对称密码设计与实现

第 2 讲

北京电子科技学院
密码系
李艳俊

本讲内容

第2章　基础部件的设计及分析

2.1　S盒的密码指标及设计

2.2　EASY1 分组密码差分分析

作 业

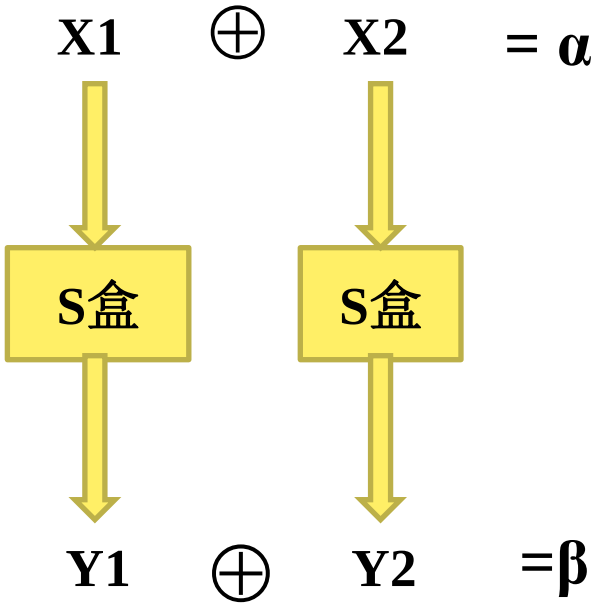
2.1 S盒的密码指标及设计

检测S盒的六个指标

in	0	1	2	3	4	5	6	7
out	0	3	6	1	4	7	2	5

in	0	1	2	3	4	5	6	7
out	2	1	3	0	6	4	7	5

in	0	1	2	3	4	5	6	7
out	2	5	3	7	6	4	0	1



P(α→β)=?

例1 S盒密码指标——差分均匀度

000	001	010	011	100	101	110	111
010	111	101	000	011	001	100	110

$$\delta_s(\alpha,\beta)=\left|\left\{x\in GF(2)^n : S(x)\oplus S(x\oplus\alpha)=\beta\right\}\right|$$

差分分布表

α,β	000	001	010	011	100	101	110	111
000	8	0	0	0	0	0	0	0
001	0	0	4	0	0	4	0	0
010	0	0	0	0	0	0	0	8
011	0	**0**	**4**	**0**	**0**	**4**	**0**	**0**
100	0	**4**					**4**	
101	0			**4**	**4**			
110	0	**4**					**4**	
111	0			**4**	**4**			

差分均匀度

1.差分均匀度

S盒是分组密码的基本非线性模块，衡量S盒抵抗差分分析能力的重要指标：差分均匀度。

定义：对于一个函数

$$S(x)=\left(f_1(x),\ldots,f_m(x)\right):\mathrm{GF}(2)^n\to\mathrm{GF}(2)^m,n\geq m,$$

差分均匀度为：$\delta_S=\max\limits_{\substack{\beta\in GF(2)^m\\ 0\neq\alpha\in GF(2)^n}}\delta_S(\alpha,\beta)$

其中 $\delta_s(\alpha,\beta)=\left|\left\{x\in GF(2)^n:S(x)\oplus S(x\oplus\alpha)=\beta\right\}\right|$

作业：检测以下3个S盒的差分分布表和差分均匀度

in	0	1	2	3	4	5	6	7
out	0	3	6	1	4	7	2	5

in	0	1	2	3	4	5	6	7
out	2	1	3	0	6	4	7	5

in	0	1	2	3	4	5	6	7
out	2	5	3	7	6	4	0	1

差分均匀度为2

2. 非线性度

定义： 令$f(x):GF(2^n)\to GF(2)$是一个**n**元布尔函数，称

$$N_f=\min_{l\in L_n} d_H(f,l)$$

为**f(x)**的非线性度。其中L_n表示全体**n**元线性和仿射函数的集合，

$d_H(f,l)$表示**f**和**l**之间的汉明距离。

定义：令$S(x)=(f_1(x),\cdots,f_m(x)):GF(2)^n\to GF(2)^m$是一个多输出函数，则

$$N_s=\min_{\substack{l(x)\in L_n\\ u\neq 0\in GF(2)^m}} d_H(u\cdot S(x),l(x))$$

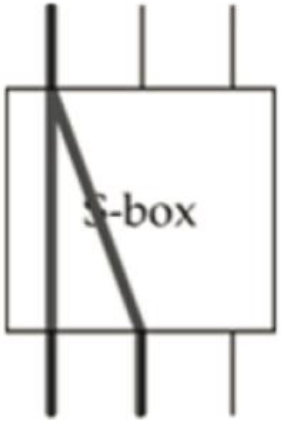
为**S (x)**的非线性度。

例2 S盒的非线性度

[3, 7, 2, 4, 1, 5, 0, 6]

