或。则$(a', b')$称为一个差分。

$S$盒的输入输出差分分布定义为：

$$N_D(x', y') = |\{(x, x^*) \in \Delta(x') : \pi_S(x) \oplus \pi_S(x^*) = y'\}|$$

图 3.4给出了例3.1的$S$盒的所有输入输出差分分布。

对应于差分$(a', b')$的扩散率$R_p(a', b')$定义为：

$$R_p(a', b') = \frac{N_D(a', b')}{2^m} = Pr(\text{输出异或} = b' | \text{输入异或} = a')$$

# 差分分布表

更加一般的，对$S$盒$\pi_S : \{0,1\}^m \to \{0,1\}^n$，设$a'$表示输入异或，$b'$表示输出异或。则$(a', b')$称为一个差分。

$S$盒的输入输出差分分布定义为：

$$N_D(x', y') = |\{(x, x^*) \in \Delta(x') : \pi_S(x) \oplus \pi_S(x^*) = y'\}|$$

图 3.4给出了例3.1的$S$盒的所有输入输出差分分布。

对应于差分$(a', b')$的扩散率$R_p(a', b')$定义为：

$$R_p(a', b') = \frac{N_D(a', b')}{2^m} = Pr(\text{输出异或} = b' | \text{输入异或} = a')$$

# 差分分布表

更加一般的，对$S$盒$\pi_S : \{0,1\}^m \to \{0,1\}^n$，设$a'$表示输入异或，$b'$表示输出异或。则$(a', b')$称为一个差分。
$S$盒的输入输出差分分布定义为：

$$N_D(x', y') = |\{(x, x^*) \in \Delta(x') : \pi_S(x) \oplus \pi_S(x^*) = y'\}|$$

图 3.4给出了例3.1的$S$盒的所有输入输出差分分布。
对应于差分$(a', b')$的扩散率$R_p(a', b')$定义为：

$$R_p(a', b') = \frac{N_D(a', b')}{2^m} = Pr(\text{输出异或} = b' | \text{输入异或} = a')$$

# 多轮差分链构造

差分链：$x' \xrightarrow{\text{扩散率}q_1} w'_1, w'_1 \xrightarrow{q_2} w'_2, \ldots, w'_{r-2} \xrightarrow{q_{r-1}} w'_{r-1}$

# 多轮差分链构造

差分链：$x' \xrightarrow{\text{扩散率}q_1} w'_1, w'_1 \xrightarrow{q_2} w'_2, \ldots, w'_{r-2} \xrightarrow{q_{r-1}} w'_{r-1}$

$\Downarrow$ (若每一轮的扩散率独立)

$x' \xrightarrow{p=q_1 q_2 \ldots q_{r-1}} w'_{r-1}, \quad p > \frac{1}{2^n}$, $n$为明文分组长

# 多轮差分链构造

差分链：$x' \xrightarrow{\text{扩散率}q_1} w'_1, w'_1 \xrightarrow{q_2} w'_2, \ldots, w'_{r-2} \xrightarrow{q_{r-1}} w'_{r-1}$

$\Downarrow$ (若每一轮的扩散率独立)

$(x, x^* = x \oplus x') \Rightarrow x' \xrightarrow{p=q_1 q_2 \ldots q_{r-1}} w'_{r-1}, \quad p > \frac{1}{2^n}, n$为明文分组长

$\Uparrow$

$(w_{r-1}, w^*_{r-1})$

$\Uparrow$

猜测$K_r$中相关的比特,经过最后轮函数的逆$g_r^{-1}$

$\Uparrow$

$(y, y^*)$

# 对例3.1的差分分析

- $S_2^1$:$R_p(1011, 0010) = 1/2$
- $S_3^2$:$R_p(0100, 0110) = 3/8$
- $S_2^3$:$R_p(0010, 0101) = 3/8$
- $S_3^3$:$R_p(0010, 0101) = 3/8$

注意到：

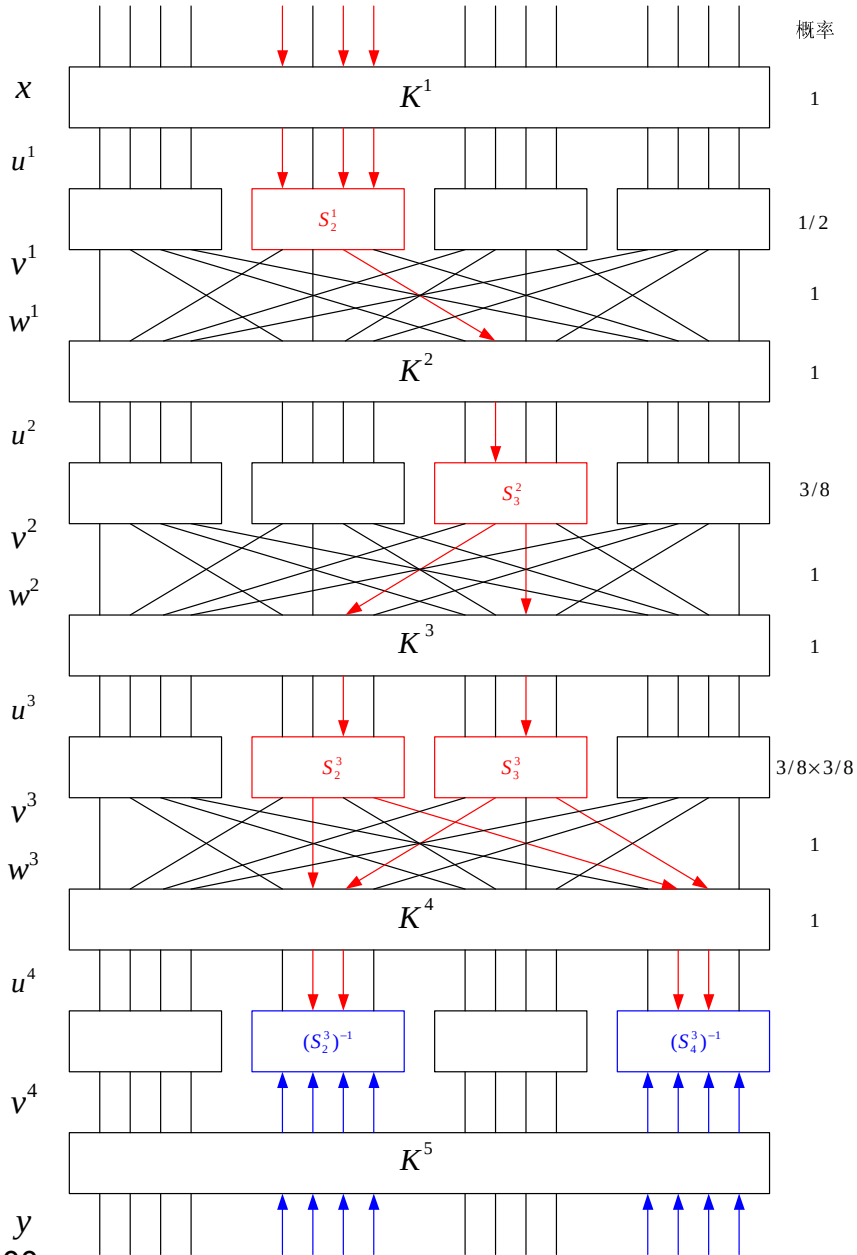
$$
\begin{aligned}
& w^{r-1} \oplus (w^{r-1})^* \\
&= (w^{r-1} \oplus K^r) \oplus ((w^{r-1})^* \oplus K^r) \\
&= u^r \oplus (u^r)^*
\end{aligned}
$$

由以上$S$盒的差分能够组合成一个差分链，最终获得前三轮的差分链的靠扩散率：

$$
\begin{aligned}
& R_p(0000\ 1011\ 0000\ 0000, 0000\ 0101\ 0101\ 0000) \\
&= \frac{1}{2} \times (\frac{3}{8})^3 = \frac{27}{1024}
\end{aligned}
$$

即

$$x' = 0000\ 1011\ 0000\ 0000 \xrightarrow{p=\frac{27}{1024}} (v^3)' = 0000\ 0101\ 0101\ 0000$$



