AES

Advanced Encryption Standard

Входные данные

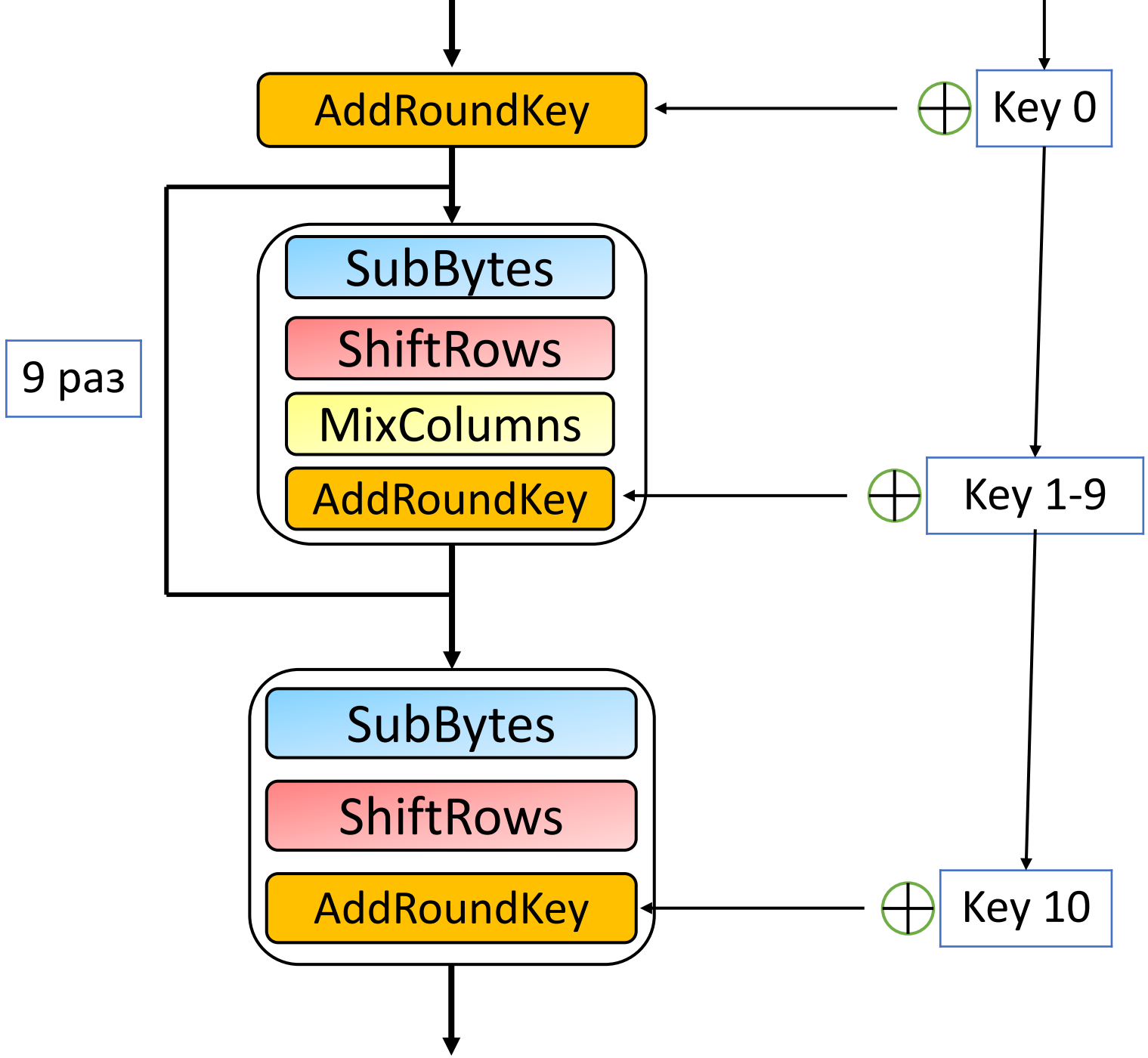
Открытое сообщение

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

Ключ

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

32 = 00110010



Алгоритм шифрования

SubBytes

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

x y

19 → 1 9 → d4

hex	y															
	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	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

x

SubBytes

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

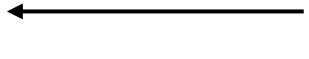
hex	y															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	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	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

x

ShiftRows

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

Циклический сдвиг на 1 байт



Циклический сдвиг на 2 байта

Циклический сдвиг на 3 байта

MixColumns

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

$$\begin{bmatrix} d4 \\ 27 \\ 11 \\ ae \end{bmatrix} \bullet \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

MixColumns

$$\begin{bmatrix} S'_{0c} \\ S'_{1c} \\ S'_{2c} \\ S'_{3c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \bullet \begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix}$$

$$S'_{0c} = (2 \bullet S_{0c}) \oplus (3 \bullet S_{1c}) \oplus S_{2c} \oplus S_{3c};$$
$$S'_{1c} = S_{0c} \oplus (2 \bullet S_{1c}) \oplus (3 \bullet S_{2c}) \oplus S_{3c};$$
$$S'_{2c} = S_{0c} \oplus S_{1c} \oplus (2 \bullet S_{2c}) \oplus (3 \bullet S_{3c});$$
$$S'_{3c} = (3 \bullet S_{0c}) \oplus S_{1c} \oplus S_{2c} \oplus (2 \bullet S_{3c}).$$

