AES 加密算法

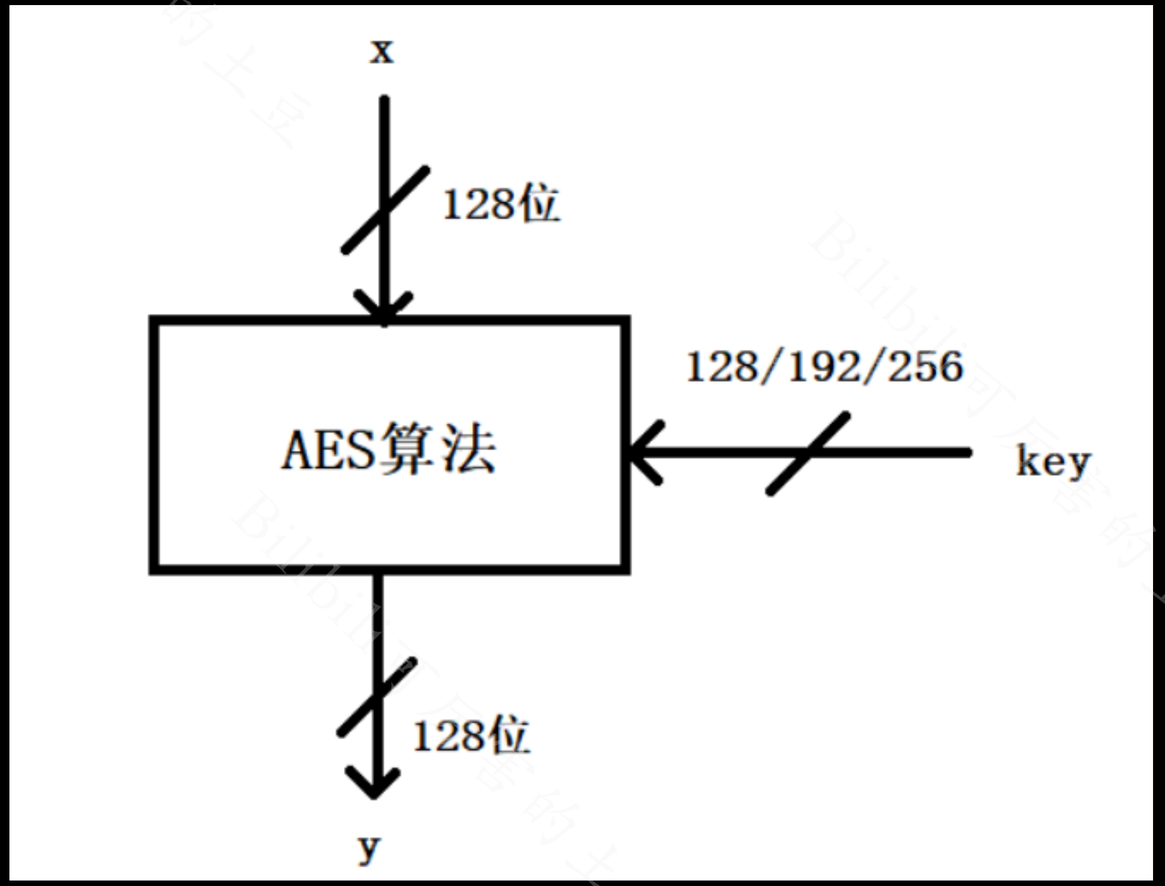
Advanced Encryption Standard

—可厉害的土豆

AES 属于 分组加密 算法

明文长度固定为128位

密钥长度可以是128、192、256位



明文与密钥的长度均为128比特（16字节）

参考资料: [1]

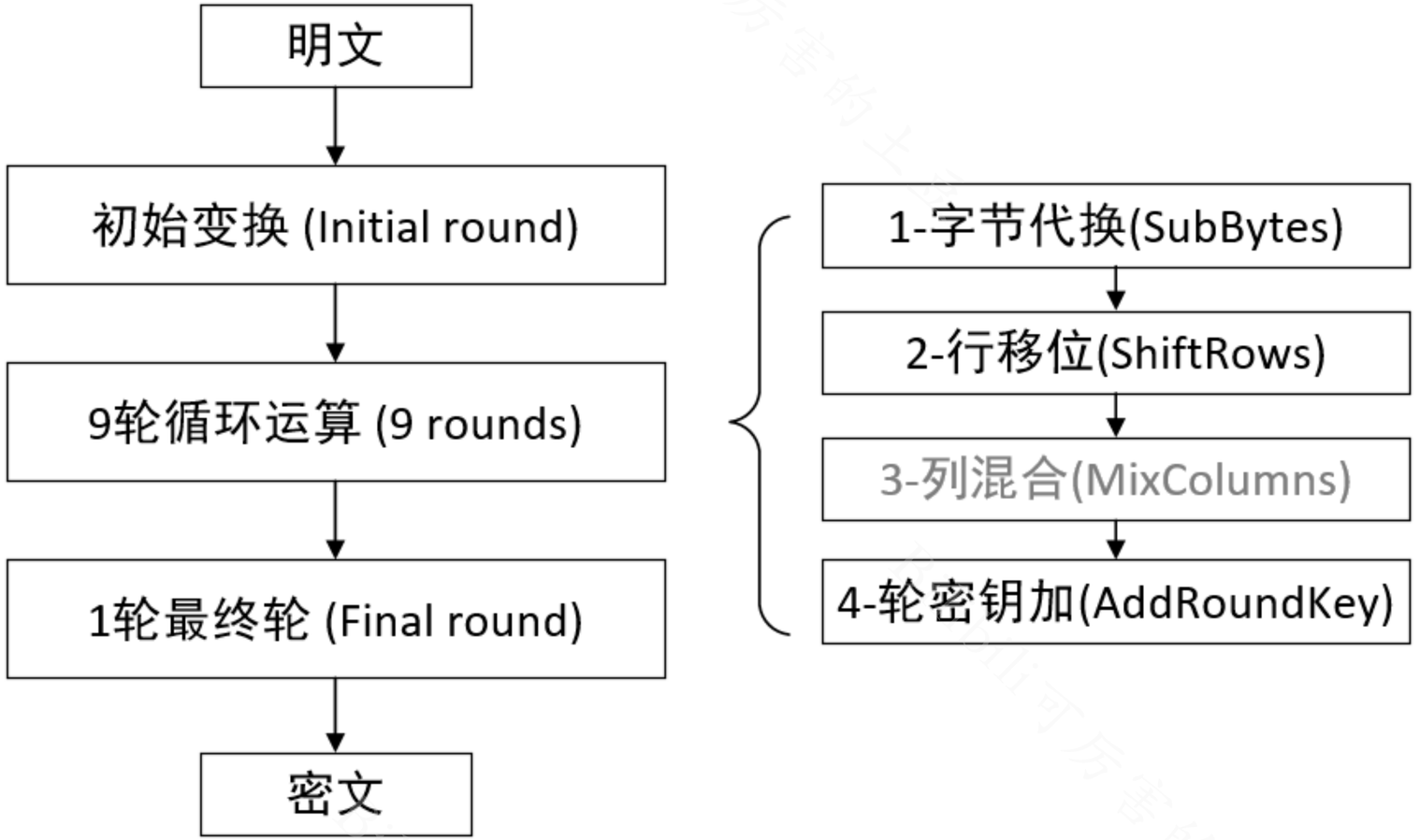
输入的字节顺序:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

规定的字节排列方式:

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

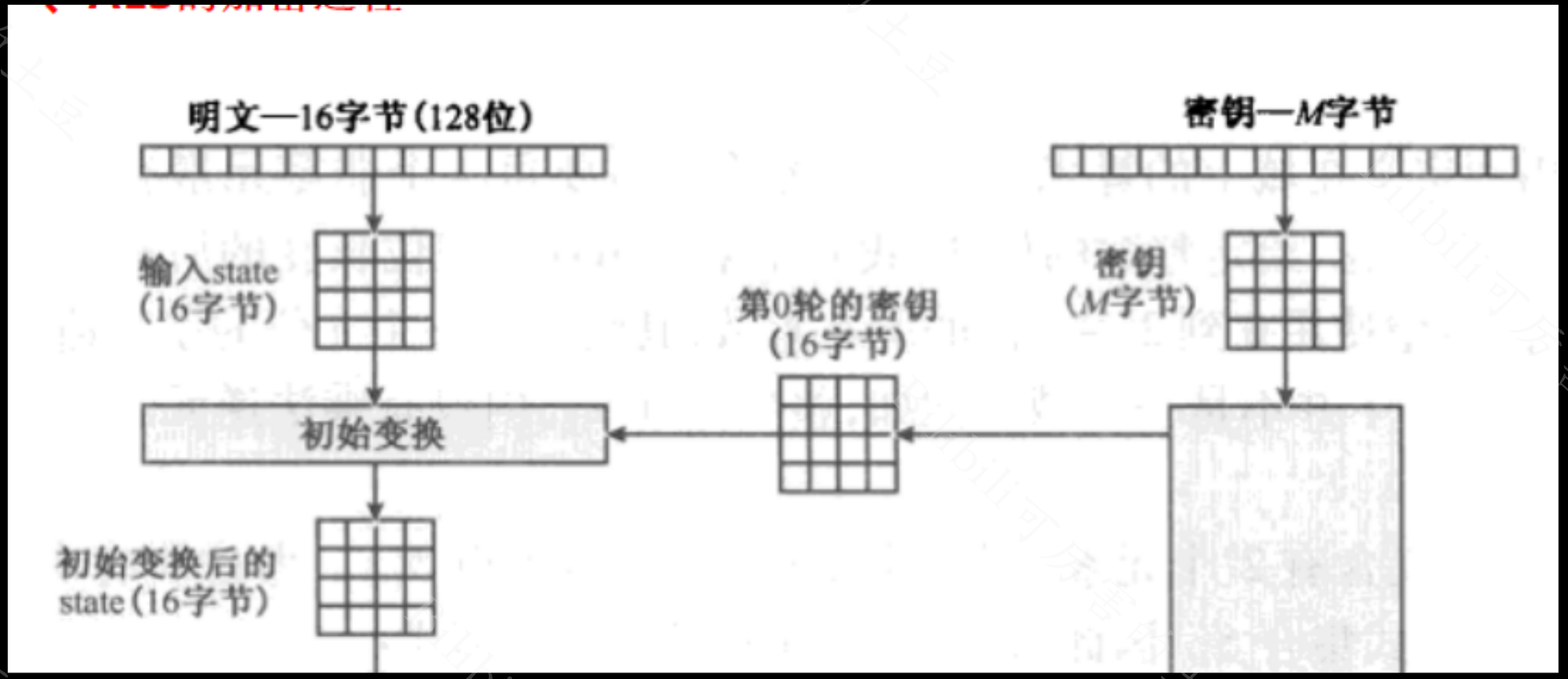
16字节数据的排列方式



AES加密过程

参考资料: [3]

初始变换(Initial round)



参考资料: [1]

初始变换(Initial round)

明文矩阵

p1	p5	p9	p13
p2	p6	p10	p14
p3	p7	p11	p15
p4	p8	p12	p16

子密钥矩阵

k1	k5	k9	k13
k2	k6	k10	k14
k3	k7	k11	k15
k4	k8	k12	k16

处理结果:

p1^k1	p5^k5	p9^k9	p13^k13
p2^k2	p6^k6	p10^k10	p14^k14
p3^k3	p7^k7	p11^k11	p15^k15
p4^k4	p8^k8	p12^k12	p16^k16

参考资料: [4]

字节代换(SubBytes)

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x 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	62	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

S-BOX

参考资料: [4]

字节代换(SubBytes)

d4	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

S-BOX

hex		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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	62	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

参考资料: [4]

字节代换(SubBytes)

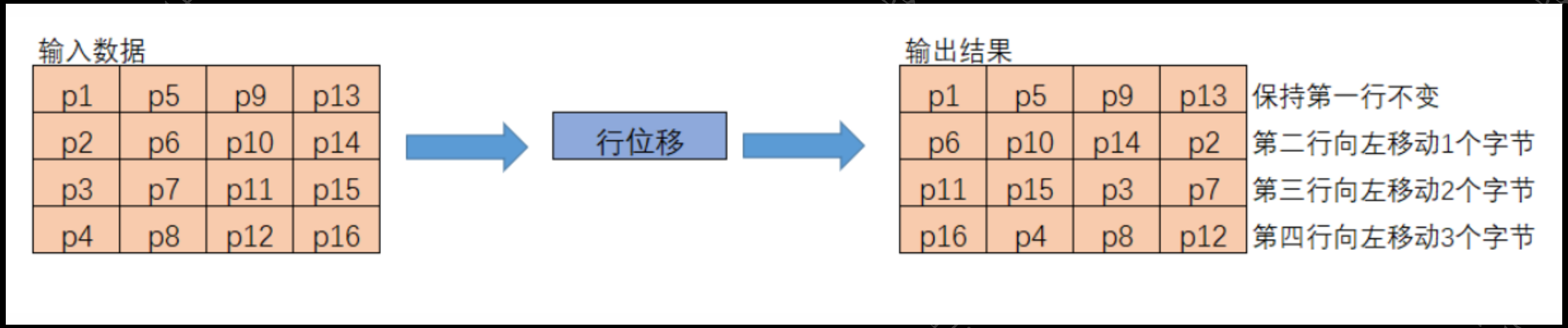
19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

SubBytes

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

参考资料: [1]

行移位(ShiftRows)



参考资料: [4]

行移位(ShiftRows)

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

ShiftRows

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

参考资料: [1]

列混合(MixColumn)

将输入的4*4的矩阵左乘一个给定的4*4矩阵

正矩阵

0x02	0x03	0x01	0x01
0x01	0x02	0x03	0x01
0x01	0x01	0x02	0x03
0x03	0x01	0x01	0x02

输入数据

p1	p5	p9	p13
p2	p6	p10	p14
p3	p7	p11	p15
p4	p8	p12	p16

参考资料: [4]

列混合(MixColumn)

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

ShiftRows

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

参考资料: [4]

轮密钥加(AddRoundKey)