# 对例3.1的差分分析

$$x' = 0000\ 1011\ 0000\ 0000$$

$$\xrightarrow{p=\frac{27}{1024}} (v^3)' = 0000\ 0101\ 0101\ 0000$$

$$\xrightarrow{p=1} (u^4)' = 0000\ 0110\ 0000\ 0110$$

那么

$$x' = 0000\ 1011\ 0000\ 0000$$

$$\xrightarrow{p=\frac{27}{1024}} (u^4)' = 0000\ 0110\ 0000\ 0110$$

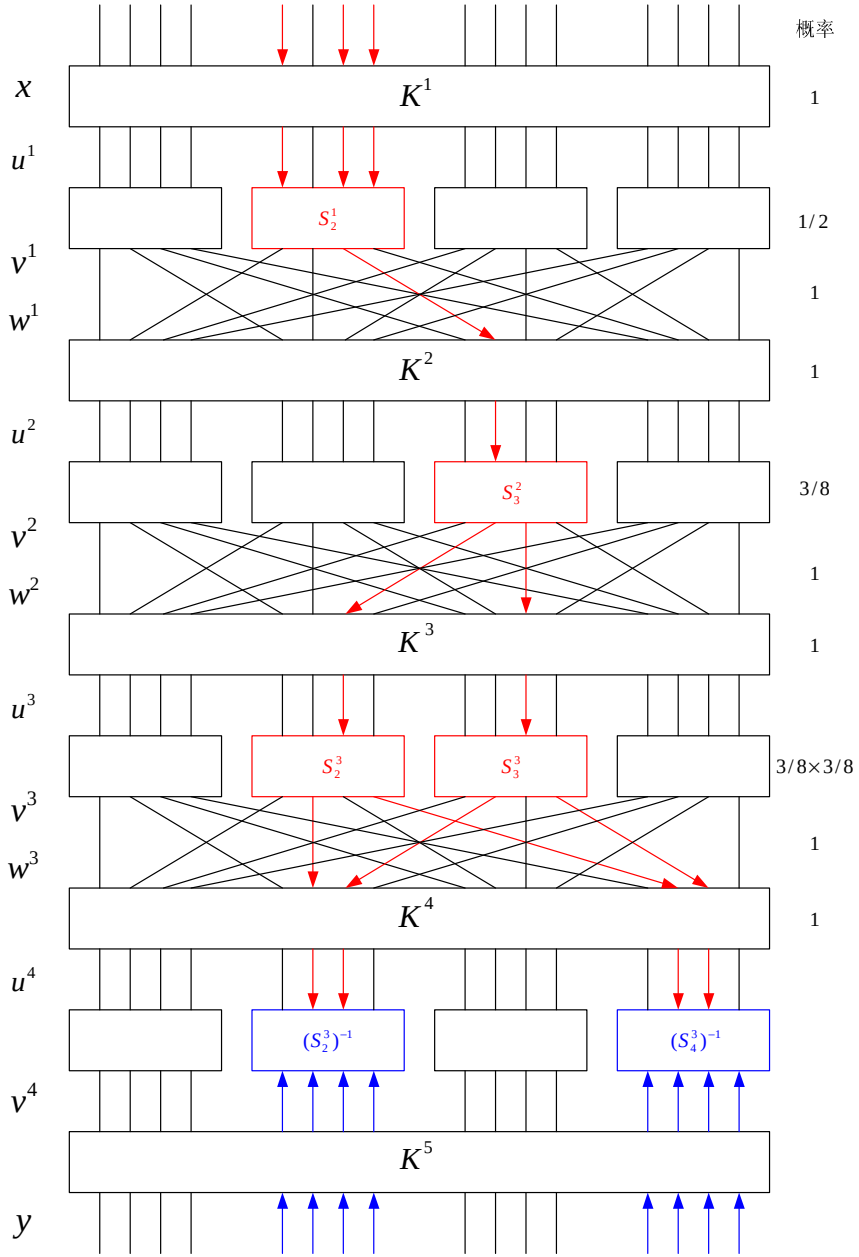
使得差分成立的4重组$(x, x^*, y, y^*)$称为一个正确对。注意到，一个正确对满足：

$$(u^4_{(1)})' = (u^4_{(3)})' = 0000$$

因此

$$y_{(1)} = (y^*_{(1)}),\quad y_{(3)} = (y^*_{(3)})$$

由此可以过滤到一些不正确的密钥比特

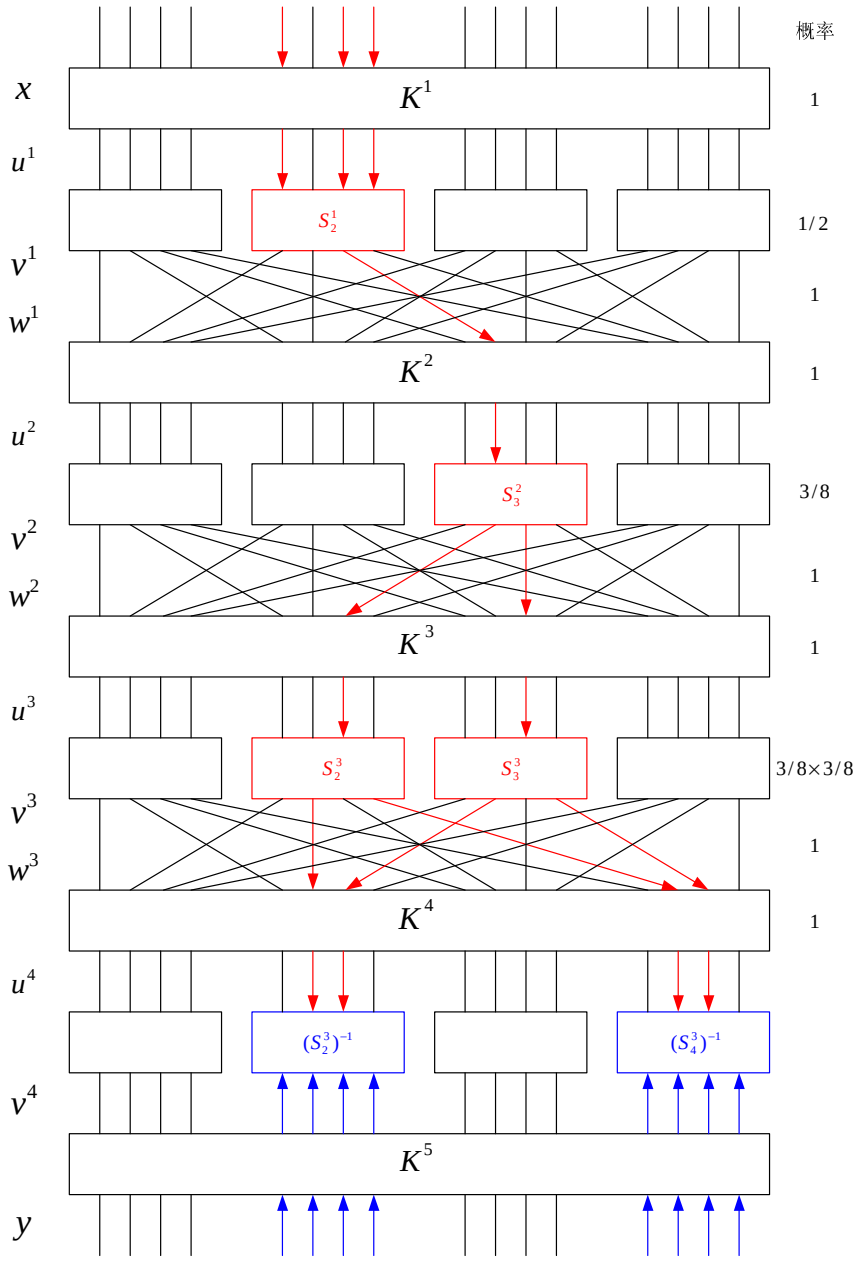


# 对例3.1的差分分析算法

算法3.3：
**输入：** 约50 ∼ 100对选择明-密文对：$(x, y), (x^*, y^*)$，而且$x \oplus x^* = 0000\ 1011\ 0000\ 0000$
**算法：** 对所有$K^5_{(2)}, K^5_{(4)}$的可能值$L_1, L_2 \in \{0,1\}^4$做如下计算：
(1)计数器$Count[L_1, L_2] = 0$
(2)对每一对选择明密文对$(x, y), (x^*, y^*)$做如下计算：
如果$y_{(1)} = (y^*_{(1)}), y_{(3)} = (y^*_{(3)})$那么计算

1. $u^4_{(2)} \leftarrow \pi_S^{-1}(L_1 \oplus y_{(2)})$,
   $u^4_{(4)} \leftarrow \pi_S^{-1}(L_1 \oplus y_{(4)})$
2. $(u^4_{(2)})^* \leftarrow \pi_S^{-1}(L_1 \oplus (y_{(2)})^*)$,
   $(u^4_{(4)})^* \leftarrow \pi_S^{-1}(L_1 \oplus (y_{(4)})^*)$
3. $(u^4_{(2)})' \leftarrow u^4_{(2)} \oplus (u^4_{(2)})^*$,
   $(u^4_{(4)})' \leftarrow u^4_{(2)} \oplus (u^4_{(4)})^*$
4. 如果$(u^4_{(2)})' = 0110, (u^4_{(4)})' = 0110$,
   则$Count[L_1, L_2] + +$

找出使得$Count[L_1, L_2]$最大的$l_1, l_2 \in \{0,1\}^4$
**输出：** $K^5_{(2)} = l_1, K^5_{(4)} = l_2$



# 差分分析成功需要的选择明文对个数

差分分析成功需要的选择明-密文四重组$(x, x^*, y, y^*)$数量$T \simeq c\varepsilon^{-1}$，这里$\varepsilon$是所用的差分链的扩散率，$c$是一个小的常数。