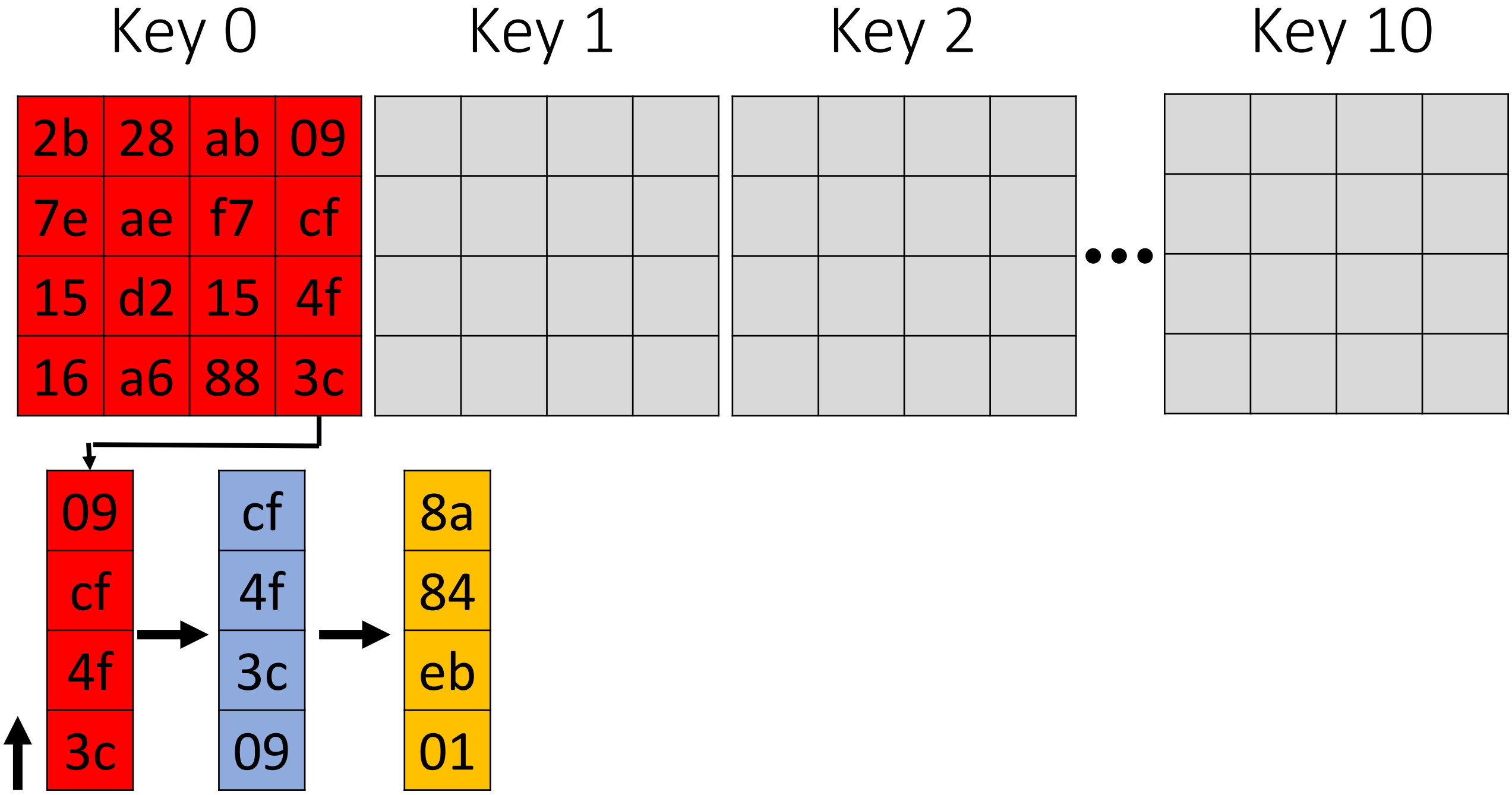
AddRoundKey

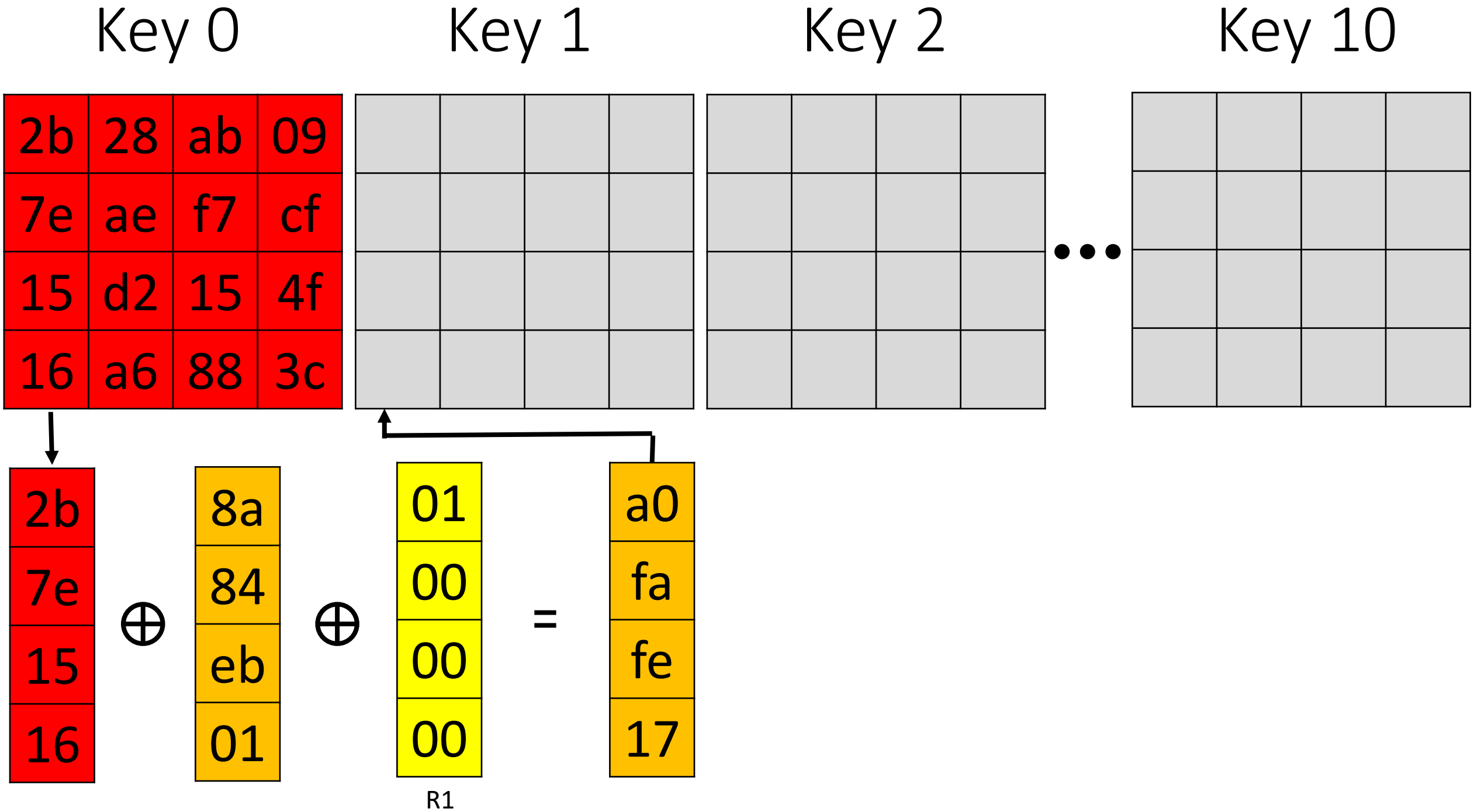
04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

