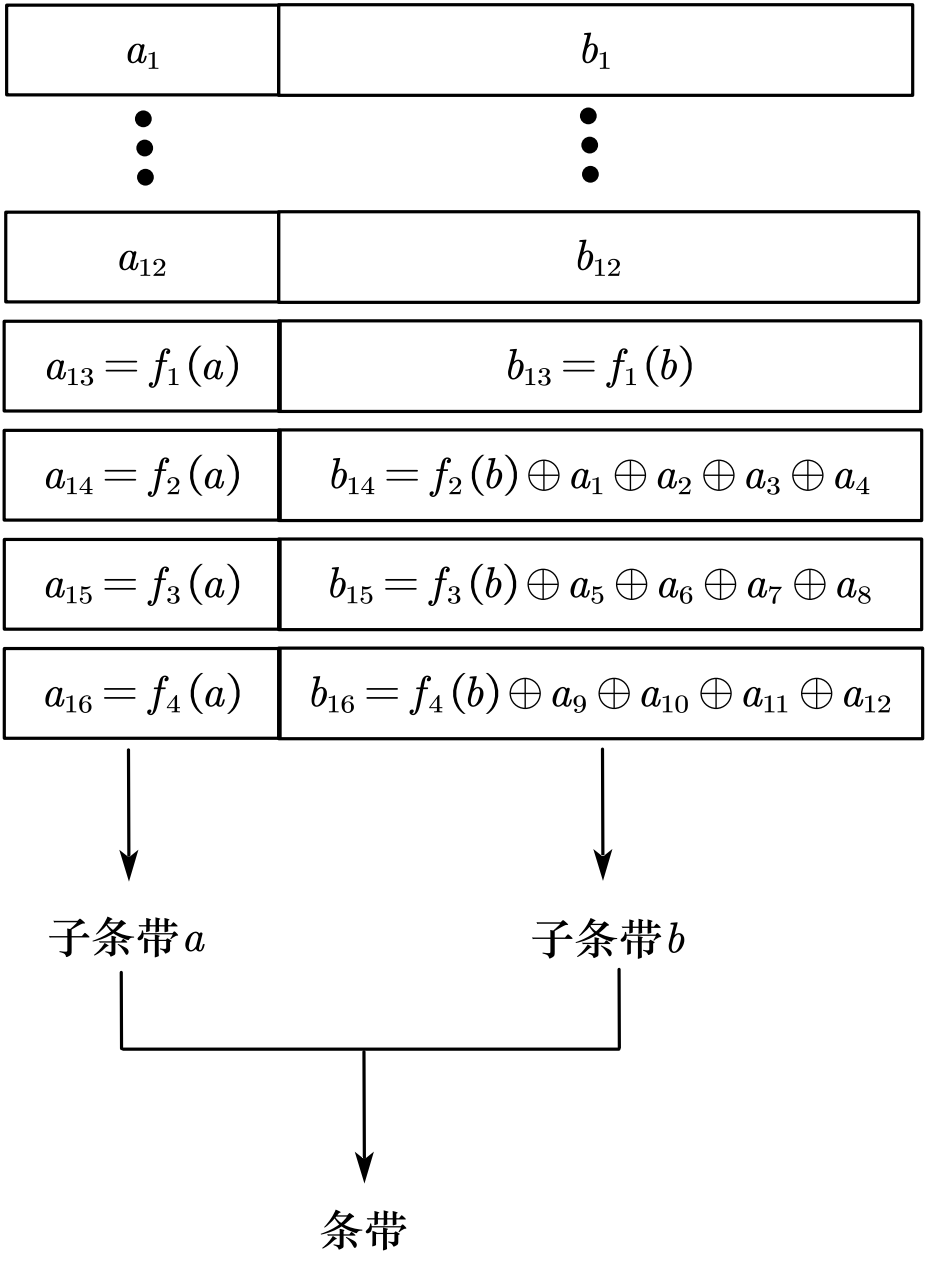
a_1
b_1
a_{12}
b_{12}
$a_{13} = f_1(a)$
$b_{13} = f_1(b)$
$a_{14} = f_2(a)$
$b_{14} = f_2(b) \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4$
$a_{15} = f_3(a)$
$b_{15} = f_3(b) \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8$
$a_{16} = f_4(a)$
$b_{16} = f_4(b) \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12}$
子条带a
子条带b
条带