在例3.1中，$\varepsilon^{-1} = 1024/27 \approx 38$, $T$在$50 \sim 100$之间。

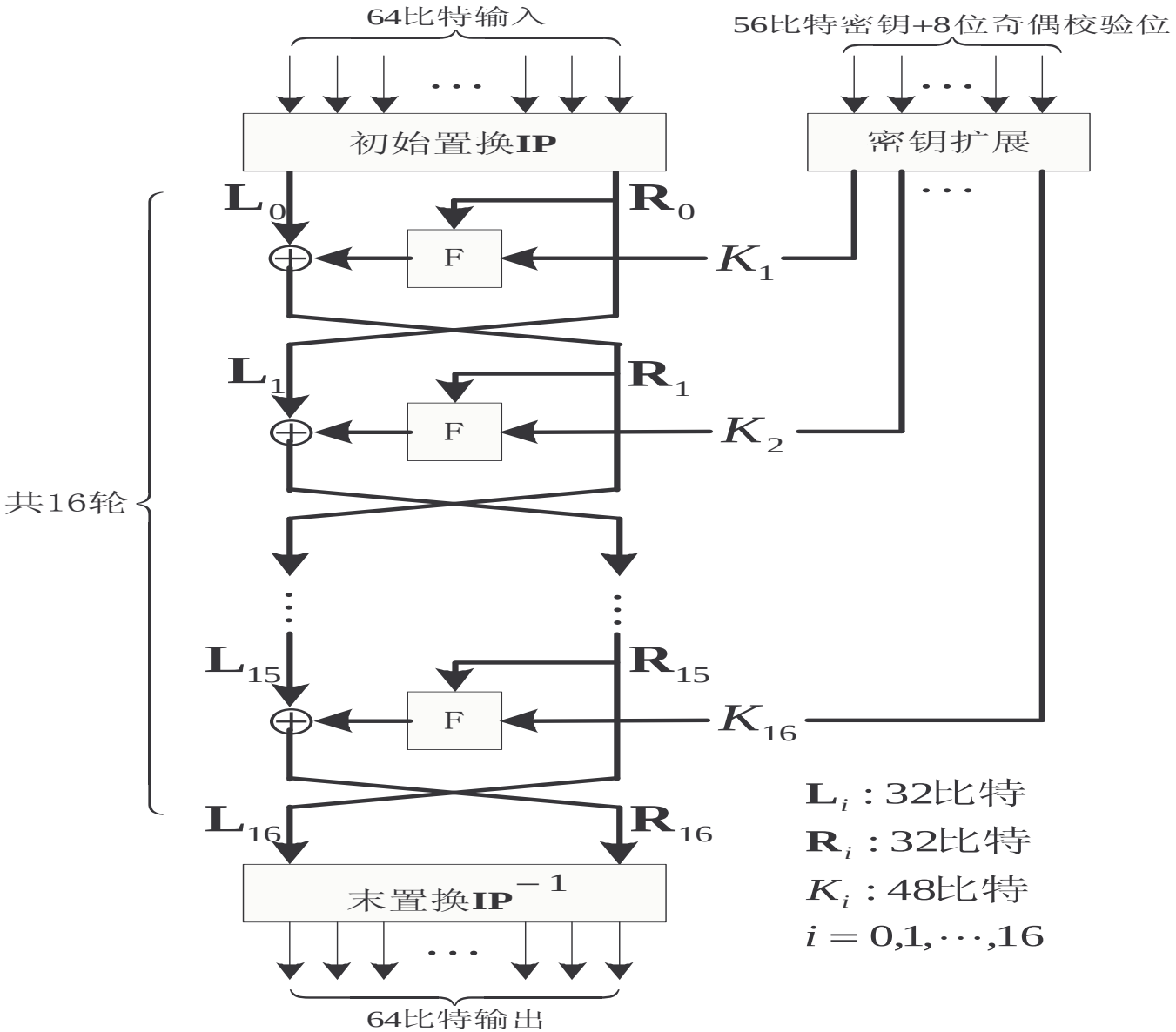
## 3.4节练习

练习3.15(a)（只需要计算一个$N_D$的值就可以），$(b)^*$（选作题）

# 数据加密标准DES
## DES的历史

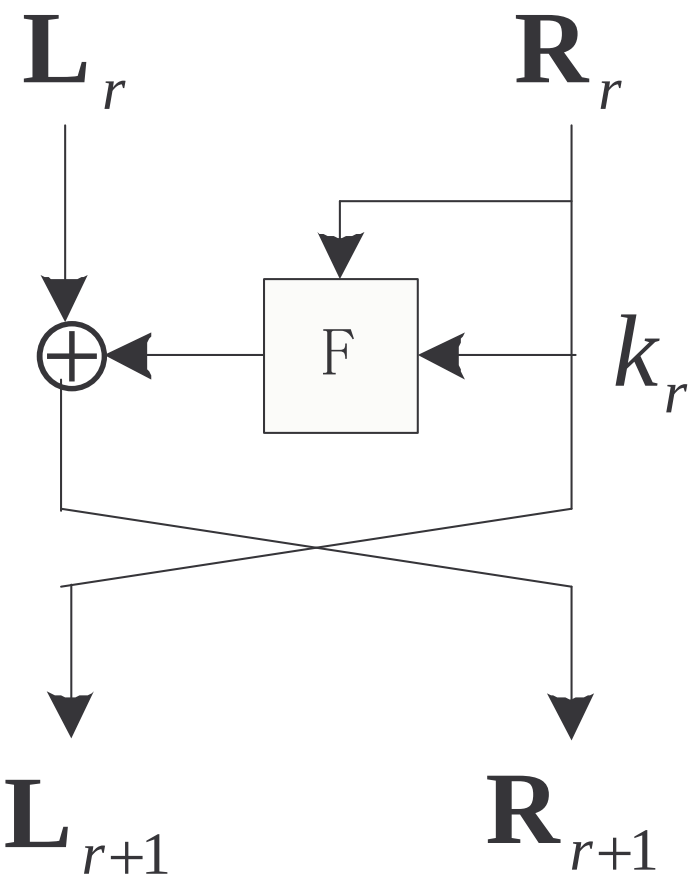
1. 1973年5月15日美国国家技术标准局（NIST）公开征集密码体制。
2. 1977年2月15日由IBM开发的DES被选择为标准，用在“非密级”应用中，DES是对早期版本Lucifer的改进。
3. 每隔5年对DES进行一次评审。
4. 在1999年1日对DES最后一次评审。
5. 2001年11月26日DES最终被AES代替。

DES算法结构图：

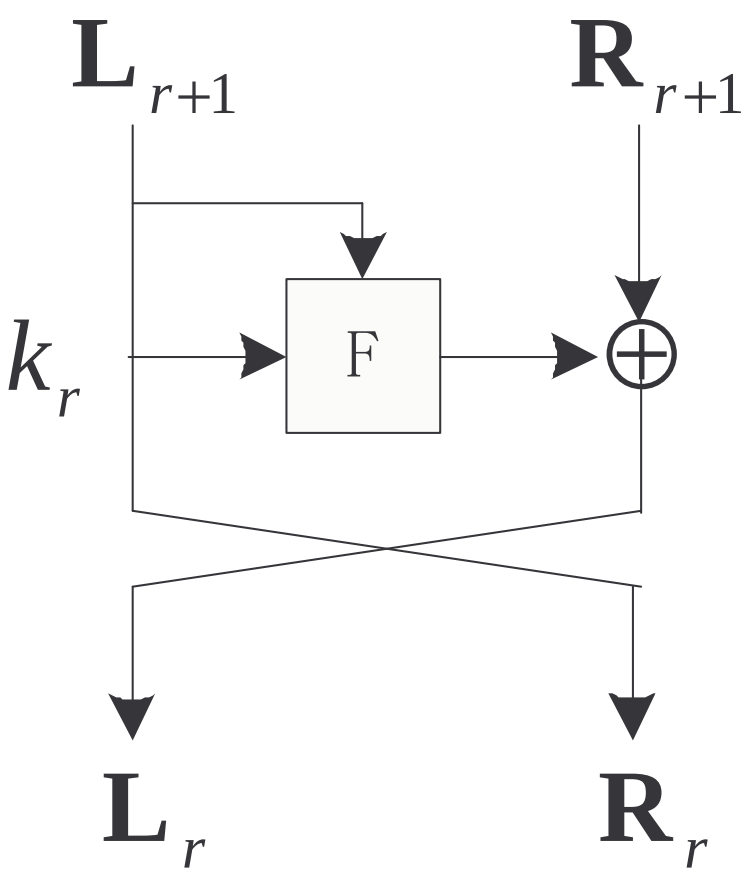

64比特输入
56比特密钥+8位奇偶校验位
初始置换IP
密钥扩展
$L_0$
$R_0$
F
$K_1$
$L_1$
$R_1$
F
$K_2$
共16轮
$L_{15}$
$R_{15}$
F
$K_{16}$
$L_{16}$
$R_{16}$
末置换$IP^{-1}$
64比特输出
$L_i$：32比特
$R_i$：32比特
$K_i$：48比特
$i = 0,1,\cdots,16$