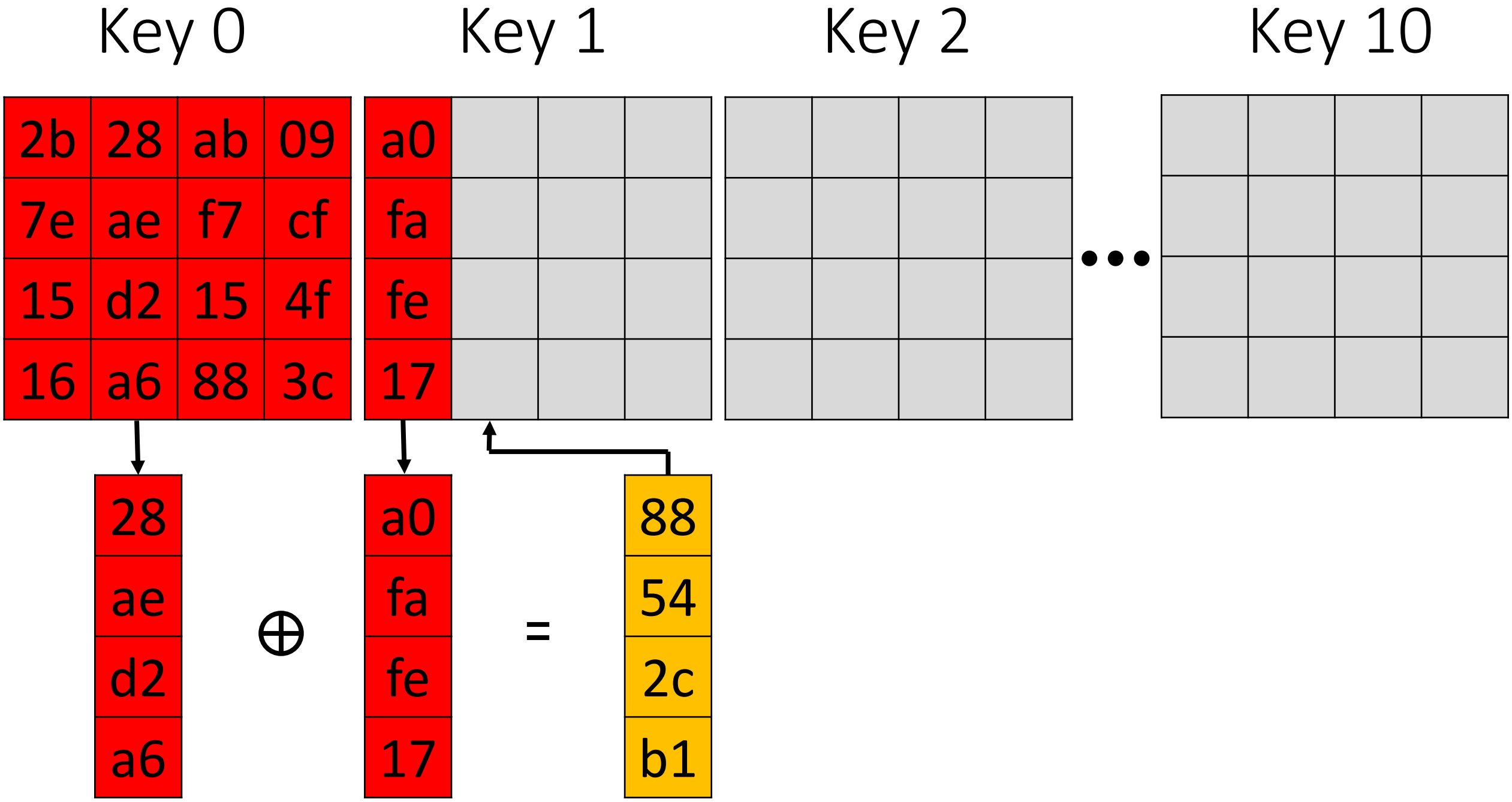
04	⊕	a0	=	a4
66		fa		9c
81		fe		7f
e5		17		f2

