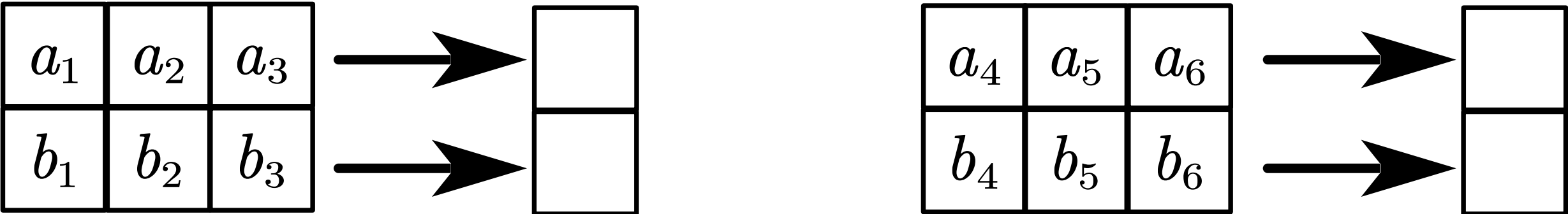
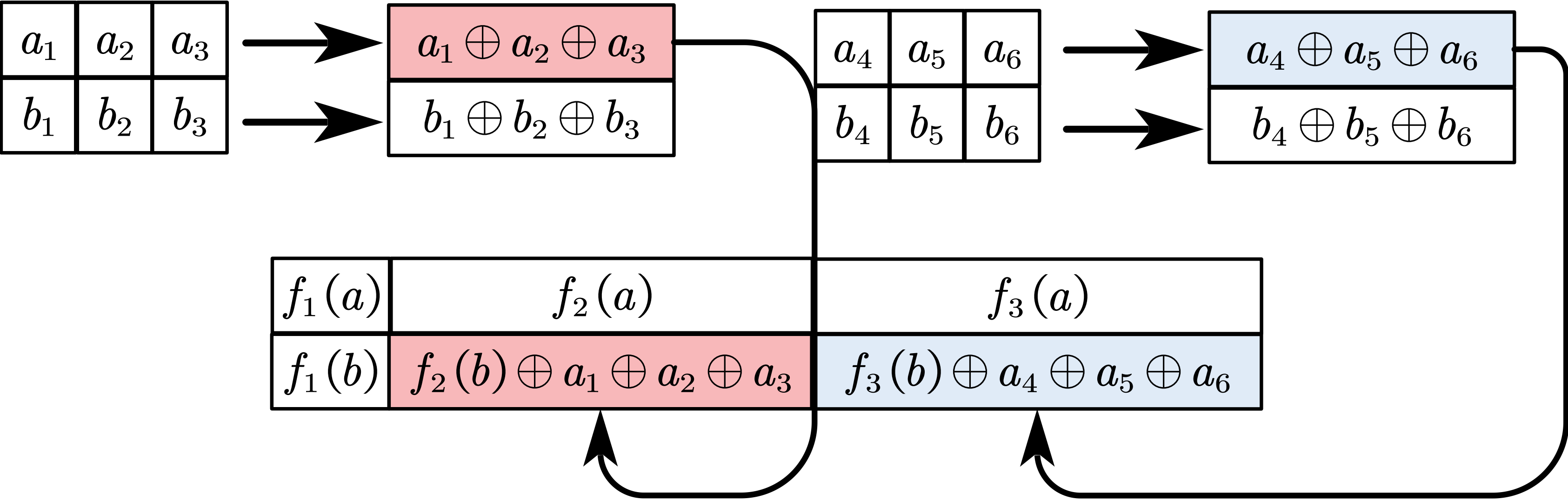


| | | | | | | | | |
|-------|-------|-------|-------|-------|-------|----------|---|---|
| a_1 | a_2 | a_3 | a_4 | a_5 | a_6 | $f_1(a)$ | $f_2(a)$ | $f_3(a)$ |
| b_1 | b_2 | b_3 | b_4 | b_5 | b_6 | $f_1(b)$ | $f_2(b) \oplus a_1 \oplus a_2 \oplus a_3$ | $f_3(b) \oplus a_4 \oplus a_5 \oplus a_6$ |



| | | |
|----------|---|---|
| $f_1(a)$ | $f_2(a)$ | $f_3(a)$ |
| $f_1(b)$ | $f_2(b) \oplus a_1 \oplus a_2 \oplus a_3$ | $f_3(b) \oplus a_4 \oplus a_5 \oplus a_6$ |



| | | | | | | | | | | |
|-------|-------|-------|-------|-------|-------|----------|----------|----------|-----------------------------|-----------------------------|
| a_1 | a_2 | a_3 | a_4 | a_5 | a_6 | $f_1(a)$ | $f_2(a)$ | $f_3(a)$ | $a_1 \oplus a_2 \oplus a_3$ | $a_4 \oplus a_5 \oplus a_6$ |
| b_1 | b_2 | b_3 | b_4 | b_5 | b_6 | $f_1(b)$ | $f_2(b)$ | $f_3(b)$ | $b_1 \oplus b_2 \oplus b_3$ | $b_4 \oplus b_5 \oplus b_6$ |