DES的Feistel轮函数结构：

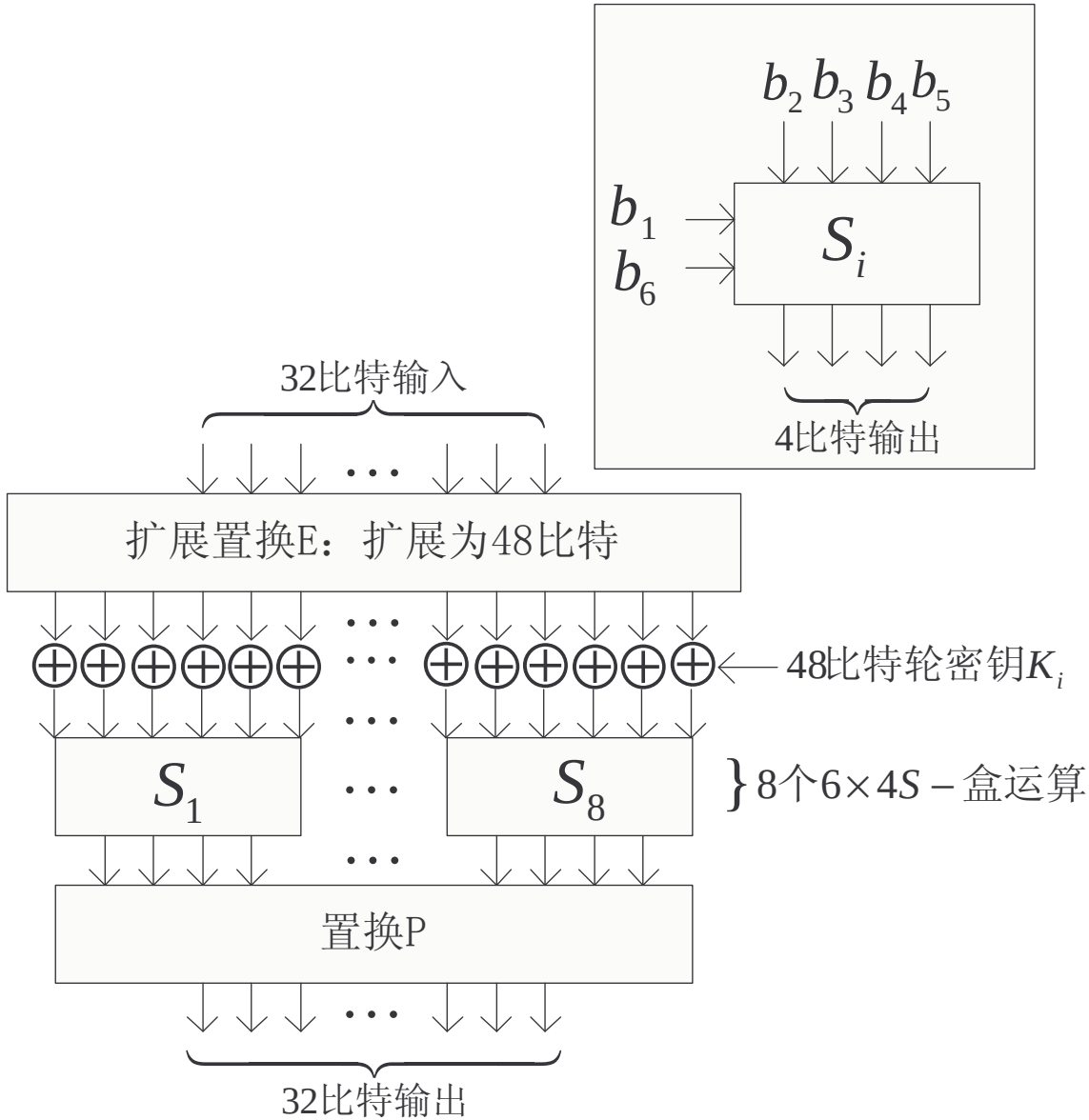
Feistel网络




Feistel网络的
逆过程



*F*函数：


$b_2\ b_3\ b_4\ b_5$
$b_1$
$b_6$
$S_i$
4比特输出
32比特输入
扩展置换E：扩展为48比特
48比特轮密钥$K_i$
$S_1$
$S_8$
}8个6×4S－盒运算
置换P
32比特输出

# 8个S盒：

| $S_1$ | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |
| $S_2$ | | | | | | | | | | | | | | | |
| 5 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |
| $S_3$ | | | | | | | | | | | | | | | |
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| $S_4$ | | | | | | | | | | | | | | | |
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |
| $S_5$ | | | | | | | | | | | | | | | |
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |
| $S_6$ | | | | | | | | | | | | | | | |
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |
| $S_7$ | | | | | | | | | | | | | | | |
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |
| $S_8$ | | | | | | | | | | | | | | | |
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

$S$盒计算例子：

$S_1$的输入：　$b_1b_2b_3b_4b_5b_6 = (11001)_2$

所在行：　$b_1b_6 = (11)_2 = 3$

所在列：　$b_2b_3b_4b_5 = (1100)_2 = 12$

输出：　10

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

# 数据加密标准DES
## DES算法描述

初始置换IP、末置换$IP^{-1}$、扩展置换$E$、置换$P$、密钥编排算法中的置换PC-1和压缩置换PC-2的运算和古典密码的置换密码一样。

初始置换$IP$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

末置换$IP^{-1}$

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

**Table:** 初始置换$IP$和末置换$IP^{-1}$

| E | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

| P | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

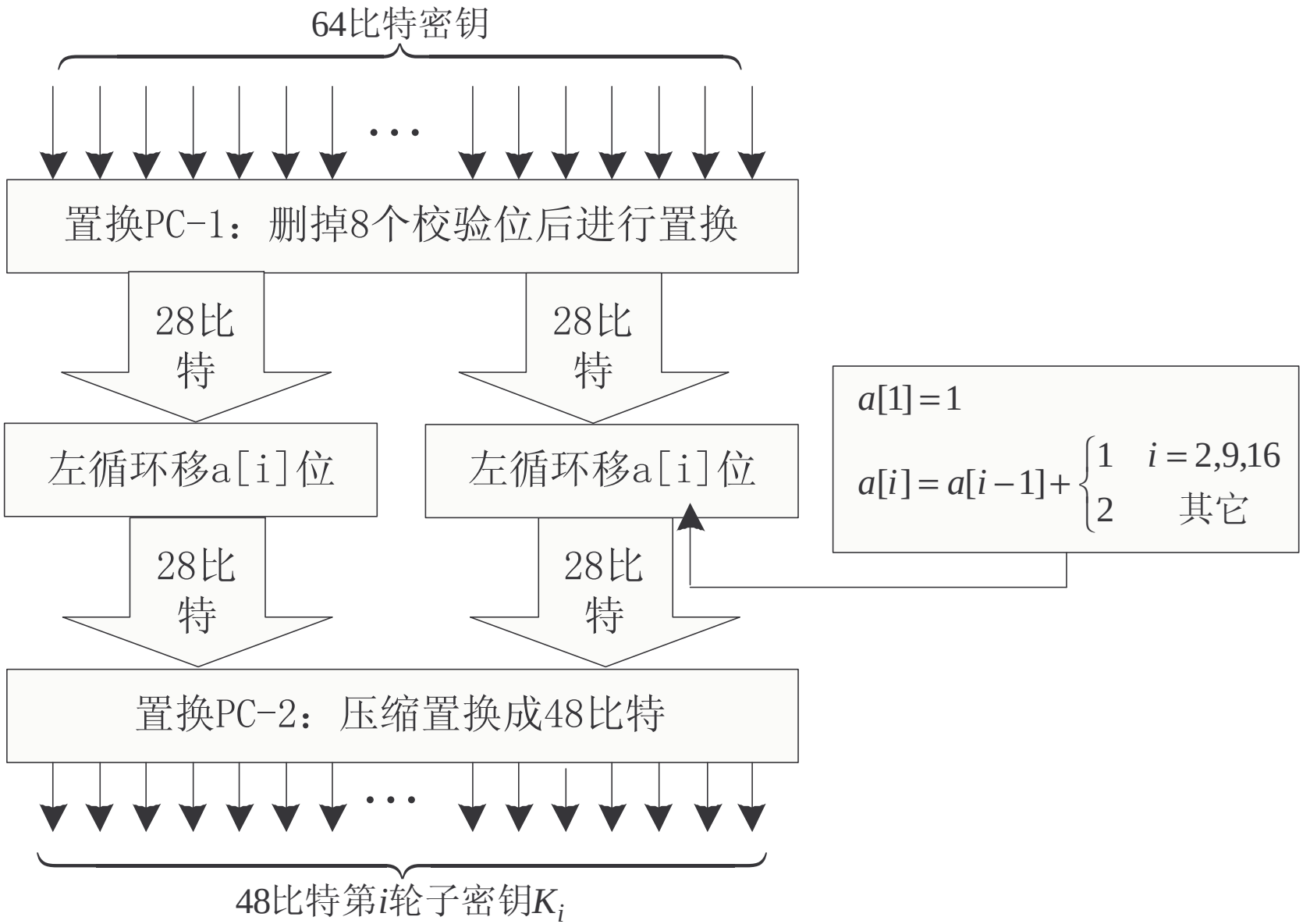
**Table:** F函数中的扩展置换$E$和置换$P$

给定32比特串输入$A = (a_1, a_2, \ldots, a_{32})$,

$$E(A) = (a_{32}, a_1, a_2, a_3, a_4, a_5, a_4, \ldots, a_{31}, a_{32}, a_1)$$

$$P(A) = (a_{16}, a_7, a_{20}, a_{21}, a_{29}, \ldots, a_{11}, a_4, a_{25})$$

密钥编排算法：


64比特密钥
置换PC-1：删掉8个校验位后进行置换
28比特
28比特
左循环移a[i]位
左循环移a[i]位
28比特
28比特
置换PC-2：压缩置换成48比特
48比特第i轮子密钥$K_i$
$a[1]=1$
$a[i]=a[i-1]+\begin{cases}1 & i=2,9,16\\ 2 & \text{其它}\end{cases}$

| PC-1 | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

| PC-2 | | | | | |
|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |

**Table:** 密钥扩展中的置换PC-1和压缩置换PC-2

# 数据加密标准DES
## DES的分析

对DES的*S*盒的“陷门”争议：

- S-盒是整个DES算法的关键部件，DES靠它实现非线性变换。关于S-盒的设计准则还没有完全公开。
- 许多密码学家怀疑NSA设计S-盒时隐藏了“陷门”，这样只有他们才可以破译算法，但没有证据能标明这点。
- 在1976年，NSA披露了S-盒的几条设计准则。直到1990年，Eli Biham和Adi Shamir提出对DES的差分密码分析后，IBM公布了S-盒和P置换的设计准则。