000	001	010	011	100	101	110	111
011	111	010	100	001	101	000	110

$$N_s(\alpha,\beta)=\#\left\{x\in GF(2)^n : \alpha\cdot x=\beta\cdot S(x)\right\}$$



X2 = Y1 ⊕ Y2

p = 1/4

α,β	000	001	010	011	100	101	110	111
000								
001								
010								
011								
100	4	4	2	6	4	4	2	2
101								
110								
111								

偏差Bias is $|\frac{1}{4}-1/2|=1/4$

作业：检测以下3个S盒的非线性度。

in	0	1	2	3	4	5	6	7
out	0	3	6	1	4	7	2	5

in	0	1	2	3	4	5	6	7
out	2	1	3	0	6	4	7	5

in	0	1	2	3	4	5	6	7
out	2	5	3	7	6	4	0	1

3．代数次数和项数分布

S盒的代数次数用于衡量S盒的代数非线性程度，代数次数的大小一定程度上反映了S盒的线性复杂度，S盒线性复杂度越高，越难用线性表达式逼近，而项数分布的程度和插值攻击密切相关。

定义： 设 $f(x):GF(2)^n \to GF(2)$ 的**代数正规型（ANF）**为

$$f(x)=a_0 \oplus \sum_{\substack{1\le i_1<\cdots<i_k\le n \\ 1\le k\le n}} a_{i_1 i_2 \cdots i_k} x_{i_1} x_{i_2} \cdots x_{i_k}$$

则$f(x)$的**代数次数** $D(f)=\max\left\{0\le k\le n \middle| a_{i_1 i_2 \cdots i_k}=1, 1\le i_1<\cdots<i_k\le n\right\}$

其中 $x=(x_1,\cdots,x_n)$， $a_0, a_{i_1 i_2 \cdots i_k} \in GF(2)$。

$f(x)$的代数正规型中的i次项的个数称为$f(x)$的i次项数，所有i $(1\le i\le n)$ 次项数之和称为$f(x)$的**项数**。

定义：设 $n\times m$ S盒 $F(x)=(f_1(x),\cdots,f_m(x))$，其代数次数定义为

$$D(F)=\max\left\{D(\beta\cdot F)\middle|\beta\neq 0,\beta\in GF(2)^m\right\}$$

$$=\max\left\{D(\bigoplus_{i=1}^{m}b_i f_i(x))\middle|(b_1,\cdots,b_m)\neq 0,(b_1,\cdots,b_m)\in GF(2)^m\right\}.$$

特别地，当 $D(F)$ =k时，称为k次S盒。

例：设n=m=3，令

$$f_1(x)=x_1x_2\oplus x_1x_3\oplus x_1\oplus x_2$$

$$f_2(x)=x_1\oplus x_1x_3\oplus x_3$$

$$f_3(x)=1\oplus x_1\oplus x_1x_2\oplus x_2x_3$$

则 $GF(2)^3$ 上置换 $F(x)=(f_1(x),f_2(x),f_3(x))$

代数次数 $D(F)=3-1=2$

000	001	010	011	100	101	110	111
011	111	010	100	001	101	000	110

用真值表的方式写出代数正规型：

x2	x1	x0	y2	y1	y0
0	0	0	0	1	1
0	0	1	1	1	1
0	1	0	0	1	0
0	1	1	1	0	0
1	0	0	0	0	1
1	0	1	1	0	1
1	1	0	0	0	0
1	1	1	1	1	0

$$y_0 = f_0(x)$$
$$= \overline{x_2}\,\overline{x_1}\,\overline{x_0} \oplus \overline{x_2}\,\overline{x_1}x_0 \oplus \overline{x_2}x_1\overline{x_0} \oplus x_2\overline{x_1}\,\overline{x_0}$$
$$= 1 \oplus x_1$$

练习：写出y2，y1的代数正规型。

作业：写出以下3个S盒的代数正规型。

in	0	1	2	3	4	5	6	7
out	0	3	6	1	4	7	2	5

in	0	1	2	3	4	5	6	7
out	2	1	3	0	6	4	7	5

in	0	1	2	3	4	5	6	7
out	2	5	3	7	6	4	0	1

4. 雪崩特性和 5.扩散特性

严格雪崩特性和扩散特性用于衡量S盒的输入改变量和输出改变量之间的随机性，也是S盒设计的重要指标之一。

除了以上五个指标以外，还有针对代数攻击而提出的代数免疫阶指标。根据不同的解方程算法，代数免疫阶的定义不同，具体见[1]。此外，S盒最好是可逆的。

[1] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with over defined systems of equations. Proceedings of ASIACRYPT 2002, Lecture Notes in Computer Science 2501, pp. 267-287, 2002.