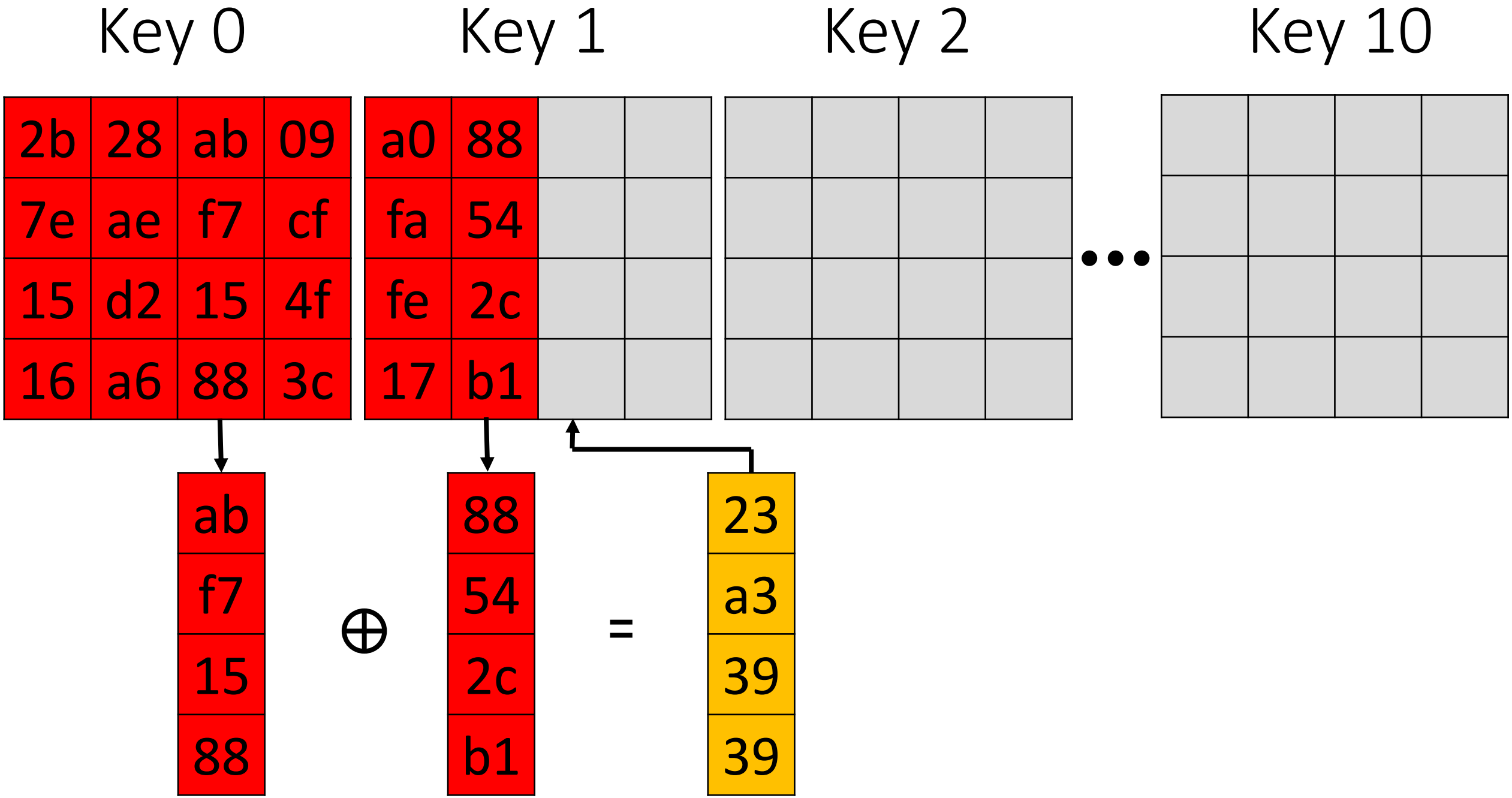
a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

