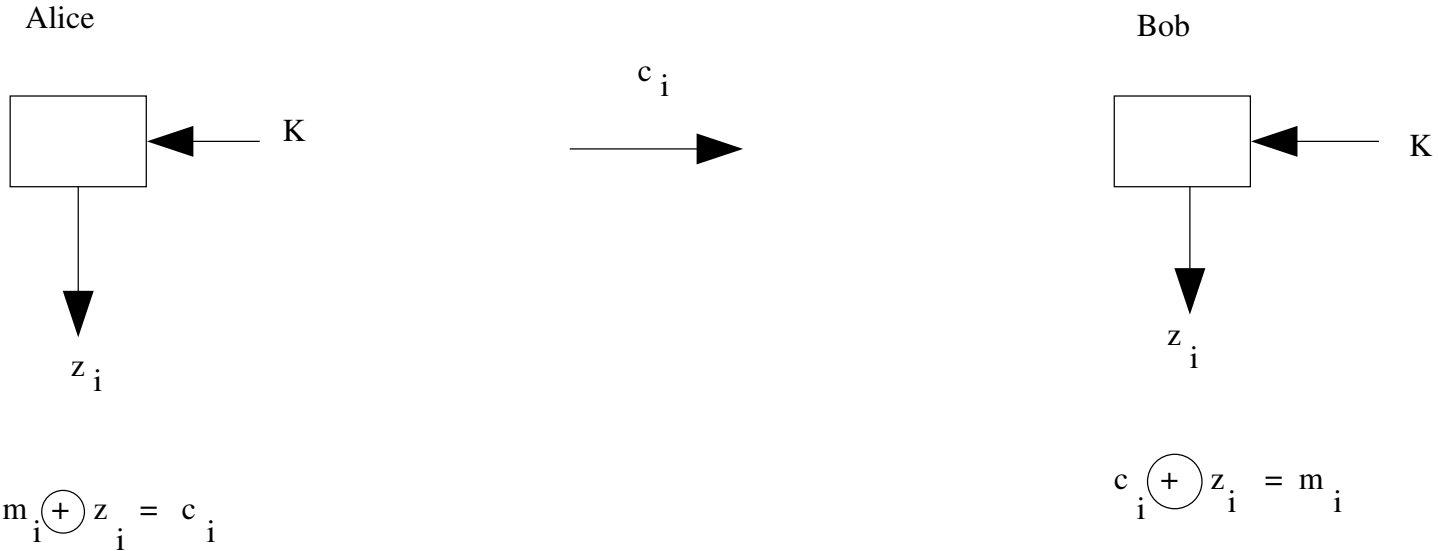
Alice
K
z_i
c_i
Bob
K
z_i
$m_i \oplus z_i = c_i$
$c_i \oplus z_i = m_i$