2.1 S盒的密码指标及设计

S盒的构造方法主要有以下几种：

1. **随机生**

尽管

来寻找好

力允许的

2. 基于一

1976年，美国NSA披露了DES的S盒设计原则：

✓每个S-盒的每一行是整数0~15的一个全排列；

✓每个S-盒的输出都不是其输入的线性或仿射函数；

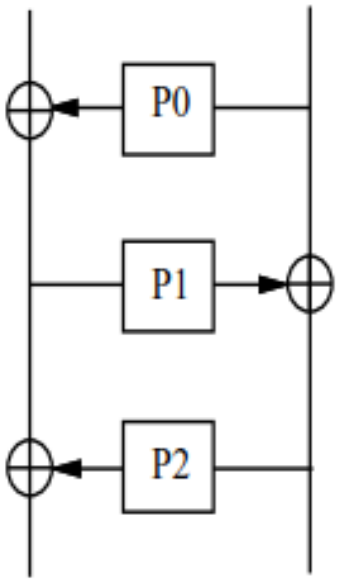
✓改变任一S-盒任意1bit的输入，其输出至少有2bit发生变化；

✓……

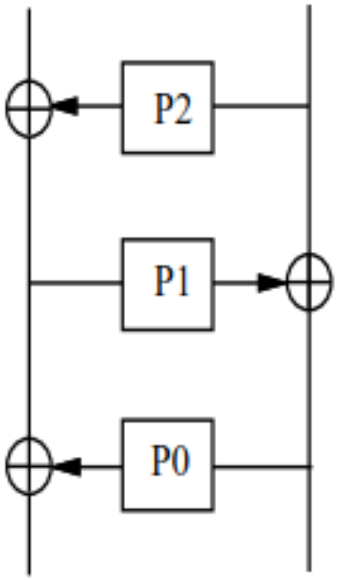
Serpent算法所使用的S盒就是基于DES中S盒满足的要求构造出来的。通过这种构造方法找到一个满足各项指标的S盒并不容易，小规模S盒组合构造的方式有很多，测试量较大，而且很有可能组合生成的新S盒不满足某项设计指标。

3.通过使用某个**特定的密码结构**来构造S盒。

例：CRYPTON v0.5中使用的S盒利用3轮Feistel结构来构造.