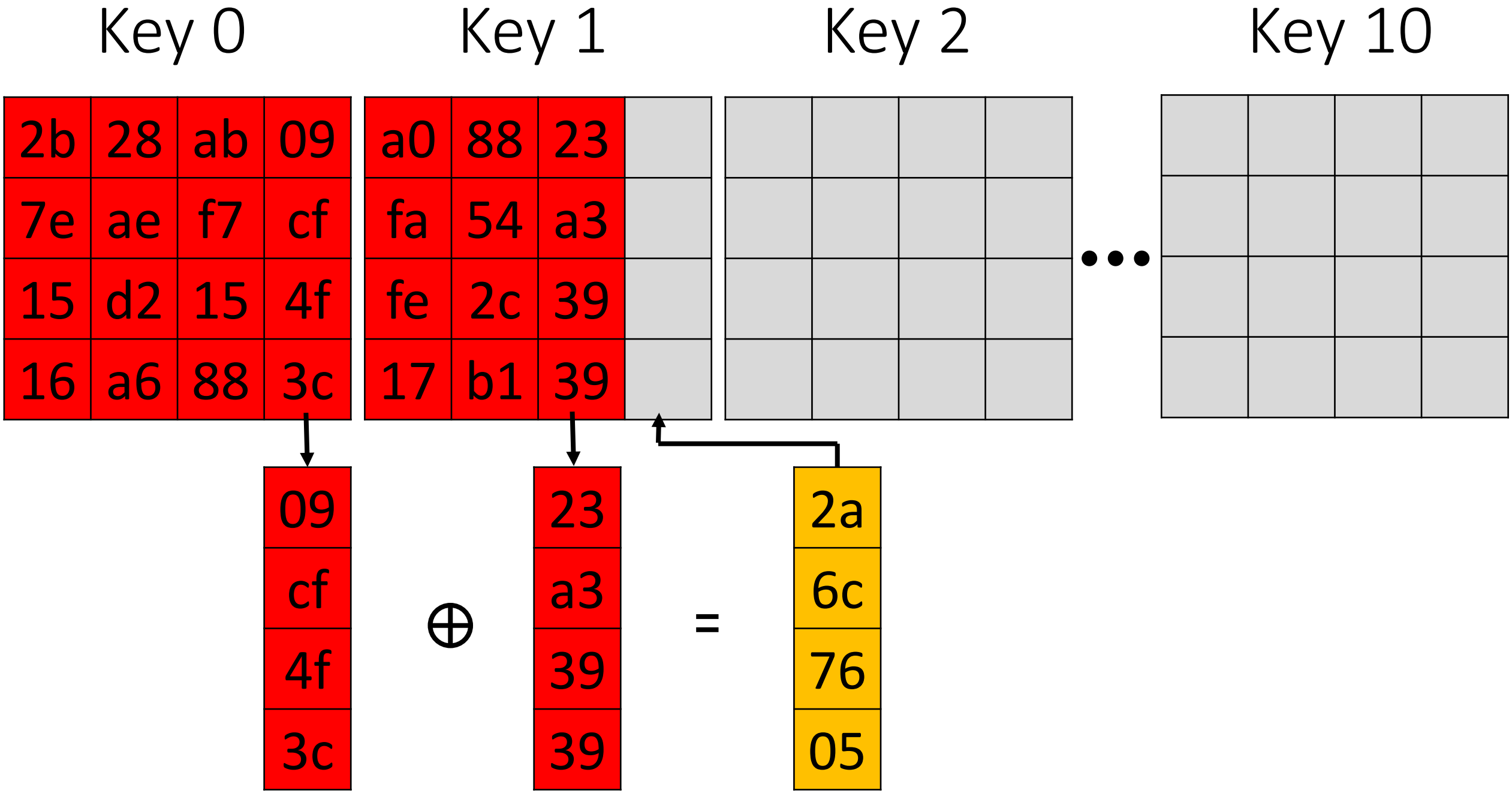
Key

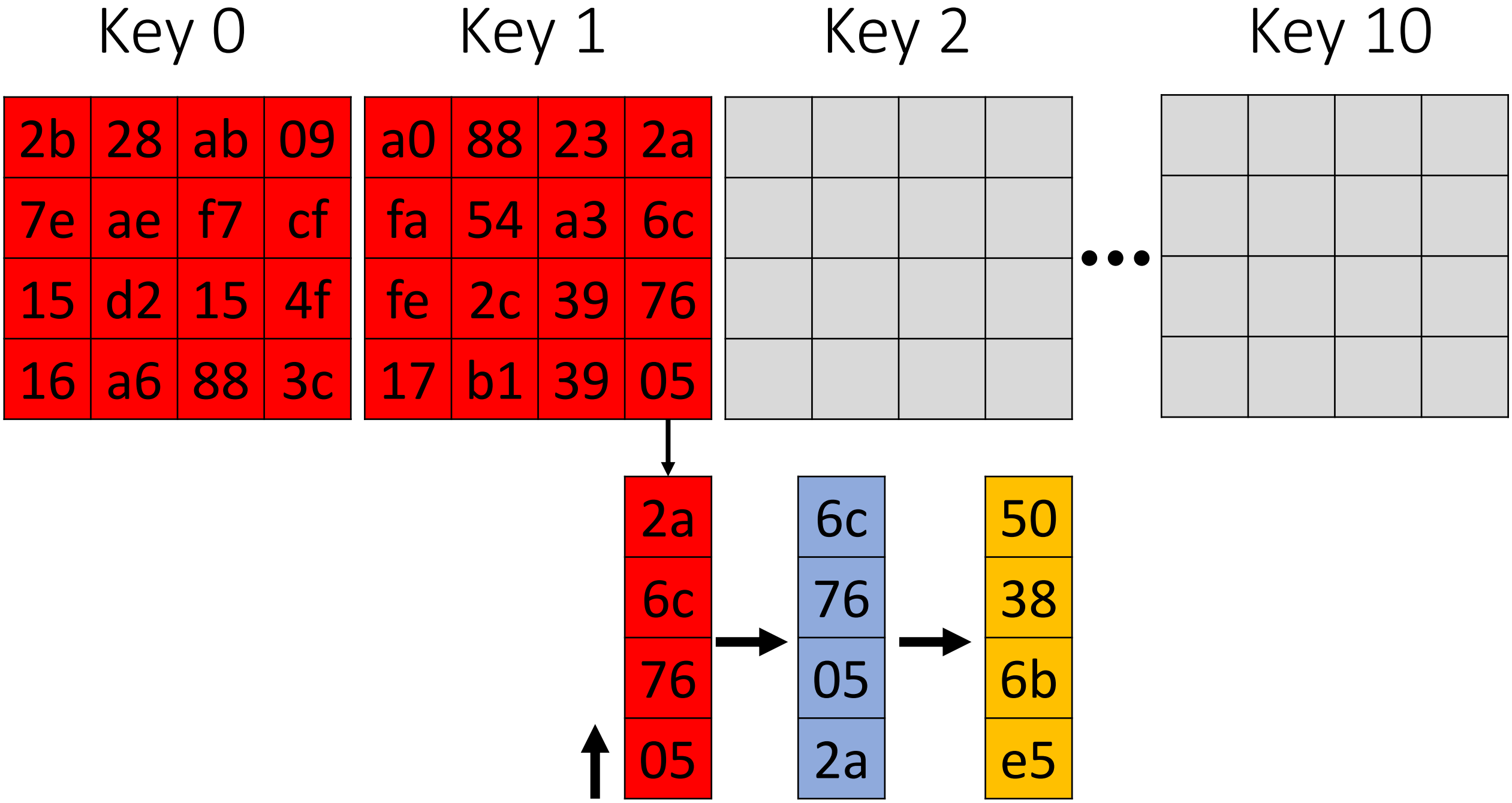

Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
09 cf 4f 3c
cf 4f 3c 09
8a 84 eb 01