# 数据加密标准DES
## DES的分析

经过20多年的分析，DES基本上发现没有重大安全缺陷，下表给出了对DES的攻击结果，其中百分比表示成功概率。

| 分析方法 | 数据复杂度 | | 存储复杂度 | 处理复杂度 |
|---|---|---|---|---|
| | 已知明文 | 选择明文 | | |
| 预处理的穷搜索 | – | 1 | $2^{56}$ | 1(查表) |
| 穷搜索 | 1 | – | 可忽略 | $2^{55}$ |
| 线性攻击 | $2^{43}$(85%) | – | 明-密文对量 | $2^{43}$ |
| | $2^{38}$(10%) | – | 明-密文对量 | $2^{50}$ |
| 差分攻击 | – | $2^{47}$ | 明-密文对量 | $2^{47}$ |
| | $2^{55}$ | – | 明-密文对量 | $2^{55}$ |

**Table:** DES的密码分析结果

# 数据加密标准DES
## DES的分析

- 对DES最有效的攻击还是强力攻击，因为无论对差分密码分析，还是线性密码分析，所需要的海量选择明文-密文对是不现实的，而且单是存贮明文-密文对就至少需要140,000GB。
- 事实上，对DES的穷搜索攻击是威胁DES安全的重要因素。例如：
  1. 美国克罗多州的程序员Verser从1997年3月13日起，用了96天的时间，在Internet上数万名志愿者的协同工作下，于6月17日成功地找到了美国RSA公司悬赏一万美金破译的密钥长度为56比特的DES的密钥。
  2. 1998年电子边境基金会(EFF)使用一台25万美元的电脑在56小时内再次破解了56比特的DES。
  3. 1999年1月RSA数据安全会议期间，EFF用22小时15分钟就宣告成功破解DES。但如果DES的密钥长度为128比特，那么它可以在1018年内攻破。(http://www.rsa.com/rsalabs/node.asp?id=2108)

## 3.5节练习

练习3.2，3.3

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# 高级数据加密标准AES

## AES的遴选：

1. 1997年1月，美国国家标准技术研究所(NIST)开始对高级数据加密标准（AES）进行研究，并成立了AES标准工作室。
2. 1997年9月12日，NIST发布征集算法的正式公告。
3. 至1998年6月15日提交了21个侯选算法。
4. 于1998年8月20日召开了第一次AES候选人会议（AES1），宣布了来自全世界的15个候选算法。
5. 1999年3月开始的第二次候选人会议，选出了五个决赛算法：MARS, RC6, Rijndael, Serpent和Twofish。
6. 2000年4月召开了第三次AES会议(AES3)。
7. 于2000年10月2日美国商业部长Norman Y.Mineta宣布Rijndeal最终获胜。
8. 2001年11月26日，NIST发布了联邦信息处理标准，即FIPS-197，正式公告了高级数据加密标准(AES)，2002年5月26日公告正式生效。
9. 每隔5年重新进行一次正式评估。

# AES的遴选标准

1. AES是公开；
2. AES是分组加密单钥体制，支持128比特长分组和128-，192-和256比特长密钥；
3. AES的密钥长度可变，可以根据需要增加；
4. AES可以用软件和硬件实现；
5. AES可以自由使用，或依据符合美国国家标准技术研究所（NIST）策略的条件使用；

# AES的遴选标准

满足以上要求的AES，需要依据以下特性判断优劣：

1. 安全性；至少考虑到以下因素：
   - 与其他侯选算法的实际安全性的比较；
   - 算法对输入分组的输出与随机置换对输入分组的输出的差异程度；
   - 算法安全性所依赖的数学基础是否坚固；
   - 在评估过程中由公众提出的其他安全因素，包括那些证明算法的安全强度比提交者所声明的要弱的任何攻击。
2. 计算效率（从运行速度及存储空间方面考虑）；
3. 灵活性；
4. 使用简单性；
5. 其它在活动中提出的意见。

# AES－Rijndeal简介

- Rijndeal为比利时密码学家Joan Daemen和Vincent Rijmen所设计(Rijndeal就由两位作者名字的组合而成：Rijmen+Daemen)
- Rijndeal的前身是Square，于1997年在快速软件加密会议(FSE'97)上公布，1998年6月，在对Square作修改、重新命名为Rijndeal后作为AES候选算法。
- Rijndeal胜出的原因：
  - 其软件和硬件实现对计算环境的适应性强，性能稳定、优良。
  - 密钥建立时间短，密钥灵活性好。
  - 而对存储量要求低使它适合资源紧缺的环境，且保持优秀的性能。
  - Rijndeal的运算是所有提交算法中最易于抵抗能量和计时攻击。
  - Rijndeal可灵活组合不同的分组长和密钥长，对算法所作的改动仅是增加它的轮数。

# AES的描述

| | | | |
|---|---|---|---|
| 分组长 | 128 | 128 | 128 |
| 密钥长 | 128 | 192 | 256 |
| 轮数$Nr$ | 10 | 12 | 14 |

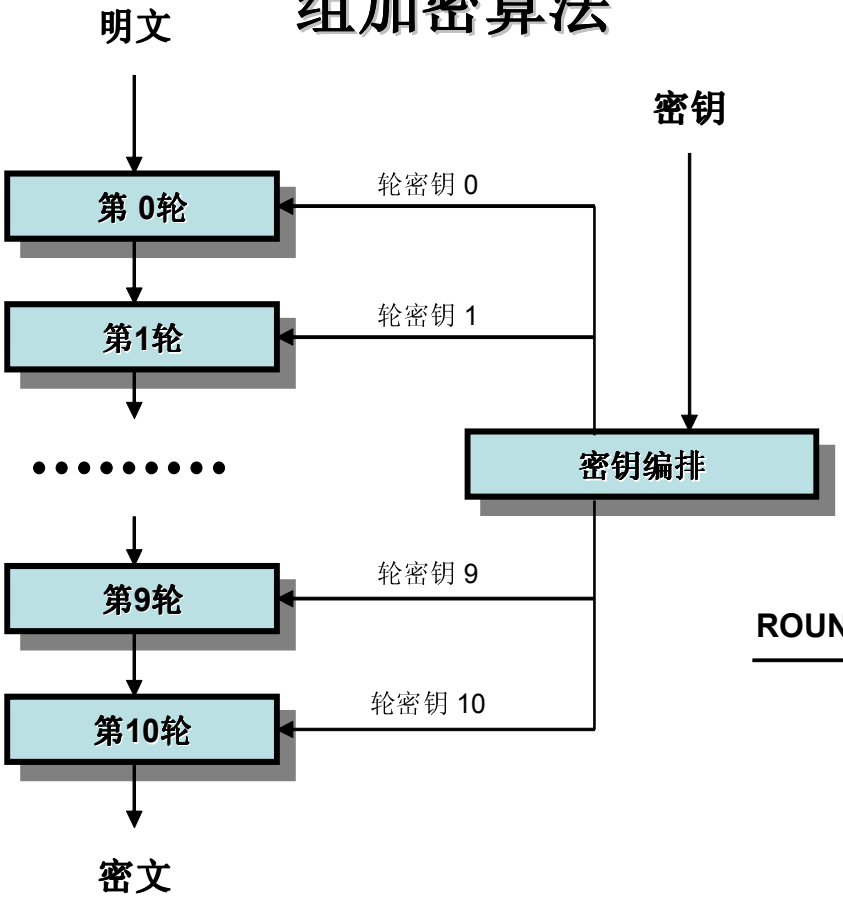
AES的算法结构：观看128比特密钥的AES的Flash演示。

AES的四个运算：

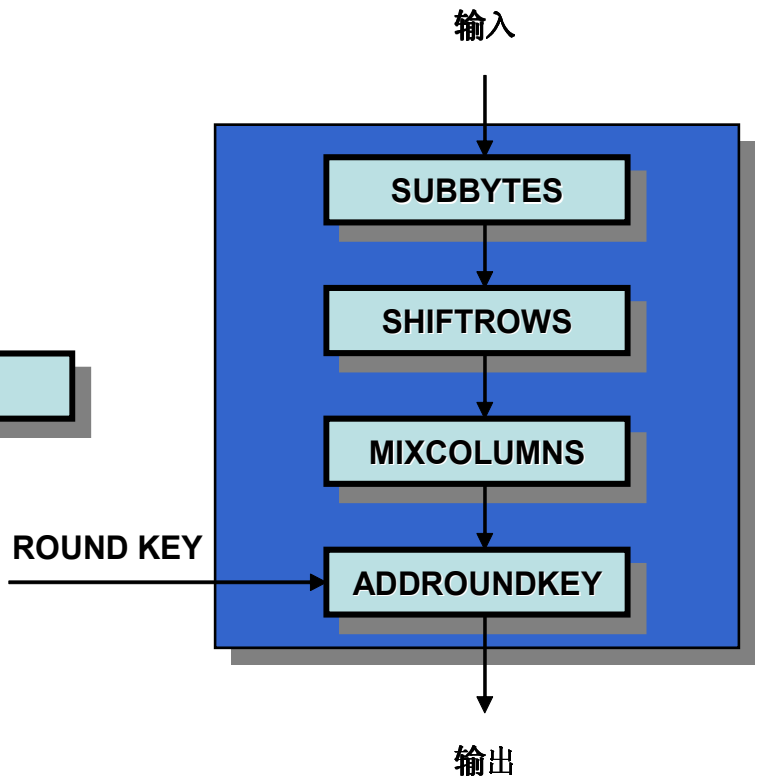
- S盒运算：SubByte
- 行移位：ShiftRow
- 列混合：MixColumn
- 轮密钥异或：AddRoundKey