S0



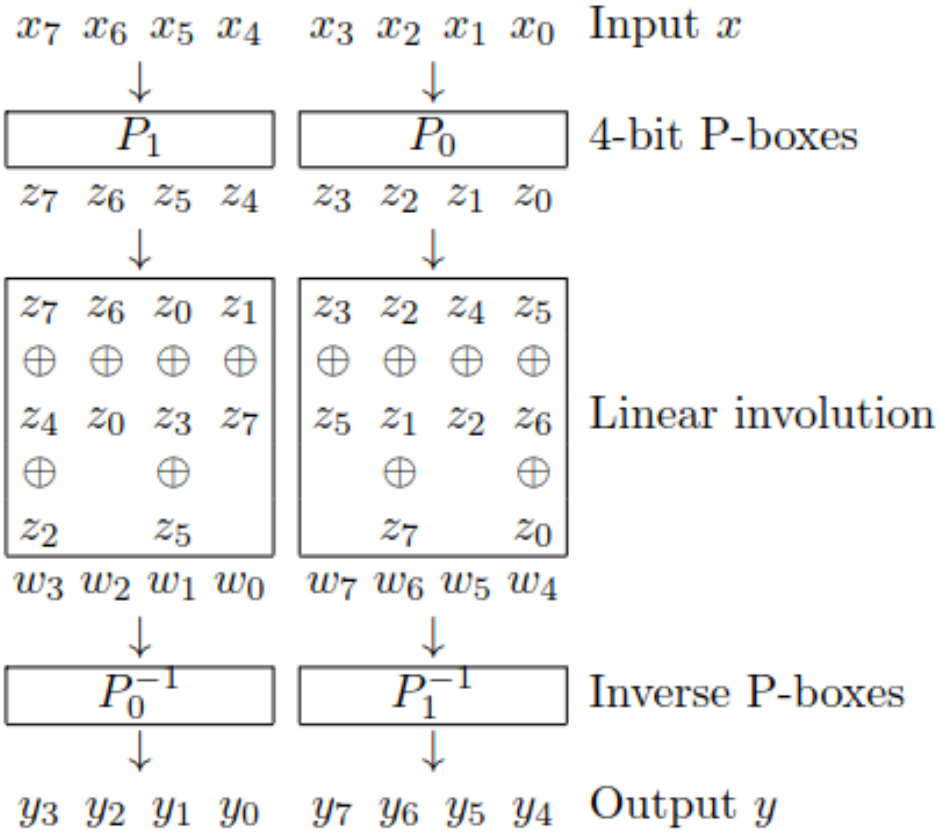
S1

P0，P1，P2是3个4*4的S盒

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P_0	15	9	6	8	9	9	4	12	6	2	6	10	1	3	5	15
P_1	10	15	4	7	5	2	14	6	9	3	12	8	13	1	11	0
P_2	0	4	8	4	2	15	8	13	1	1	15	7	2	11	14	15

- 这个S盒的密码指标与P0、P1、P2是什么关系？

例：CRYPTON v1.0中使用的S盒利用可逆SP结构来构造.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P_0	15	14	10	1	11	5	8	13	9	3	2	7	0	6	4	12
P_1	11	10	13	7	8	14	0	5	15	6	3	4	1	9	2	12

- 这个S盒的密码指标怎么样？
- 如何改进？

4. 数学函数，包括指数函数、对数函数、幂函数（逆函数可以看作幂函数的一种）、混沌映射，以及基于不同群上数学函数的复合。

例：**AES算法的S盒**由以下两个域上的变换合成而得：

①对于$\underline{x}\neq 00$，$\underline{x}\rightarrow\underline{x}^{-1}$（在$GF(2^8)$中）；$00\rightarrow 00$。

②
$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$
（F_2上仿射变换）

例： ①对于$57^{-1} \rightarrow 57^{-1} = BF$;

②

$$BF: \begin{pmatrix}1\\1\\1\\1\\1\\1\\0\\1\end{pmatrix} \mapsto \begin{pmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\\1\\1\\0\\1\end{pmatrix} + \begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\\1\\0\\1\\0\end{pmatrix} + \begin{pmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{pmatrix} = \begin{pmatrix}1\\1\\0\\1\\1\\0\\1\\0\end{pmatrix} : 5B$$

所以有：57→5B

同理，有12 →C9； 35 →96； 49 →3B； ……

2.1 S盒的密码指标及设计

为了提高软件实现速度，将上述S盒变换做成如下替换表：

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	B2	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

00	01	02	…	0F	10	11	…	FE	FF
63	7C	77		76	CA	82		BB	16

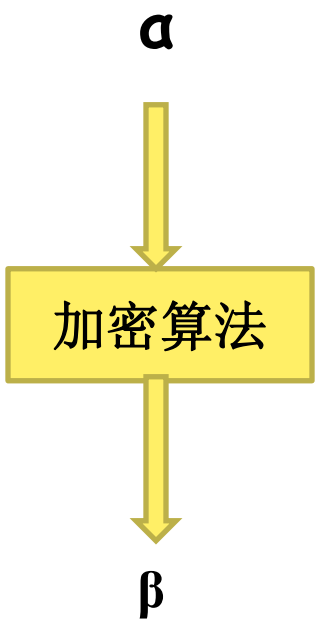
2.1 S盒的密码指标及设计

此外，S盒还可以基于**几乎完全非线性置换**设计，如MISTY算法中使用的S盒；或基于**电路结构**设计、基于人工智能**遗传算法**设计、基于**混沌映射**方法设计等等。

区别：随机实现的S盒性能不易达到最好，非随机实现的则易达到安全性最优，或者更易于软硬件实现和优化。

2.2 EASY1 分组密码差分分析

- 利用S盒差分分布表对算法进行分析



P(α→β)