04		a0		a4
66	⊕	fa	=	9c
81		fe		7f
e5		17		f2

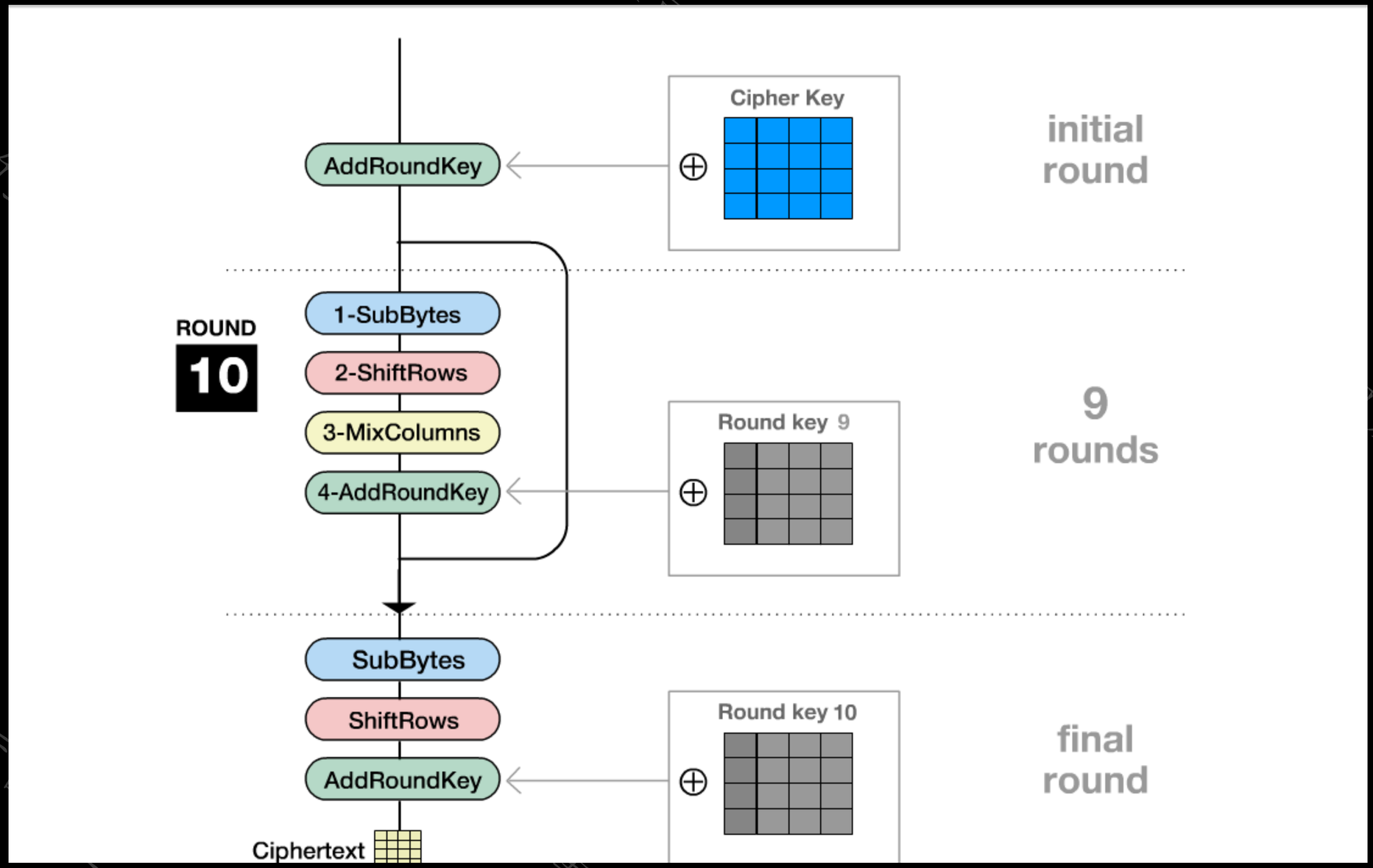
04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

AddROundKey

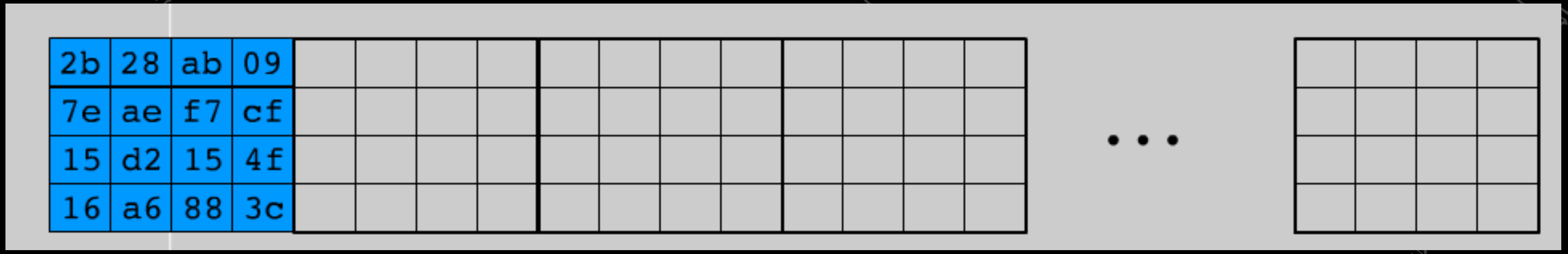
a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

参考资料: [4]


Cipher Key
AddRoundKey
initial round
ROUND
10
1-SubBytes
2-ShiftRows
3-MixColumns
4-AddRoundKey
Round key 9
9 rounds
SubBytes
ShiftRows
AddRoundKey
Round key 10
final round
Ciphertext

参考资料: [4]

密钥扩展



01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

参考资料: [2]、[4]

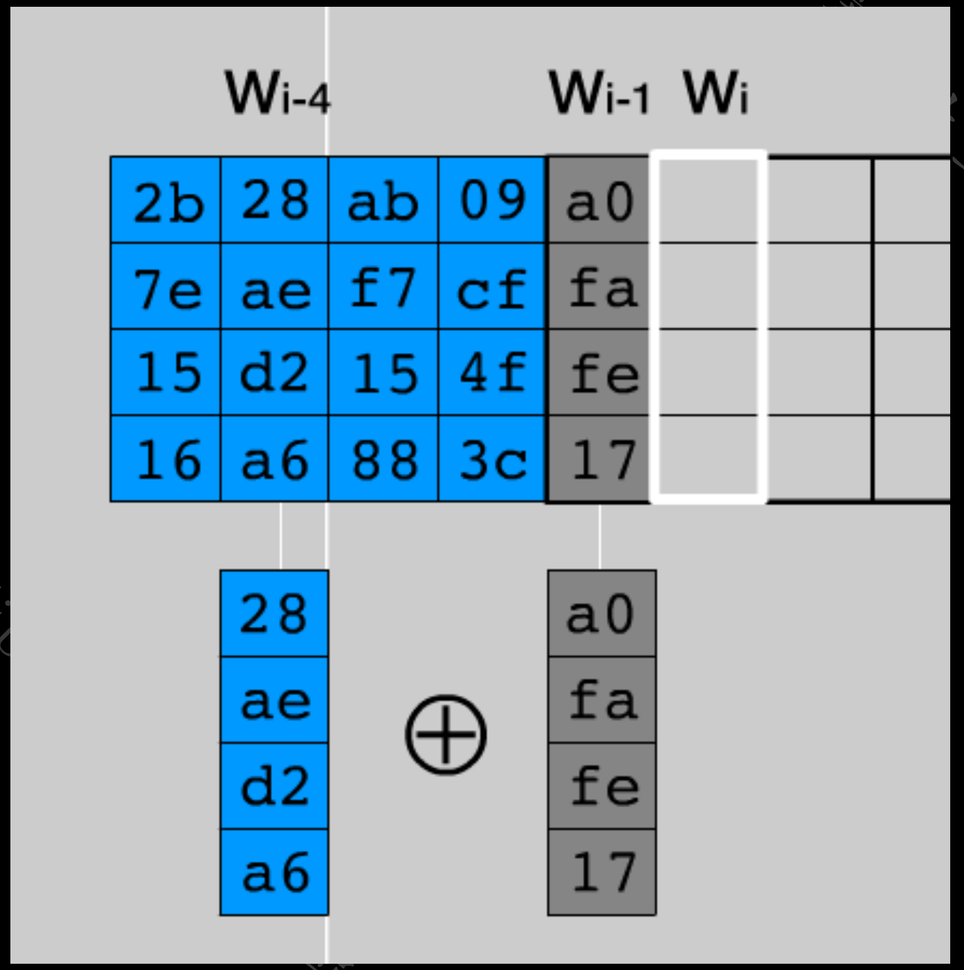
密钥扩展

1.如果i不是4的倍数，那么第i列由如下等式确定：

W[i]=W[i-4]⊕W[i-1]

2.如果i是4的倍数，那么第i列由如下等式确定：

W[i]=W[i-4]⊕T(W[i-1])