# AES加密过程

## 128比特分组加密算法




## 0-9轮的轮结构（第10轮少了MixColumns）



# S盒运算：SubByte

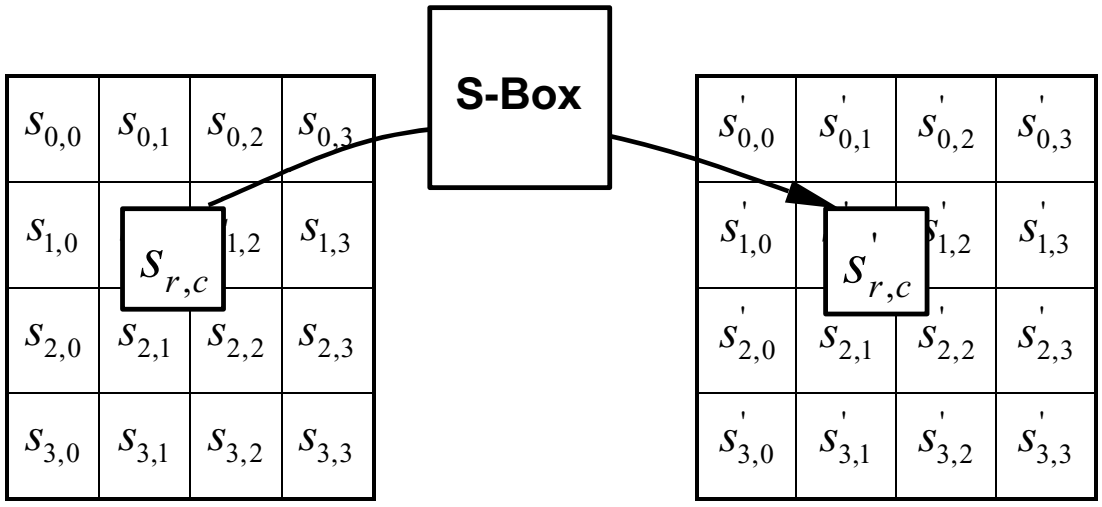



**Figure:** `SubByte()`作用在状态的单个字节上

# S盒运算：SubByte

- Subbytes的数学结构：见p.82 算法3.4
- Subbytes可以用查表方式实现：见p.81 表3.8所示的$S$盒。
  查表方法：

  输入 $XY$，其中$X, Y$都是4比特
  输出 $S$盒的第$X$行第$Y$列的项。

  例：

  输入 $(00111011)_2$，那么$X = (0011)_2 = 0x3$，$Y = (1011)_2 = 0xB$
  输出 $S$盒的3行$B$列的项是$E2$，二进制表示为11100010
- Subbytes在软件实现中用1维表格实现比2维快速（印刷版使用2维表格是出于方便表示），一次查表操作1维表格只需1次操作，2维表格则需要额外计算行和列。1维表格的$XY$位置的值对应$S$盒中$X$行$Y$列值。从1维表格可以很方便计算出其逆置换(方法请参考代换密码)。

# 行移位：ShiftRow

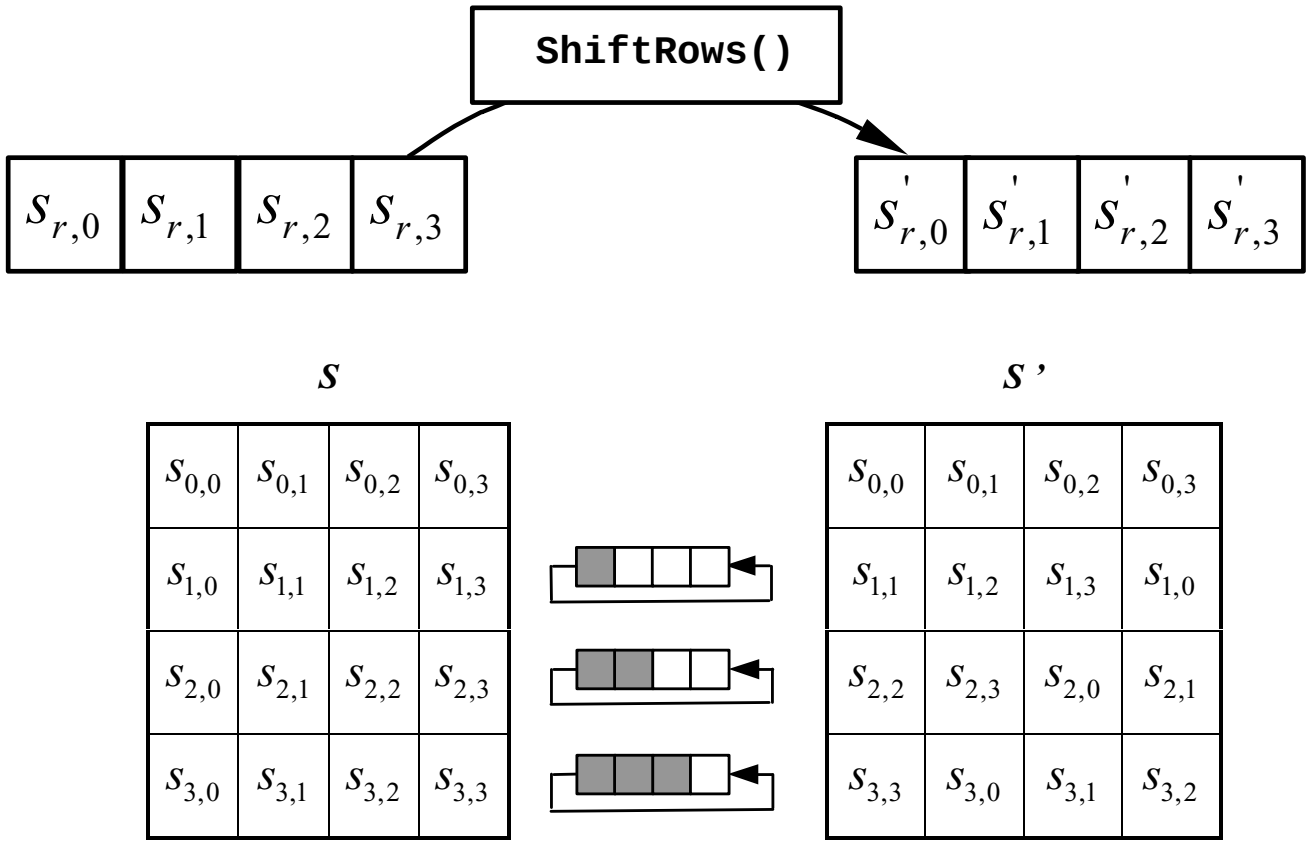



**Figure:** ShiftRow()作用在状态的行上

# 列混合：MixColumn

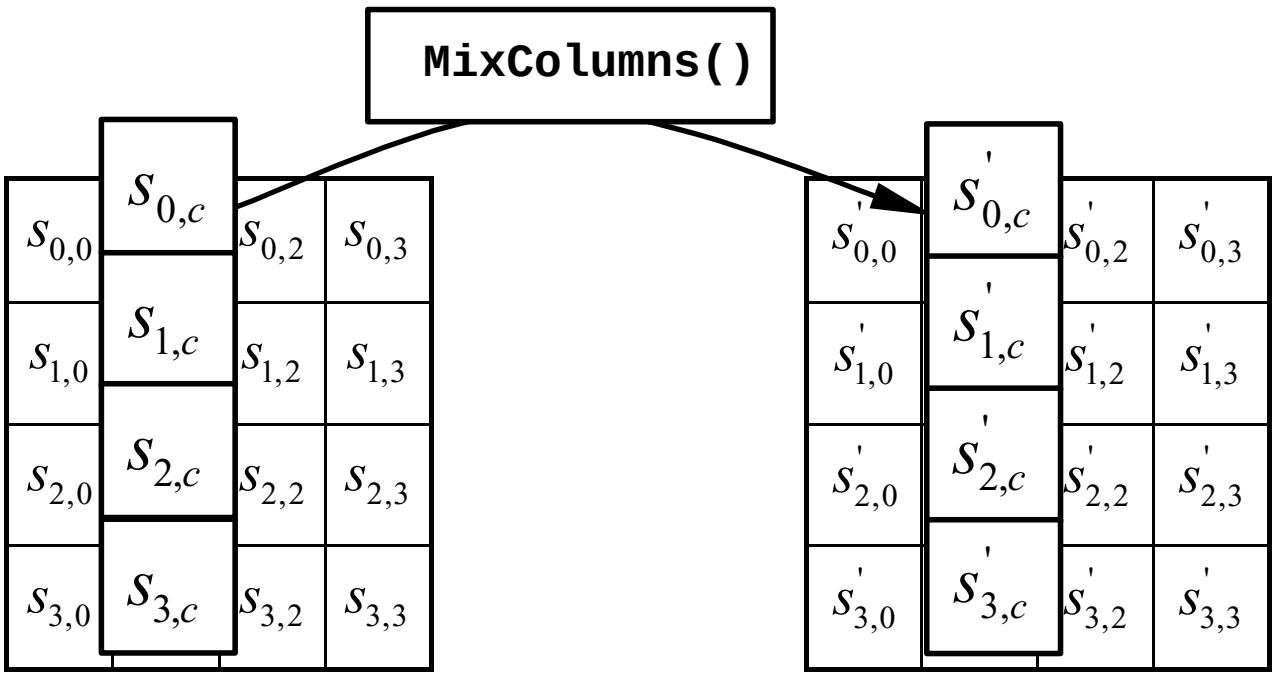



**Figure:** `MixColumn()`在状态的列上运算

# 列混合：MixColumn

- MixColumn的数学结构：将状态的列视为系数在有限域$GF(2^8)$上的多项式$a(x)$，输出为$a(x)c(x) \bmod x^4+1$；其中$c(x)$为

$$c(x) = \text{`}03'x^3 + \text{`}01'x^2 + \text{`}01'x + \text{`}02'$$

$c(x)$与$x^4+1$互素，因此是模$x^4+1$可逆的。

- MixColumn运算可以表示成$GF(2^8)$上的可逆线性变换

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

p.83 算法3.5表示了以上的矩阵运算。

# 列混合：MixColumn

MixColumn(c)的快速软件实现(对第$c$列的字节$s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}$操作)