如果 f(x)=y 是线性函数，则满足以下性质：

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

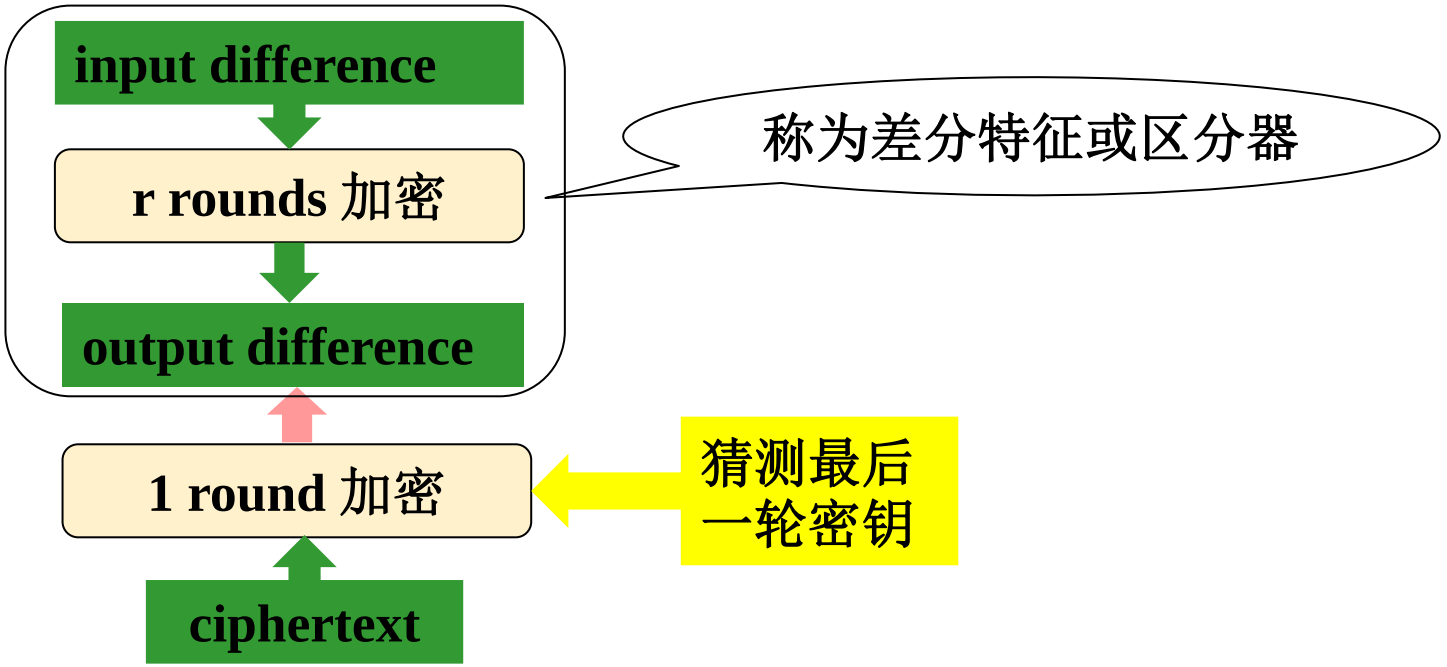
$$y \oplus y' = f(x \oplus x')$$

设 $\Delta x = x \oplus x'$

则 $\Delta y = f(\Delta x)$

2.2 EASY1 分组密码差分分析

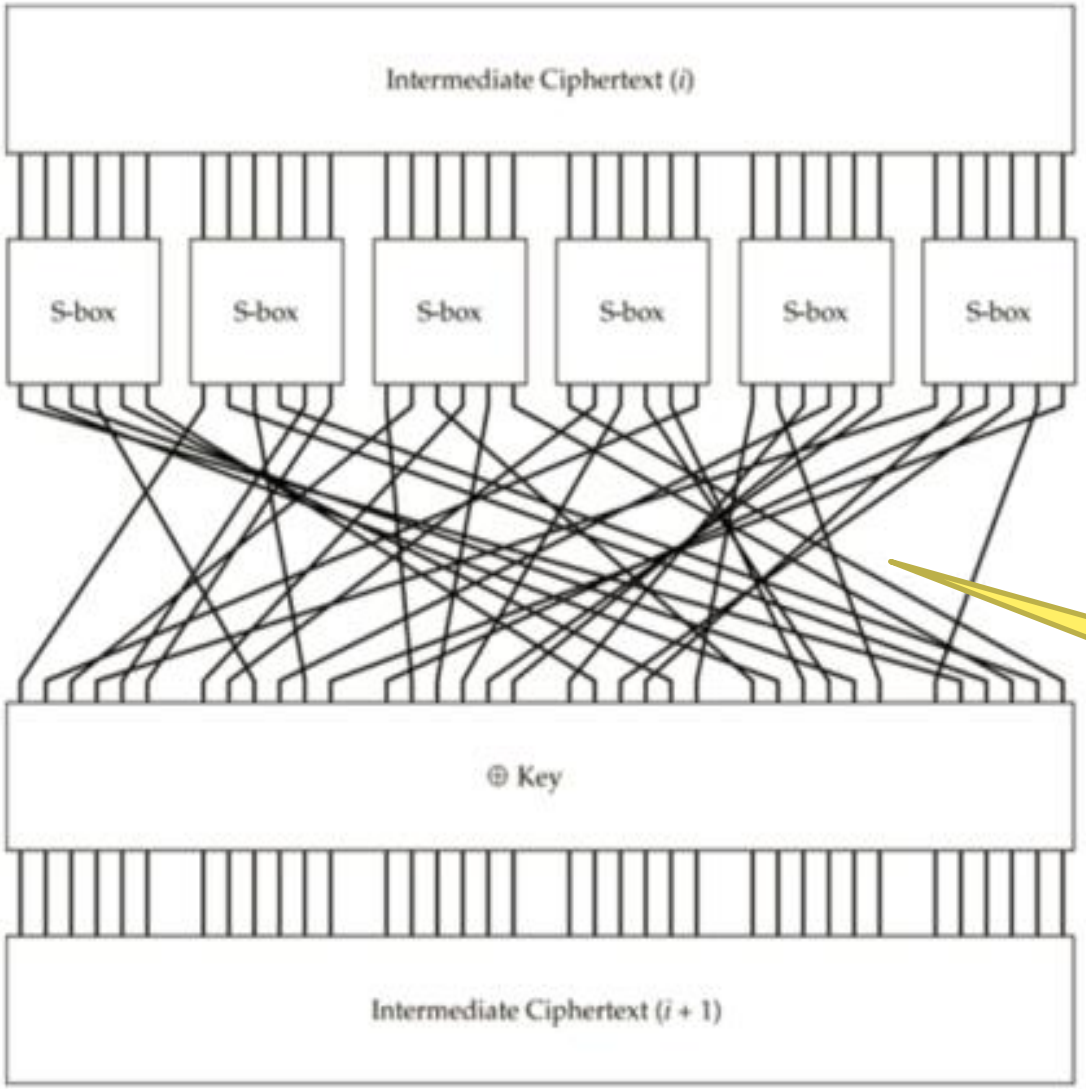
◆对于r轮分组算法，如果存在差分轨迹，其概率为$P(\alpha \to \beta) < 1$，且大于随机函数的概率，那么称之为差分特征或差分区分器。