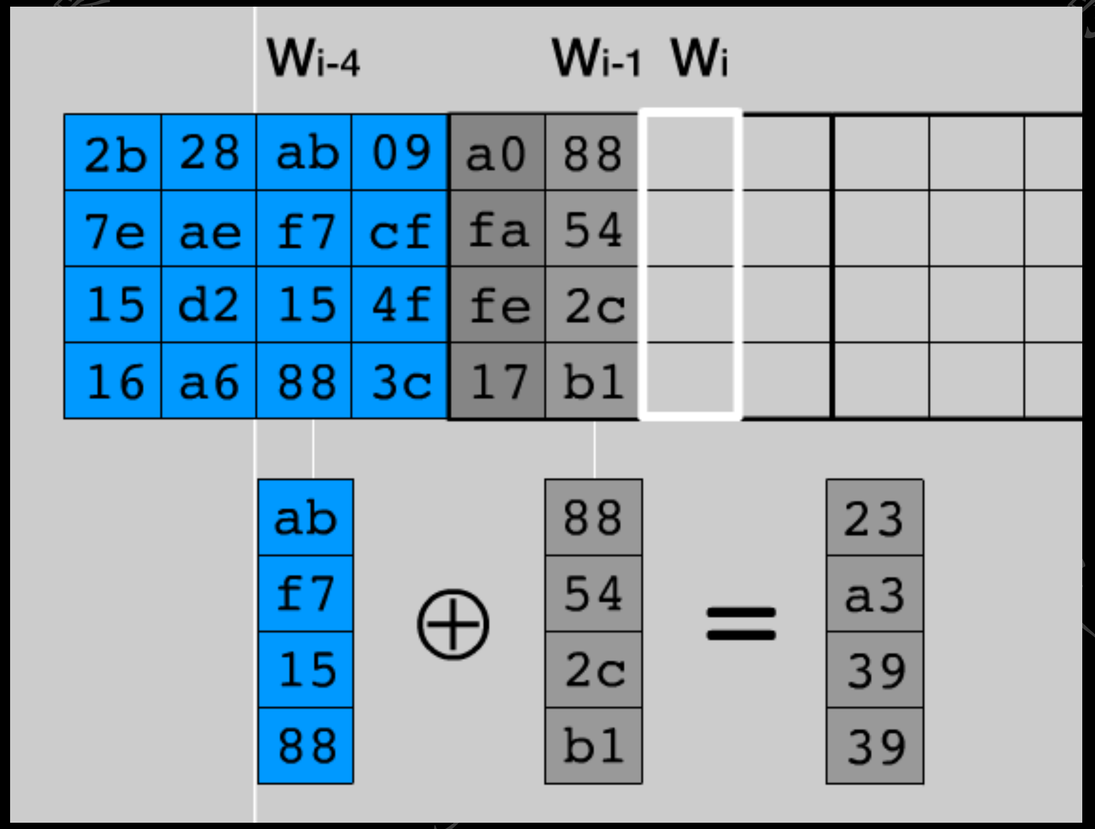


参考资料: [4]

密钥扩展（不是4的倍数）

$$W[i]=W[i-4]\oplus W[i-1]$$

2b	28	ab	09	a0	88					
7e	ae	f7	cf	fa	54					
15	d2	15	4f	fe	2c					
16	a6	88	3c	17	b1					



密钥扩展（4的倍数）

$$W[i]=W[i-4]\oplus T(W[i-1])$$

函数T由3部分组成：字循环、字节代换和轮常量异或。

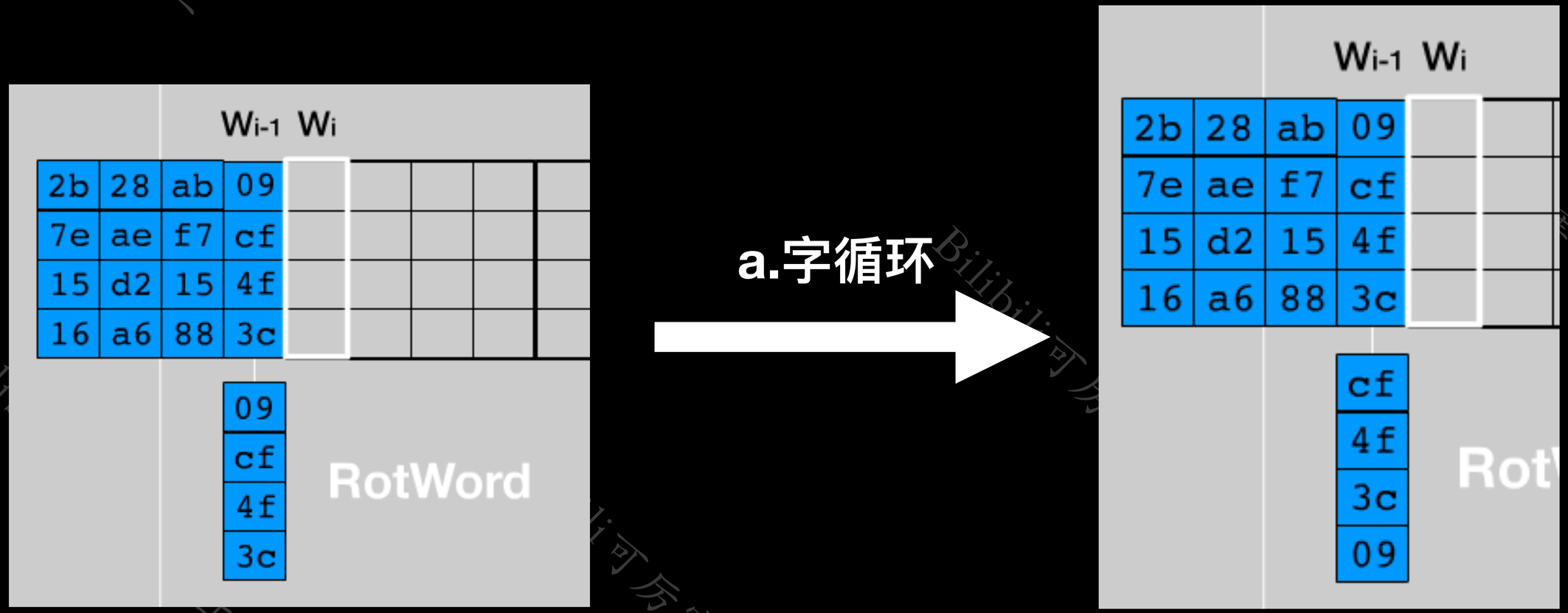
01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

参考资料: [4]

密钥扩展（4的倍数）

W[i]=W[i-4]⊕T(W[i-1])