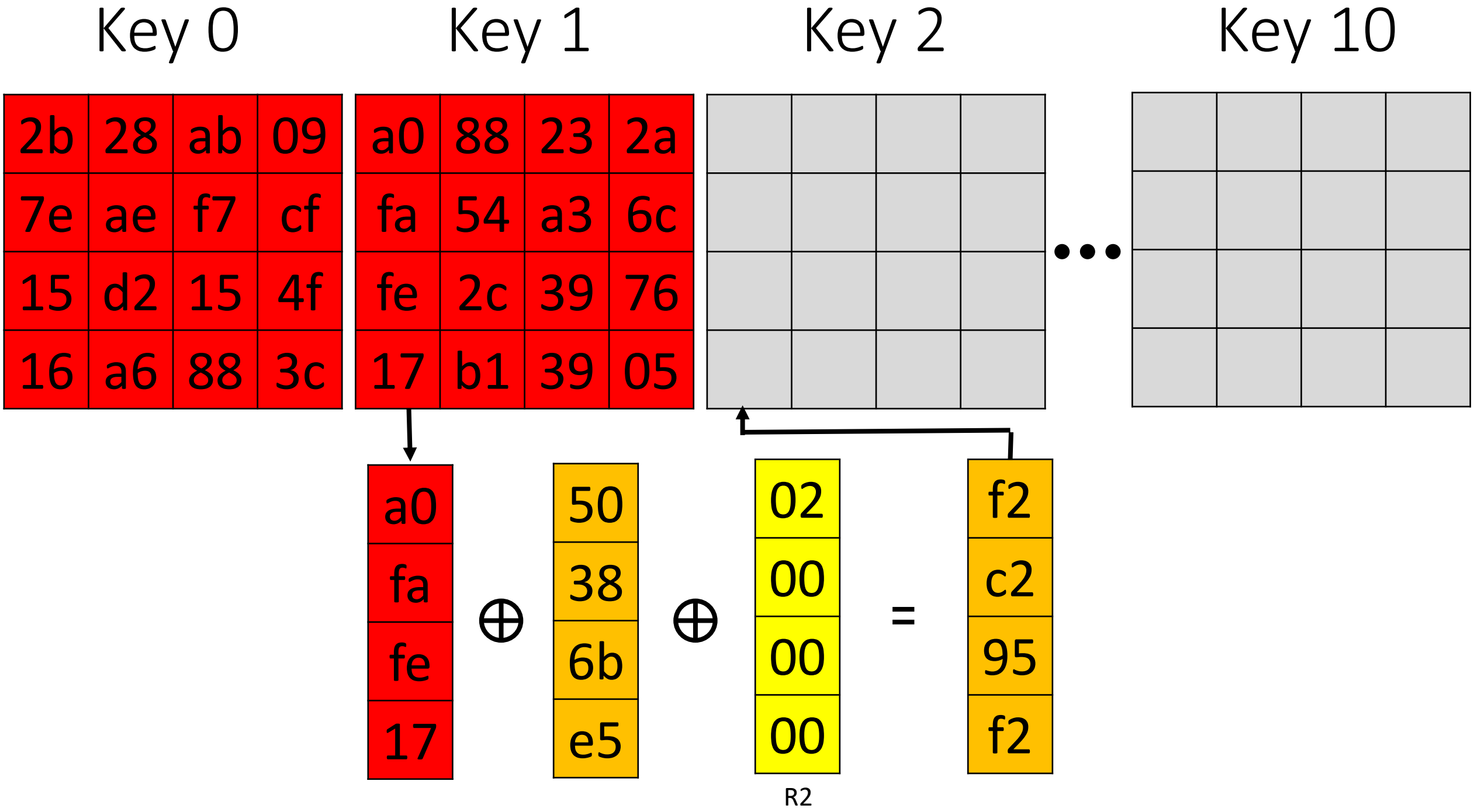

Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
2b
7e
15
16
⊕
8a
84
eb
01
⊕
01
00
00
00
=
a0
fa
fe
17
R1