*密钥比特也可以由最后一轮S盒的差分特征推导得到

2.2 EASY1 分组密码差分分析

Figure 4-5 EASY1 SPN cipher for a single round.



分组长度: 36-bit

密钥长度: 18-bit

S-box: 6 bits to 6 bits

P-线性置换

2.2 EASY1 分组密码差分分析

Ω_Y \ Ω_X	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	2	0	2	2	2
2	0	0	0	0	0	2	0	0	0	0	0	0	2	2	2	0
3	0	0	2	0	0	2	2	0	2	0	0	0	0	2	4	0
4	0	2	0	2	2	0	0	0	2	2	2	0	2	2	0	0
5	0	0	0	0	0	2	0	0	4	0	0	0	0	0	0	0
6	0	0	0	2	2	0	6	0	2	2	0	2	2	0	2	2
7	0	0	0	2	0	4	0	0	0	4	2	0	0	0	2	0
8	0	4	2	0	0	0	4	2	2	0	2	2	2	2	0	2
9	0	2	0	0	0	2	0	2	0	0	0	0	0	0	0	4
a	0	0	0	0	0	0	2	2	0	2	0	2	0	4	0	2
b	0	2	0	2	0	0	0	0	0	0	8	2	0	0	0	4
c	0	2	2	0	0	2	0	0	0	0	2	2	2	0	2	2
d	0	2	0	2	0	0	0	2	0	2	0	0	2	0	2	2
e	0	2	2	0	2	0	0	2	0	2	0	0	0	0	0	2
f	0	0	2	2	2	0	0	0	0	0	0	0	0	0	0	2

EASY1 算法S盒部分差分特征表

表中最大的两个值是6 和8, 对应的概率分别为6/64 和 8/64。

差分分析

(000110 ⇒ 000110) (000110 ⇒ 100001)
(000110 ⇒ 110000) (000111 ⇒ 101001)
(001001 ⇒ 011000) (001001 ⇒ 100010)
(001001 ⇒ 110010) (001010 ⇒ 110111)
(001100 ⇒ 101110) (001101 ⇒ 010100)
(001110 ⇒ 110001) (010001 ⇒ 010100)
(010010 ⇒ 000001) (010011 ⇒ 001000)
(011011 ⇒ 100101) (011100 ⇒ 001100)
(011100 ⇒ 111111) (011101 ⇒ 111001)
(011110 ⇒ 010101) (011111 ⇒ 100110)
(100000 ⇒ 100111) (100010 ⇒ 001101)
(100011 ⇒ 000110) (100101 ⇒ 000001)
(101000 ⇒ 001100) (101011 ⇒ 001100)
(101011 ⇒ 111100) (101100 ⇒ 101011)
(101101 ⇒ 000011) (110010 ⇒ 101101)
(110011 ⇒ 011111) (110011 ⇒ 101111)
(111000 ⇒ 100000) (111001 ⇒ 001001)
(111001 ⇒ 001101) (111011 ⇒ 010100)
(111011 ⇒ 111110) (111100 ⇒ 011100)
(111100 ⇒ 100000) (111101 ⇒ 000100)