a.字循环：将1个字中的4个字节循环左移1个字节。即将输入字[b0, b1, b2, b3]变换成[b1,b2,b3,b0]。

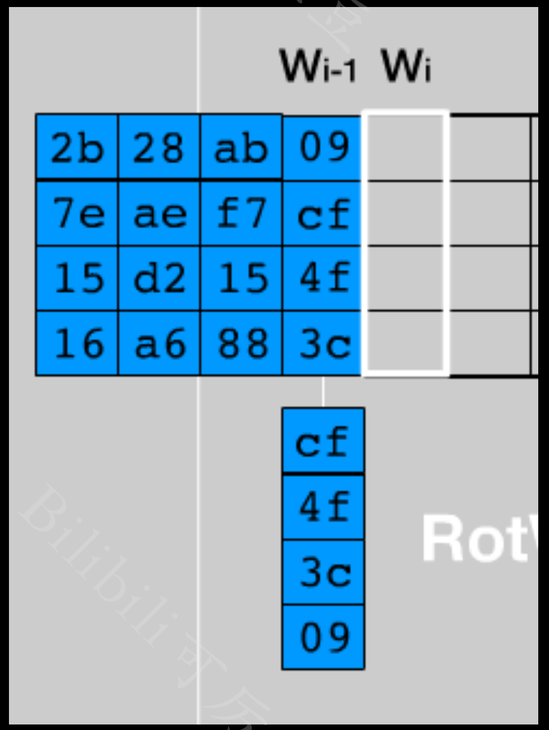


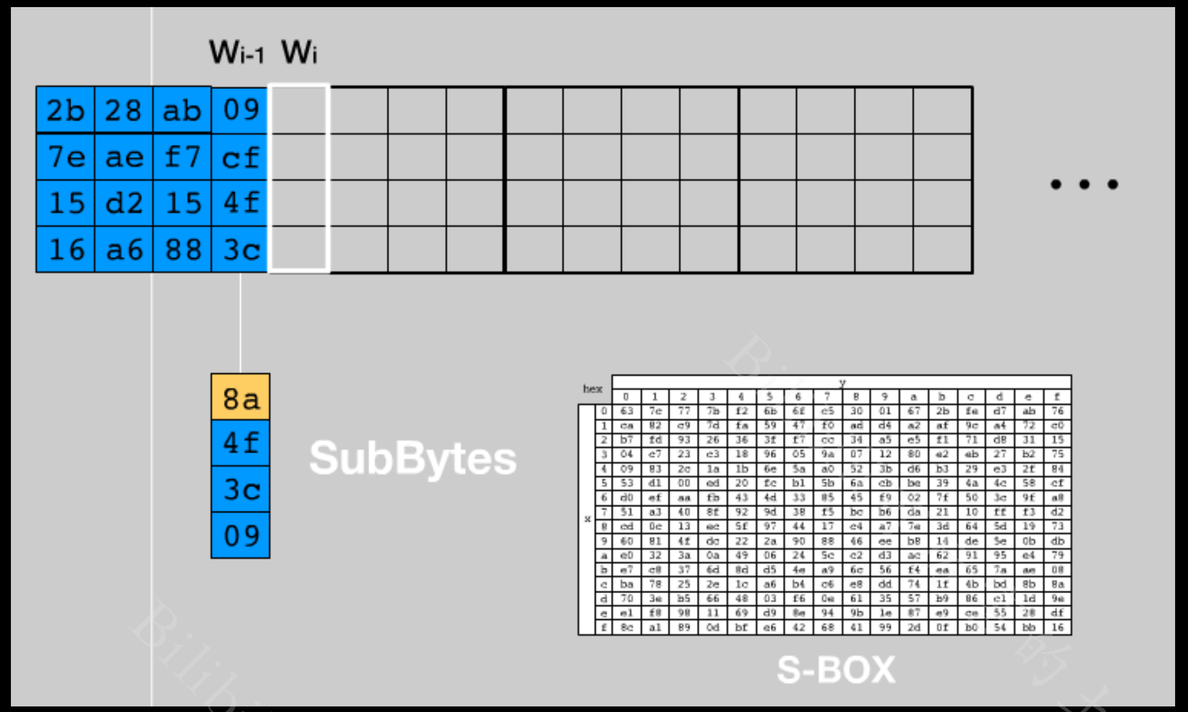
参考资料: [4]

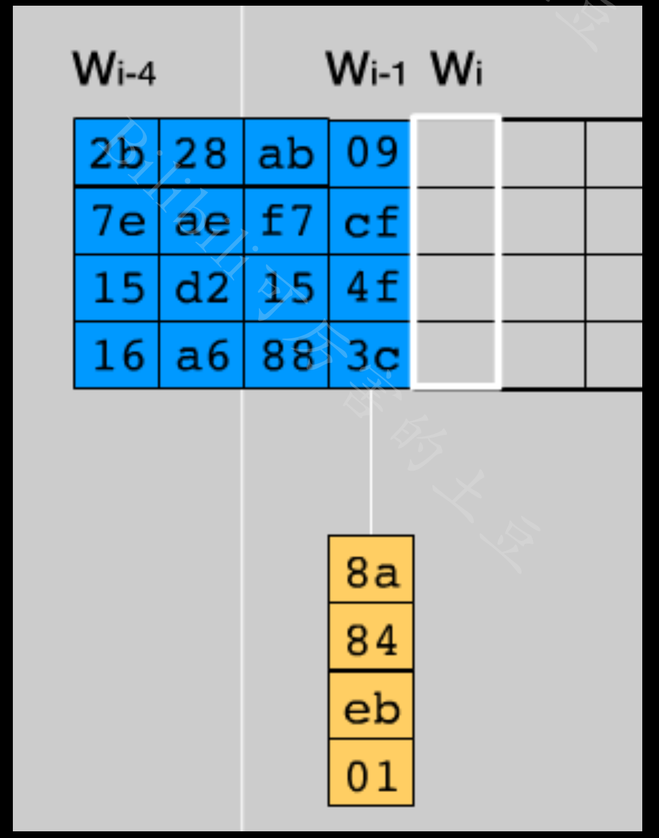
密钥扩展（4的倍数）

W[i]=W[i-4]⊕T(W[i-1])

b.字节代换：对字循环的结果使用S盒进行字节代换。







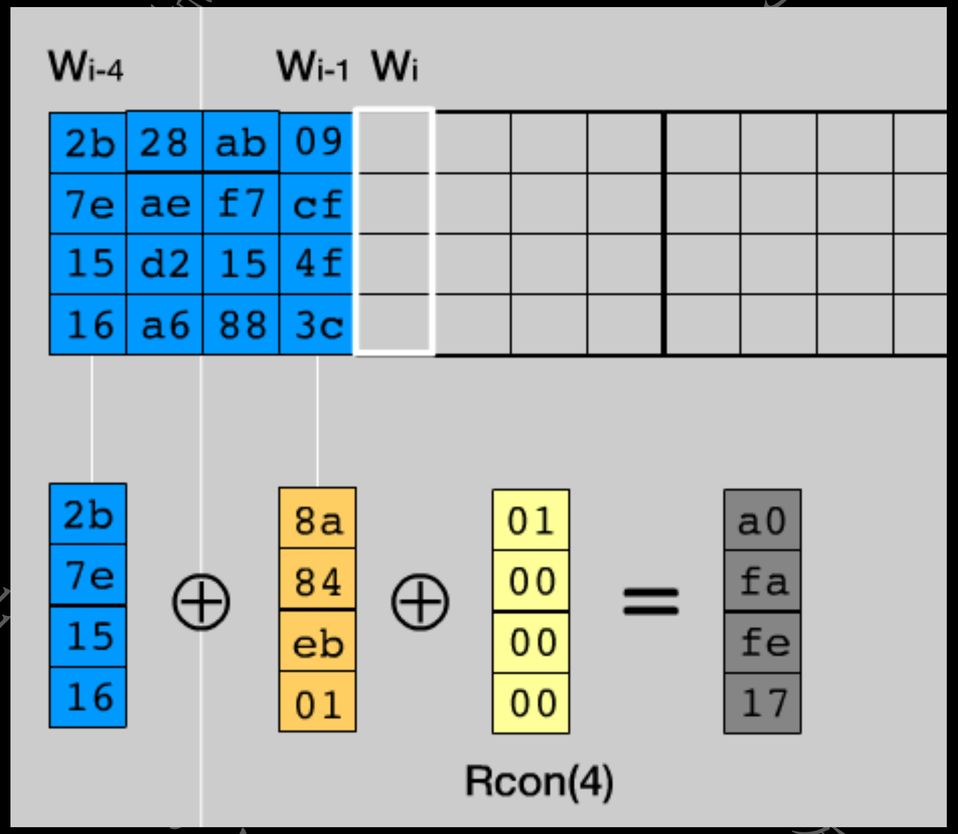
参考资料: [4]