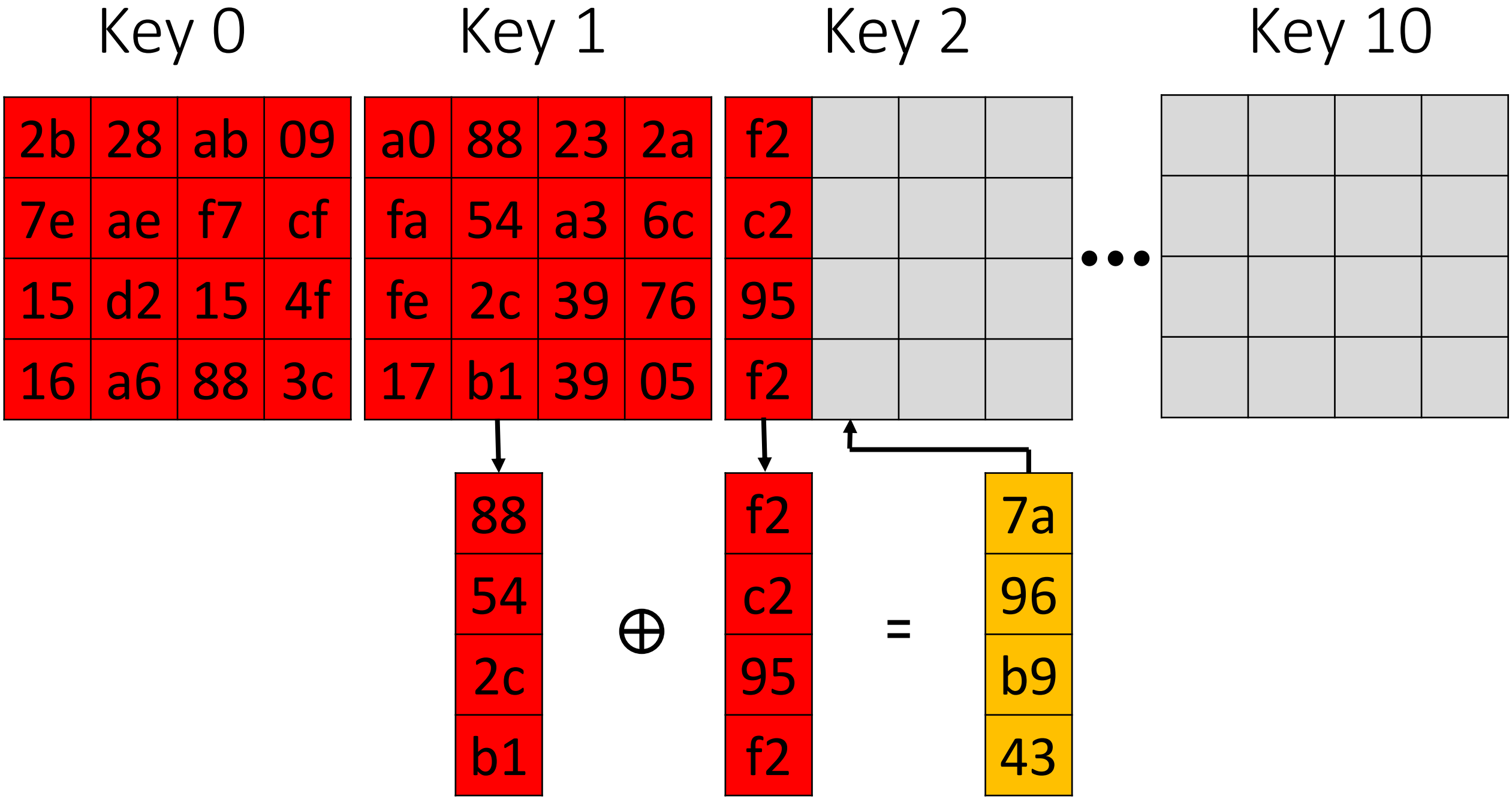

Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0
fa
fe
17
28
ae
d2
a6
⊕
a0
fa
fe
17
=
88
54
2c
b1

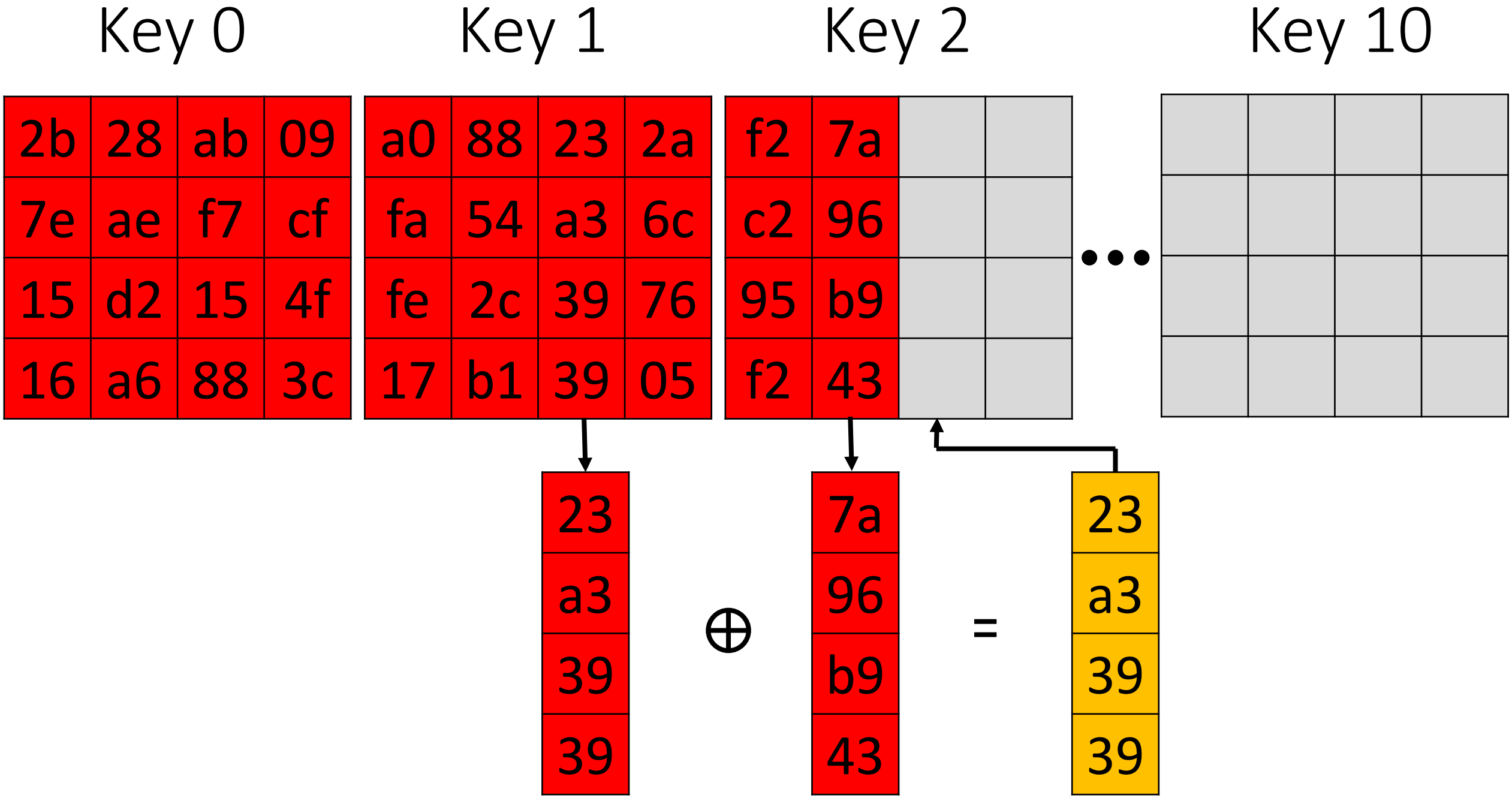

Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88
fa 54
fe 2c
17 b1
ab
f7
15
88
⊕
88
54
2c
b1
=
23
a3
39
39


Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88 23
fa 54 a3
fe 2c 39
17 b1 39
09
cf
4f
3c
⊕
23
a3
39
39
=
2a
6c
76
05


Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88 23 2a
fa 54 a3 6c
fe 2c 39 76
17 b1 39 05
2a
6c
76
05
6c
76
05
2a
50
38
6b
e5


Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88 23 2a
fa 54 a3 6c
fe 2c 39 76
17 b1 39 05
a0
fa
fe
17
⊕
50
38
6b
e5
⊕
02
00
00
00
=
f2
c2
95
f2
R2


Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88 23 2a
fa 54 a3 6c
fe 2c 39 76
17 b1 39 05
f2
c2
95
f2
88
54
2c
b1
⊕
f2
c2
95
f2
=
7a
96
b9
43


Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88 23 2a
fa 54 a3 6c
fe 2c 39 76
17 b1 39 05
f2 7a
c2 96
95 b9
f2 43
23
a3
39
39
⊕
7a
96
b9
43
=
23
a3
39
39

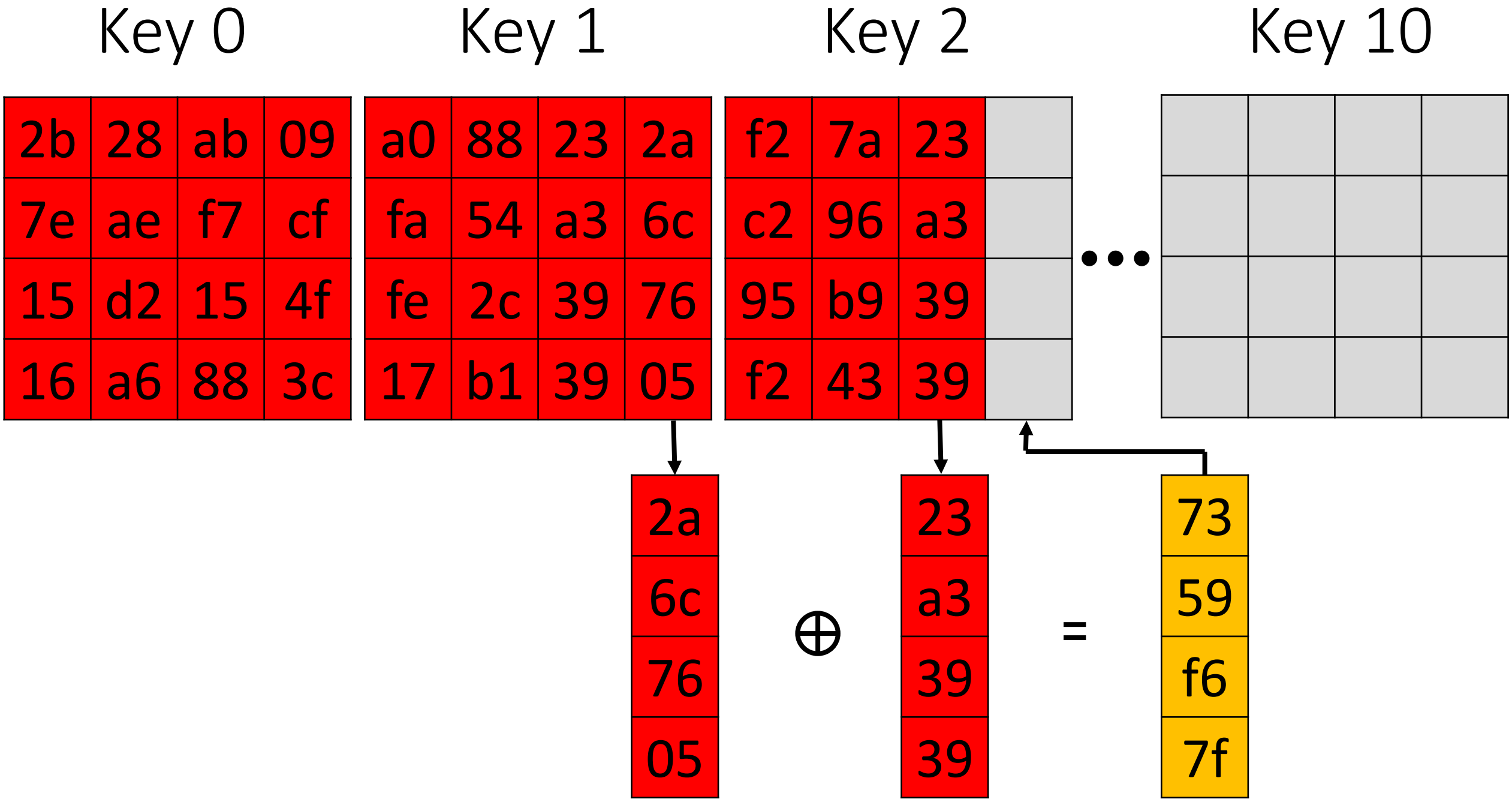

Key 0
Key 1
Key 2
Key 10
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
a0 88 23 2a
fa 54 a3 6c
fe 2c 39 76
17 b1 39 05
f2 7a 23
c2 96 a3
95 b9 39
f2 43 39
2a
6c
76
05
⊕
23
a3
39
39
=
73
59
f6
7f

ТАБЛИЦА ЗАМЕНЫ БАЙТ S-BOX АЛГОРИТМА AES

	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	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

Rcon

R1	R2	R#	R4	R5	R6	R7	R8	R9	R10
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