外部算法： $FieldMult(2, x)$

1 for $i \leftarrow 0$ to 3 do $x_i \leftarrow s_{i,c}$

2

$$s_{0,c} = x_1 \oplus x_2 \oplus x_3, \quad s_{1,c} = x_0 \oplus x_2 \oplus x_3$$
$$s_{2,c} = x_0 \oplus x_1 \oplus x_3, \quad s_{3,c} = x_0 \oplus x_1 \oplus x_2$$

3

$$x_0 = FieldMult(2, x_0), \quad x_1 = FieldMult(2, x_1)$$
$$x_2 = FieldMult(2, x_2), \quad x_3 = FieldMult(2, x_3)$$

4

$$s_{0,c} = s_{0,c} \oplus x_0 \oplus x_1, \quad s_{1,c} = s_{1,c} \oplus x_1 \oplus x_2$$
$$s_{2,c} = s_{2,c} \oplus x_2 \oplus x_3, \quad s_{3,c} = s_{3,c} \oplus x_3 \oplus x_0$$

## 列混合：MixColumn

$FieldMult(2, x)$：

输入 $x = a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0$，是8比特字节

1. $t = a_7$
2. $y = a_6 a_5 a_4 a_3 a_2 a_1 a_0 0$
3. if $t = 1$ $y = y \oplus 00011011$

输出 $y$

# 列混合：MixColumn

MixColumn(c)的逆操作的快速软件实现算法：

1 for $i \leftarrow 0$ to 3 do $x_i \leftarrow s_{i,c}$

2

$$s_{0,c} = x_1 \oplus x_2 \oplus x_3, \quad s_{1,c} = x_0 \oplus x_2 \oplus x_3$$
$$s_{2,c} = x_0 \oplus x_1 \oplus x_3, \quad s_{3,c} = x_0 \oplus x_1 \oplus x_2$$

3

$$x_0 = FieldMult(2, x_0), \quad x_1 = FieldMult(2, x_1)$$
$$x_2 = FieldMult(2, x_2), \quad x_3 = FieldMult(2, x_3)$$

4

$$s_{0,c} = s_{0,c} \oplus x_0 \oplus x_1, \quad s_{1,c} = s_{1,c} \oplus x_1 \oplus x_2$$
$$s_{2,c} = s_{2,c} \oplus x_2 \oplus x_3, \quad s_{3,c} = s_{3,c} \oplus x_3 \oplus x_0$$

# 列混合：MixColumn

MixColumn(c)的逆操作算法(续)：

**5**

$$x_0 = FieldMult(2, x_0 \oplus x_2), \quad x_1 = FieldMult(2, x_1 \oplus x_3)$$

**6**

$$\begin{aligned} s_{0,c} &= s_{0,c} \oplus x_0, \quad s_{1,c} = s_{1,c} \oplus x_1 \\ s_{2,c} &= s_{2,c} \oplus x_0, \quad s_{3,c} = s_{3,c} \oplus x_1 \end{aligned}$$

**7** $x_0 = FieldMult(2, x_0 \oplus x_1)$

**8**

$$\begin{aligned} s_{0,c} &= s_{0,c} \oplus x_0, \quad s_{1,c} = s_{1,c} \oplus x_0 \\ s_{2,c} &= s_{2,c} \oplus x_0, \quad s_{3,c} = s_{3,c} \oplus x_0 \end{aligned}$$

# 密钥异或：AddRoundKey

- AddRoundKey：轮密钥和输入逐比特异或。

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} \oplus \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

算法3.6 KeyExpansion(Key)
**external** RotWord(字节循环左移)
SubWord(对字节进行AES的S盒替换)(详见p.83)
常数$RCon[1], \ldots, RCon[10]$(常数见p.84)
**for** $i \leftarrow 0$ to 3
**do** $w[i] \leftarrow (key[4i], key[4i+1], key[4i+2], key[4i+3])$
**for** $i \leftarrow 4$ **to** 43

$$\textbf{do} \begin{cases} temp \leftarrow w[i-1] \\ \text{if } i \equiv 0 (\text{mod} 4) \\ \quad \text{then } temp \leftarrow \text{SubWord}(\text{RotWord}(temp)) \oplus Rcon[i/4] \\ w[i] \leftarrow w[i-4] \oplus temp \end{cases}$$

**return** $w[0], \ldots, w[43]$
第$i$轮密钥$= w[4i]||w[4i+1]||w[4i+2]||w[4i+3], i = 0, 1 \ldots, 10$

# AES的解密函数

1. 所有操作逆序进行
2. 密钥编排算法不变，但轮密钥顺序与加密函数的轮密钥相反
3. 所有操作均为加密函数的逆操作(SubBytes、ShiftRows和AddRoundKey的逆操作容易给出，MixColumn的逆操作已提供)

# AES的分析

- AES的设计能抵抗线性和差分分析
  - S盒使得的线性逼近和差分分布表趋于均匀；
  - 列混合使用了宽轨道策略，使得找到包含较少活动S盒的差分和线性分析成为不可能。
- 目前对AES的最好的分析方法是相关密钥分析：

| 分组长度 | 256 | 192 | 128 |
|---|---|---|---|
| 攻击复杂度 | $2^{99.5}$ | $2^{176}$ | 不比穷搜索快 |

相关密钥分析：假设攻击者能够获得一系列密钥加密的明文和密文对，虽然他不知道密钥值，但是知道这些密钥间的数学关系。

## 3.6节练习

练习3.5

# 3.7节：工作模式

工作模式：在分组密码中，使用同一密钥多次加密的方法。

1. 一般先对明文进行数据填充，使之长度为分组长度的倍数。
2. 对明文分块，按照某一工作模式加密。

# 3.7节：工作模式

DES的四种工作模式(1981年加入标准)：

- 电码本模式（ECB模式）
- 密码分组链接模式（CBC模式）
- 输出反馈模式（OFB模式）
- 密码反馈模式（CFB模式）

AES的推荐工作模式：

- 电码本模式（ECB模式）
- 密码分组链接模式（CBC模式）
- 输出反馈模式（OFB模式）
- 密码反馈模式（CFB模式）
- 计数模式（CTR）(2001年加入标准)
- XTS模式(2010年加入标准)

以上工作模式均用于机密性，另有用于消息认证码的工作模式：

- 计数密码分组链接模式（CCM模式）：将于第4章的4.4.2节介绍

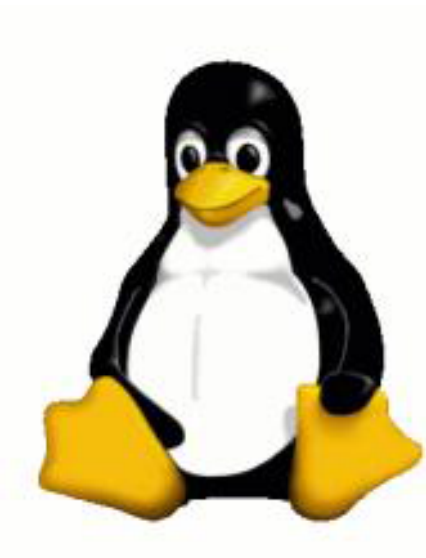
# 电码本模式（ECB模式）

明文分组序列 $x_1, x_2, \ldots$

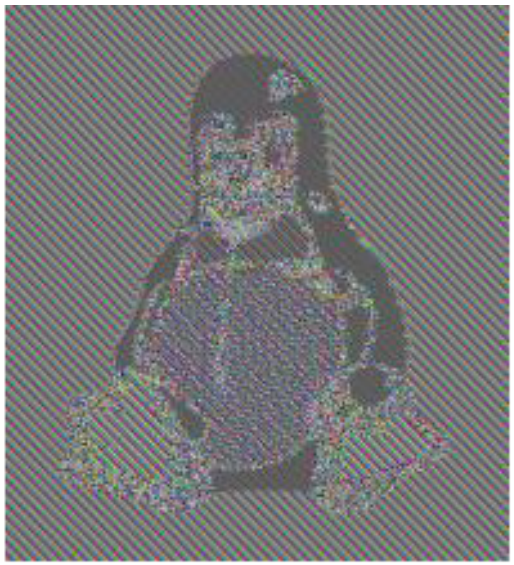
加密 $y_1 = e_K(x_1), y_2 = e_K(x_2), \ldots$

解密 $x_1 = d_K(y_1), x_2 = d_K(y_1), \ldots$

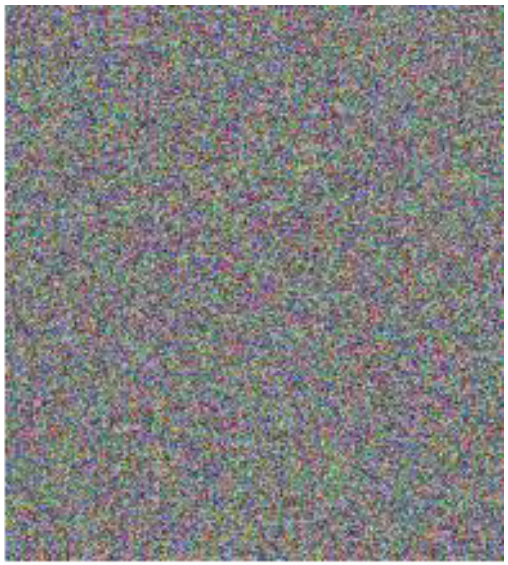
- 缺点：同一明文分组加密成同一密文分组，无法完全掩盖明文的统计特性。
  - 例：下图中，以每一像素为分组进行ECB加密，我们看到加密后仍能看出图案的形状，而其它工作模式是看不来的。