密钥扩展（4的倍数）

$$W[i]=W[i-4]\oplus T(W[i-1])$$

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

c.轮常量异或：将前两步的结果同轮常量Rcon[j]进行异或，其中j表示轮数。

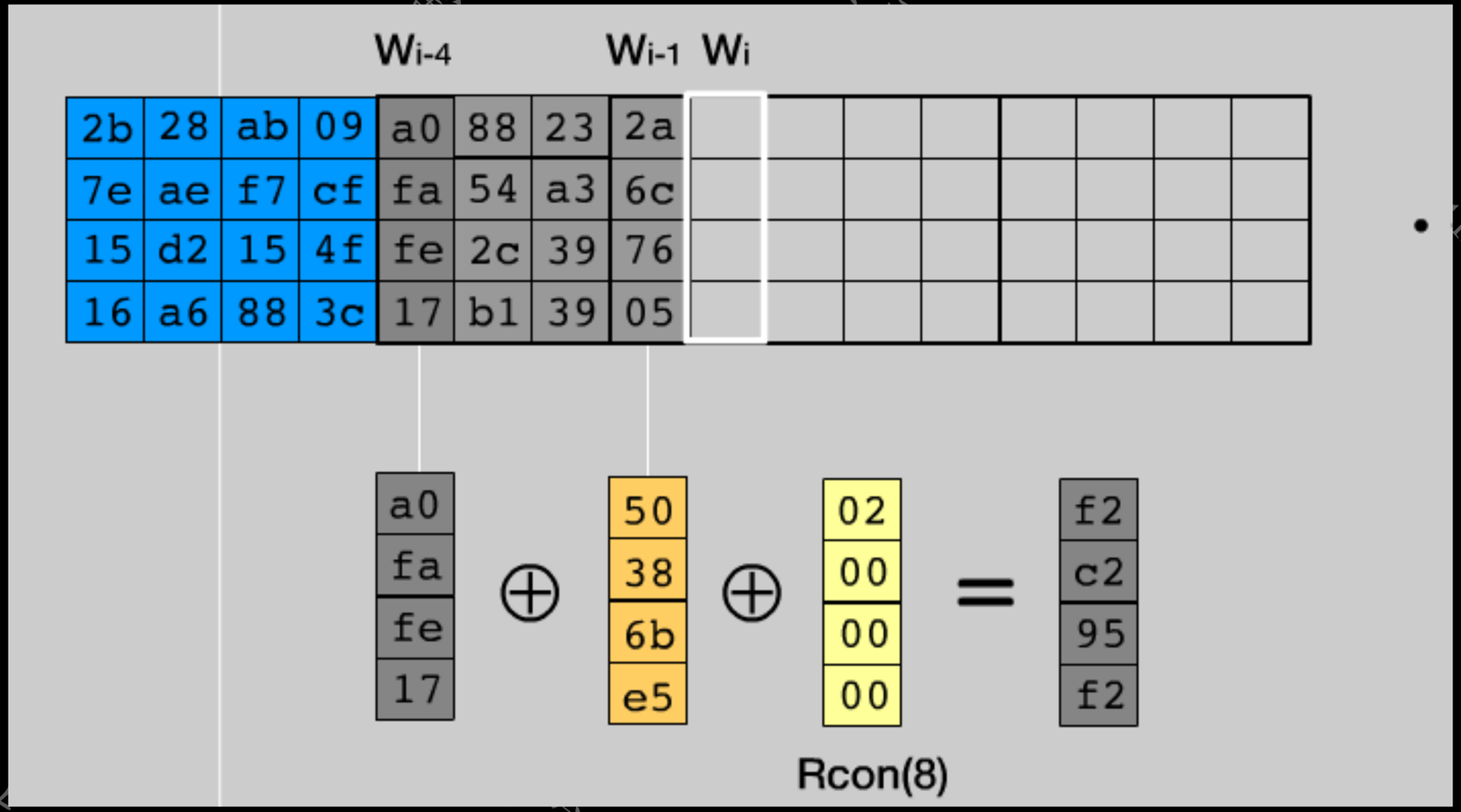


2b	28	ab	09	a0		
7e	ae	f7	cf	fa		
15	d2	15	4f	fe		
16	a6	88	3c	17		

参考资料: [4]