probabilities of 6/64

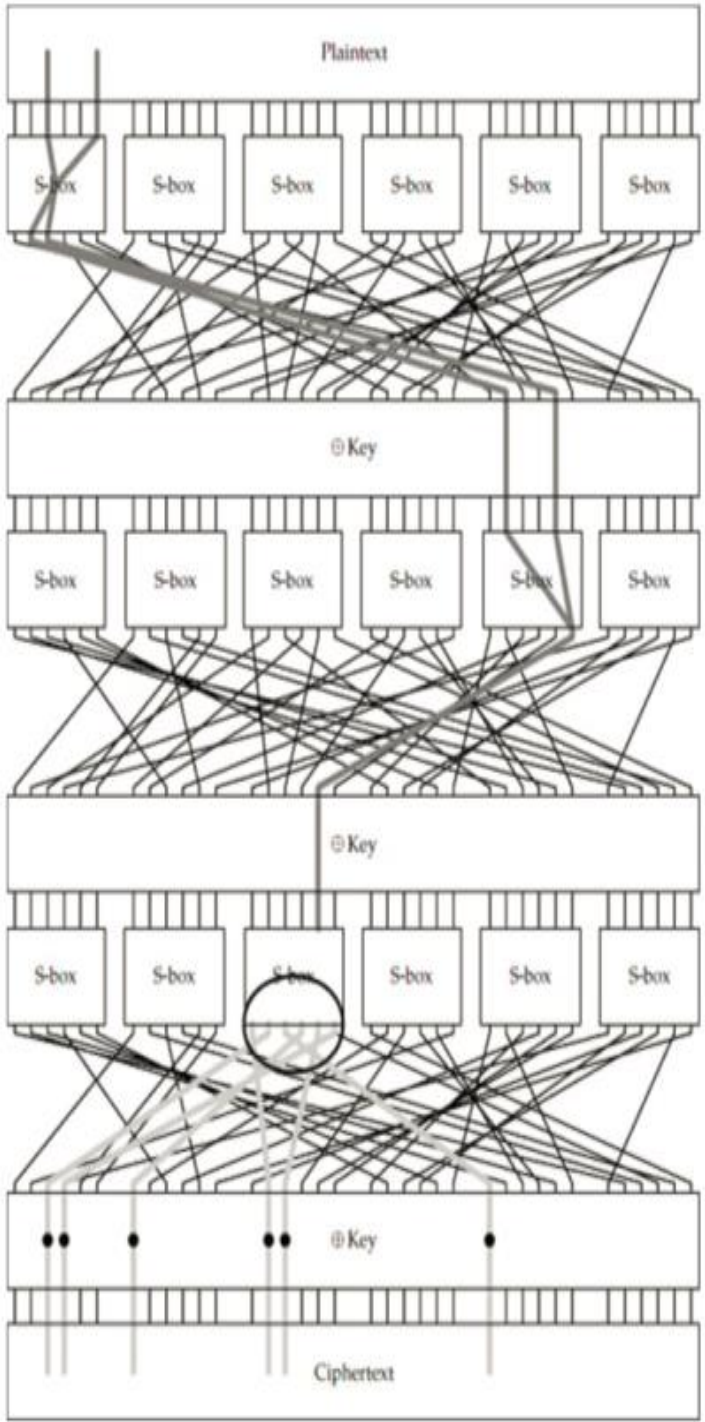
probabilities of 6/64

(001011 ⇒ 001010)

(010000 ⇒ 011001)

(011001 ⇒ 010110)

(110101 ⇒ 101001)



密码差分分析

001001 ⇒ 011000)

probability of 6/64

$$\frac{6}{64} \times \frac{6}{64} \approx 0.008789$$

010010 ⇒ 000001)