原始图片



ECB加密模式



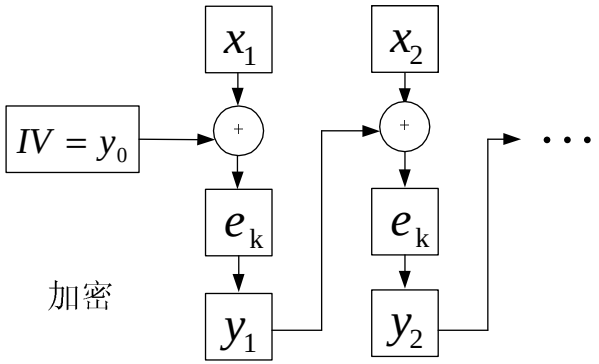
其它加密模式

# 密码分组链接模式（CBC模式）

初始向量：$IV$

加密：

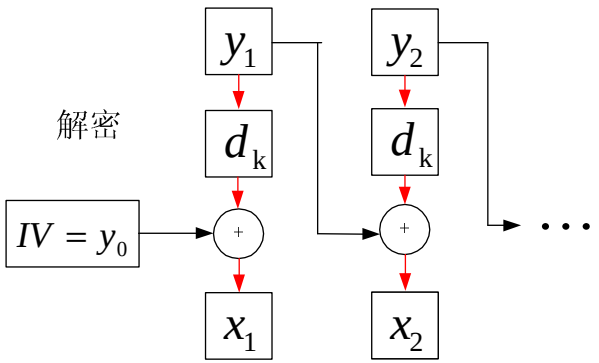
$$
\begin{aligned}
y_0 &= IV \\
y_1 &= e_K(y_0 \oplus x_1) \\
y_2 &= e_K(y_1 \oplus x_2) \\
&\cdots
\end{aligned}
$$




密文：$y_1, y_2, \cdots$

解密：

$$
\begin{aligned}
y_0 &= IV \\
x_1 &= d_K(y_1) \oplus y_0 \\
x_2 &= d_K(y_2) \oplus y_1 \\
&\cdots
\end{aligned}
$$



# 输出反馈模式（OFB模式）

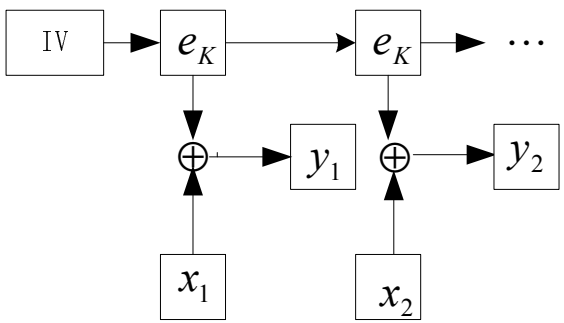
初始向量：$IV$

加密：

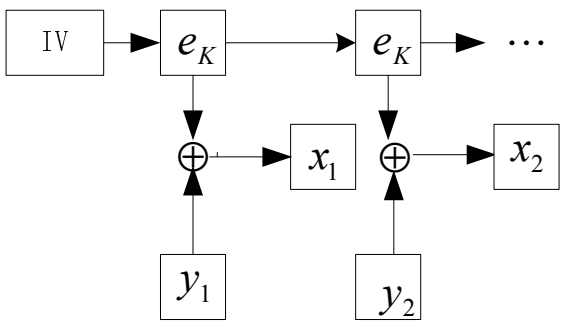
$$\begin{aligned} z_0 &= IV \\ z_i &= e_K(z_{i-1}) \\ y_i &= x_i \oplus z_i, i = 1, 2, \ldots \end{aligned}$$

解密：

$$\begin{aligned} z_0 &= IV \\ z_i &= e_K(z_{i-1}) \\ x_i &= y_i \oplus z_i, i = 1, 2, \ldots \end{aligned}$$




OFB加密



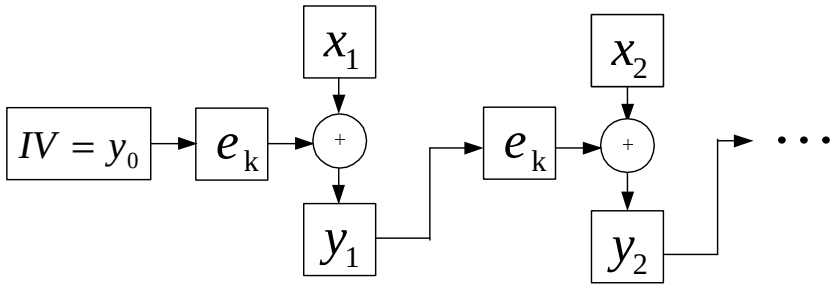

OFB解密

# 密码反馈模式（CFB模式）

初始向量：$IV$

加密：

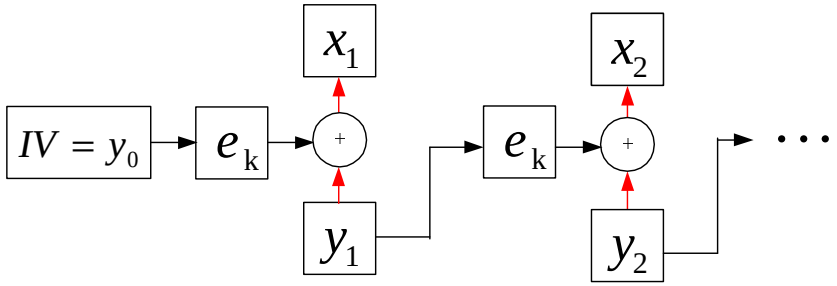
$$
\begin{aligned}
y_0 &= IV \\
z_i &= e_K(y_{i-1}) \\
y_i &= x_i \oplus z_i \\
& \quad i = 1, 2, \ldots
\end{aligned}
$$




加密

解密：

$$
\begin{aligned}
y_0 &= IV \\
z_i &= e_K(y_{i-1}) \\
x_i &= y_i \oplus z_i \\
& \quad i = 1, 2, \ldots
\end{aligned}
$$




解密

# 计数模式（CTR模式）

计数模式类似于OFB模式，差别是密钥流产生机制不同。
计数模式的工作方式：

1. 计数器$ctr$：$m$长比特串
2. 由$ctr$递归构造$m$长比特串：

$$T_i = ctr + i - 1 \bmod 2^m$$

3. 对所有的$i \geq 1$，如下加密明文分组$x_1, x_2, \ldots$

$$y_i = x_i \oplus e_k(T_i)$$

# 四种工作模式的优缺点

ECB的缺点：相同的明文分组产生相同的密文分组

改变一个明文分组，对四种模式的影响：

- ECB：只影响当前分组
- CBC：当前分组和后续分组都受影响（该特点可用做认证码）
- OFB：只影响当前分组（该特点可用在卫星通信中）
- CFB：当前分组和后续分组都受影响（该特点可用做认证码）

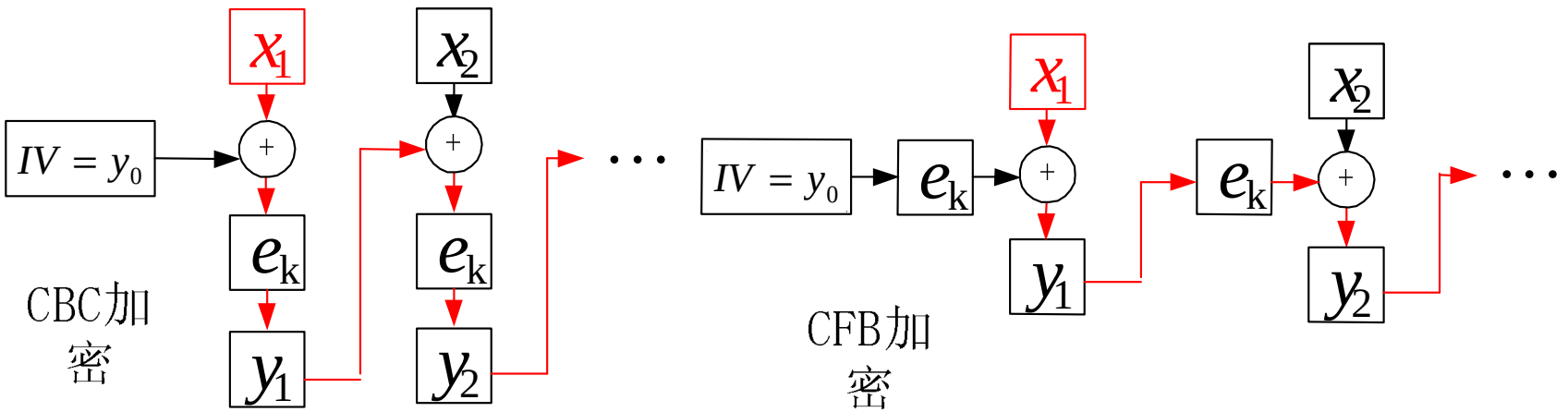



**Figure:** 一个明文分组的错误对密文的影响

## 3.7节作业

练习：3.7（讨论一个密文分组出错对解密得到的明文的影响）