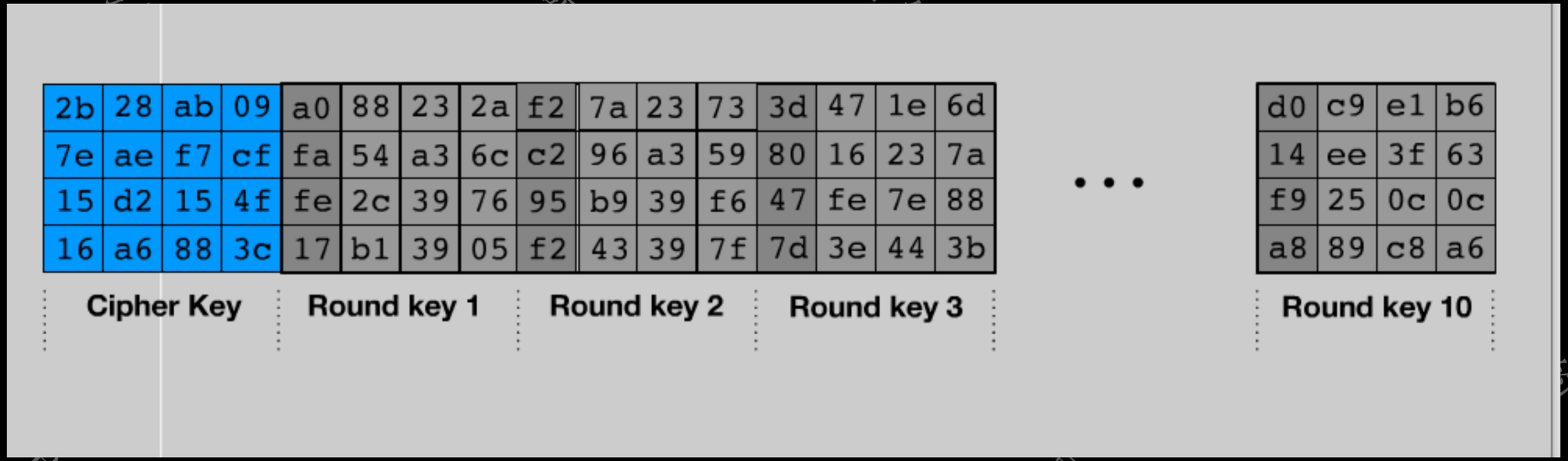
密钥扩展（4的倍数）

$$W[i]=W[i-4]\oplus T(W[i-1])$$

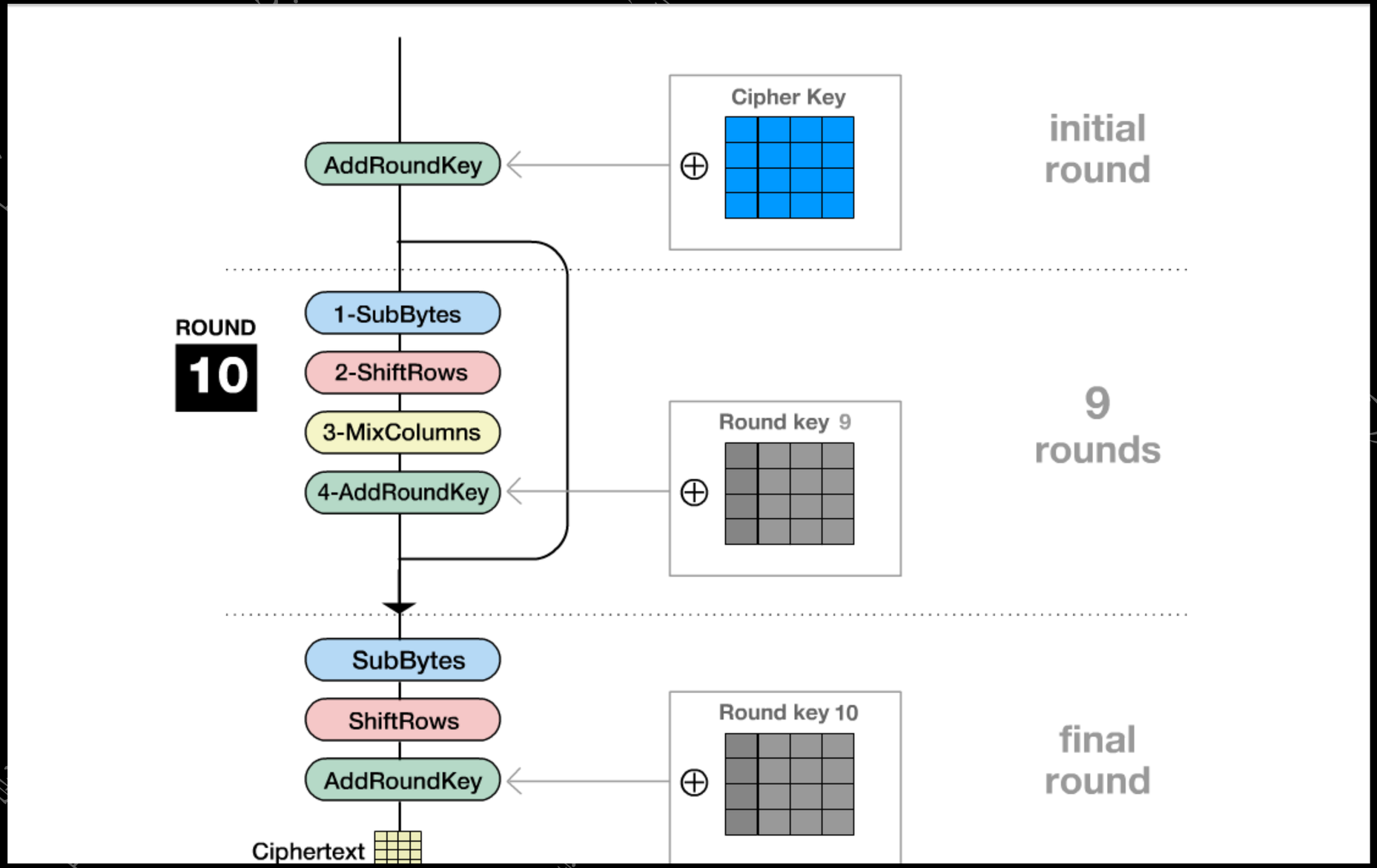


参考资料: [4]

密钥扩展



参考资料: [4]


Cipher Key
AddRoundKey
initial round
ROUND
10
1-SubBytes
2-ShiftRows
3-MixColumns
4-AddRoundKey
Round key 9
9 rounds
SubBytes
ShiftRows
AddRoundKey
Round key 10
final round
Ciphertext

参考资料: [2]

列混合(MixColumn)

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

$$s'_{0,j} = (2 * s_{0,j}) \oplus (3 * s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$
$$s'_{1,j} = s_{0,j} \oplus (2 * s_{1,j}) \oplus (3 * s_{2,j}) \oplus s_{3,j}$$
$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 * s_{2,j}) \oplus (3 * s_{3,j})$$
$$s'_{3,j} = (3 * s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 * s_{3,j})$$

参考资料: [2]

列混合(MixColumn)

$$(00000010) * (a_7a_6a_5a_4a_3a_2a_1a_0) = \begin{cases} (a_6a_5a_4a_3a_2a_1a_00), a_7 = 0 \\ (a_6a_5a_4a_3a_2a_1a_00) \oplus (00011011), a_7 = 1 \end{cases}$$

$$(00000100) * (a_7a_6a_5a_4a_3a_2a_1a_0) = (00000010) * (00000010) * (a_7a_6a_5a_4a_3a_2a_1a_0)$$

$$\begin{aligned}(00000011) * (a_7a_6a_5a_4a_3a_2a_1a_0) &= [(00000010) \oplus (00000001)] * (a_7a_6a_5a_4a_3a_2a_1a_0) \\ &= [(00000010) * (a_7a_6a_5a_4a_3a_2a_1a_0)] \oplus (a_7a_6a_5a_4a_3a_2a_1a_0)\end{aligned}$$

参考资料

[1] QiuJYu. 密码学基础：AES加密算法[DB/OL].https://bbs.pediy.com/thread-253884.htm#%E7%AC%AC%E4%B8%80%E8%8A%82%EF%BC%9Aaes%E7%AE%97%E6%B3%95%E7%AE%80%E4%BB%8B. 看雪论坛. 2019-08-15 .

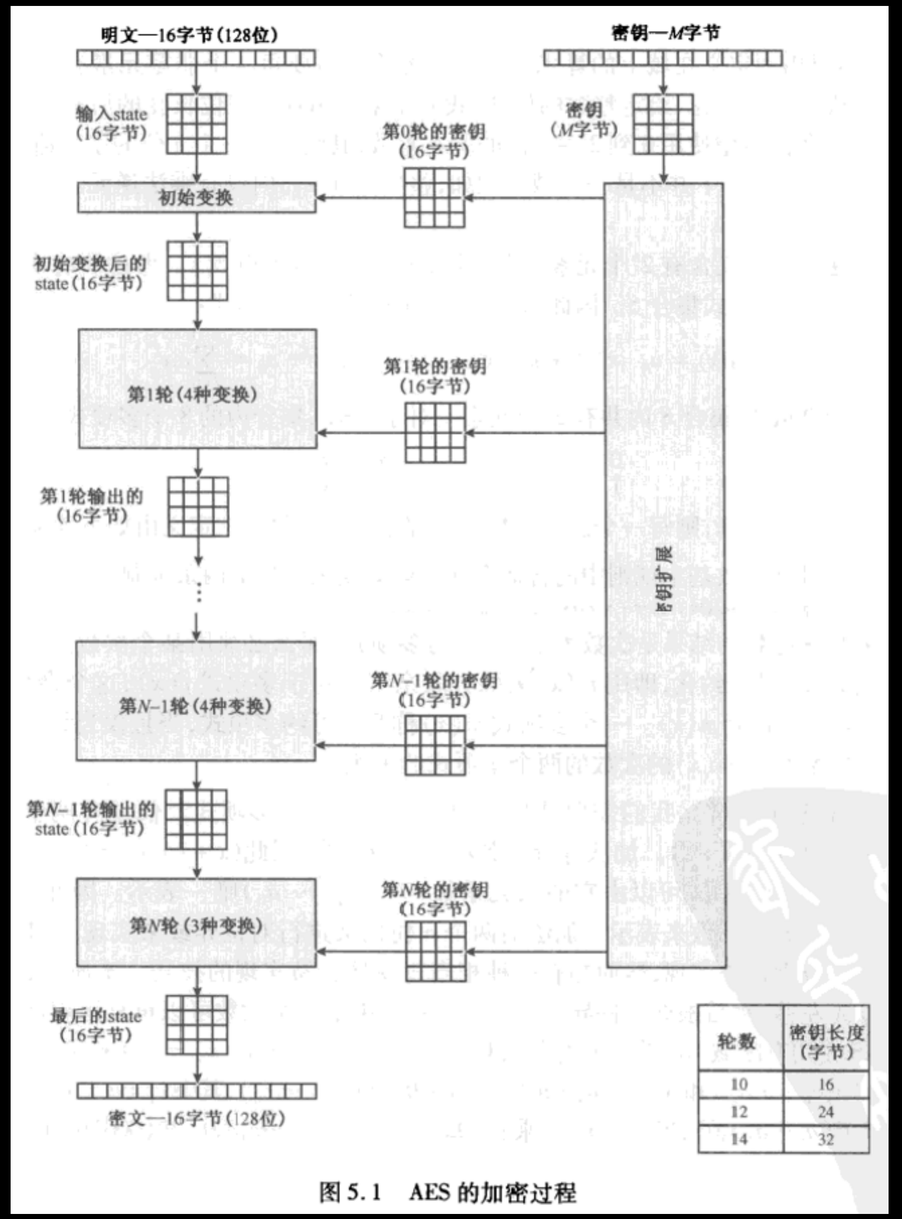
[2] TimeShatter. AES加密算法的详细介绍与实现[DB/OL].https://zhuanlan.zhihu.com/p/42629724. CSDN. 2017-02-19 .

[3] block2016. AES加密[DB/OL]. https://www.cnblogs.com/block2016/p/5596676.html. 博客园. 2016-06-18.

[4]Enrique Zabala.Rijndael Cipher[DB/OL].http://coolshell.cn/wp-content/uploads/2010/10/rijndael_ingles2004.swf.日期不详.