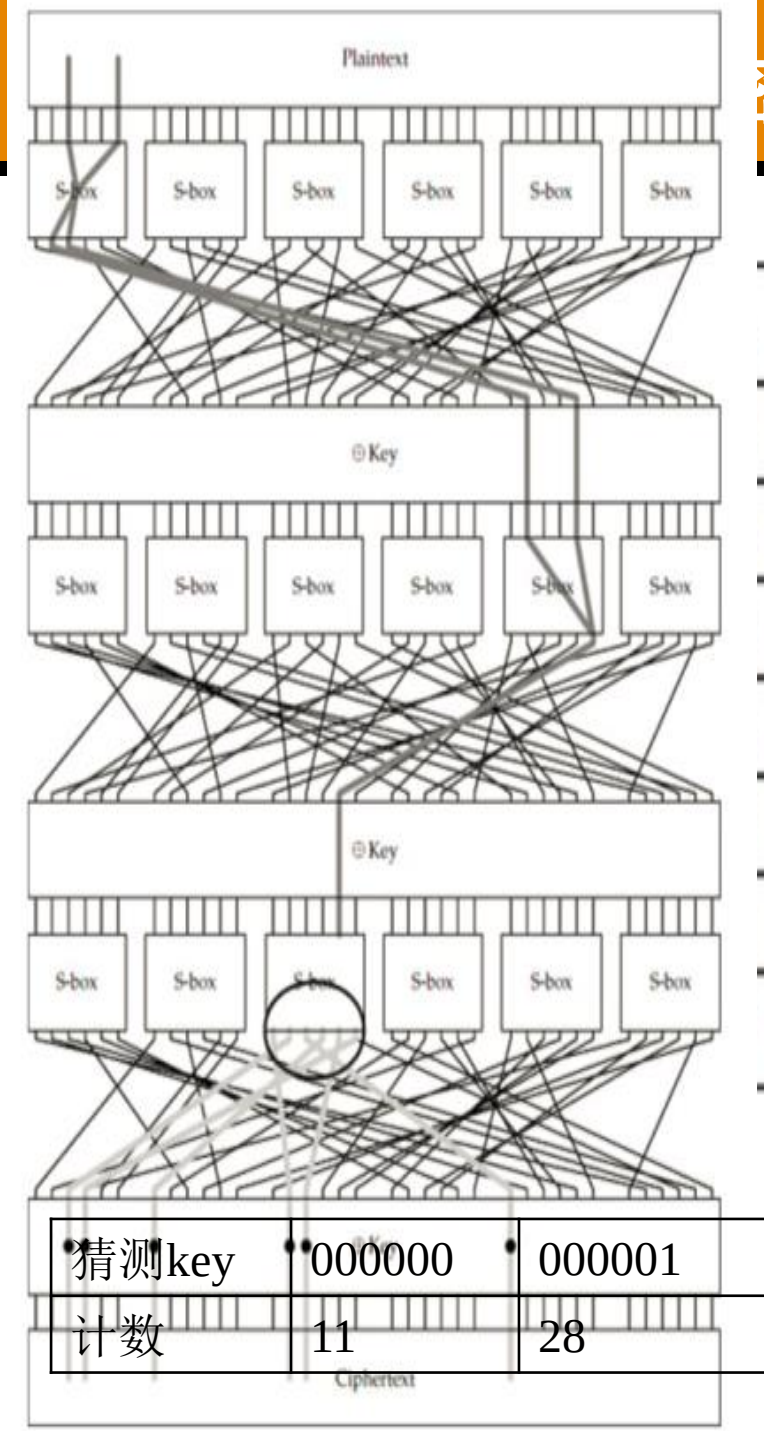
probability of 6/64

差分分析步骤

1. 现在构建3轮差分特征，$p \sim 2^{-7}$；

2. 选择满足输入差分的明文对，若输出密文对满足期望的差分，则称之为正确的明密文对；

3. 由正确的明密文对可推测出正确的密钥。



10
9
13
13
17
18
21
13

恢复密钥攻击

1. 猜测最后一轮相关的6个密钥比特；

2. 将猜测的密钥与密文对异或，得到最后一轮S盒的输出对；

3. 将S盒差分对与差分特征的输出差分进行匹配。

若匹配上的话，对猜测密钥值计数加1，计数最多的密钥为正确密钥。

猜测key	000000	000001	000010	000011	000100	…	111111	总计
计数	11	28	7	11	14	…	13	1000

2.2 EASY1 分组密码差分分析

这项工作需要$2^6 \times 1000 \approx 2^{16}$次操作。

暴力破解剩余的密钥比特需要2^{30}次操作。

总结：暴力破解需要2^{36}次操作，这里只需要2^{30}次。

Question: How can we reduce the total work?

作 业

1. 构造一个3bit输入输出的S盒，测试其密码指标，并根据指标进行调整，最后得到理想的S盒。

2.选择一个算法，学习它的S盒设计方法，完成对S盒设计描述（包括visio画图和密码指标测试结果）。

AES	Present	Keccak
ARIA	Crypton	Picolo
Camellia	MISTY	SKINNY
LBlock	Kasumi	Led
Serpent	SAFER	BLACK
SM4	E2	SKEIN

差分均匀度

非线性度

代数次数和项数

雪崩和扩散

代数免疫阶

后两个选做