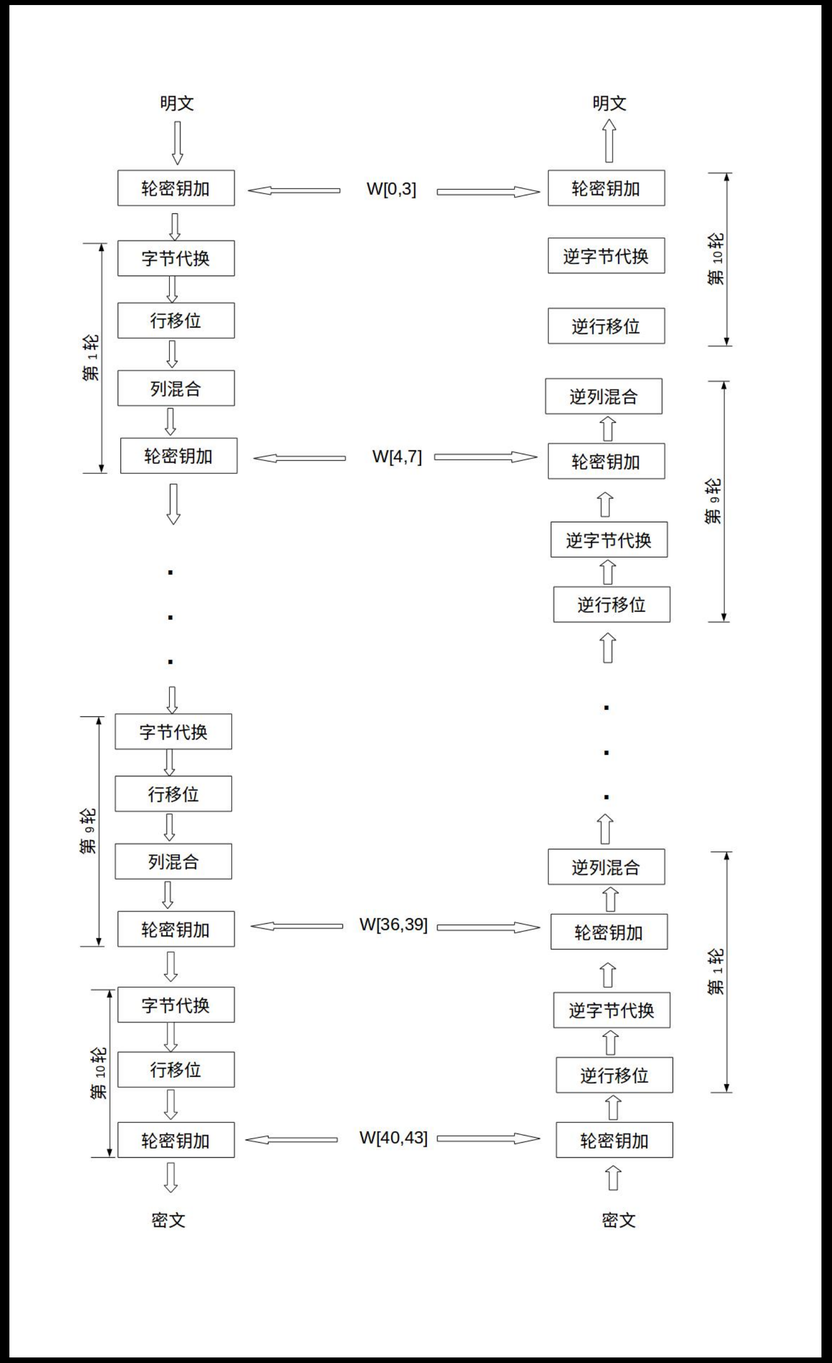
“
感谢观看
祝你每天吃饱
每晚睡好
身体健康
学业有成
工作顺利
”

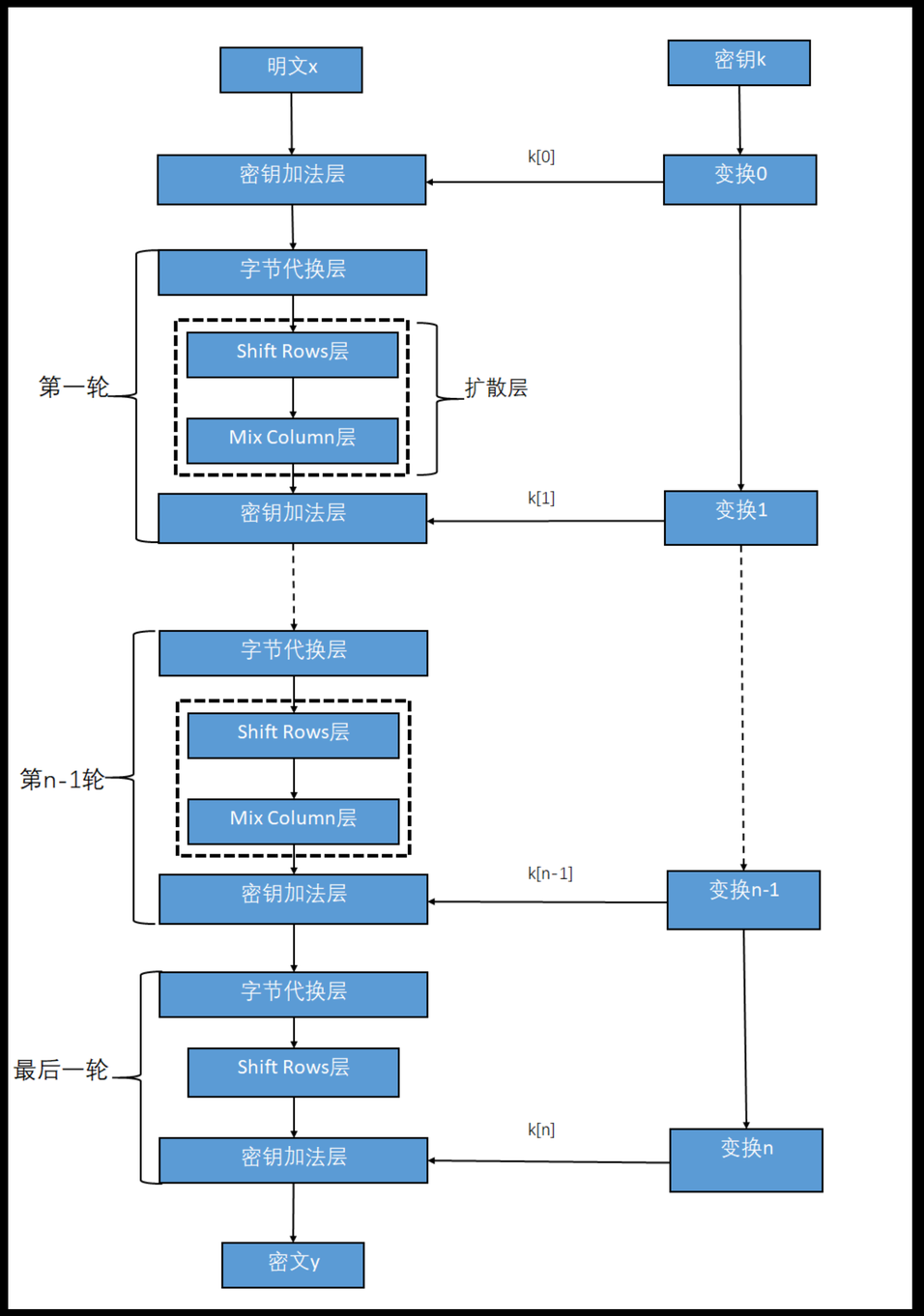
—可厉害的土豆



轮数	密钥长度(字节)
10	16
12	24
14	32

图 5.1　AES 的加密过程


明文
明文
轮密钥加
W[0,3]
轮密钥加
逆字节代换
逆行移位
第10轮
字节代换
行移位
列混合
第1轮
逆列混合
轮密钥加
W[4,7]
轮密钥加
逆字节代换
逆行移位
第9轮
字节代换
行移位
列混合
第9轮
逆列混合
轮密钥加
W[36,39]
轮密钥加
逆字节代换
逆行移位
第1轮
字节代换
行移位
第10轮
轮密钥加
W[40,43]
轮密钥加
密文
密文


明文x
密钥k
密钥加法层
k[0]
变换0
字节代换层
Shift Rows层
Mix Column层
扩散层
第一轮
密钥加法层
k[1]
变换1
字节代换层
Shift Rows层
Mix Column层
第n-1轮
密钥加法层
k[n-1]
变换n-1
字节代换层
Shift Rows层
最后一轮
密钥加法层
k[n]
变换n
密文y