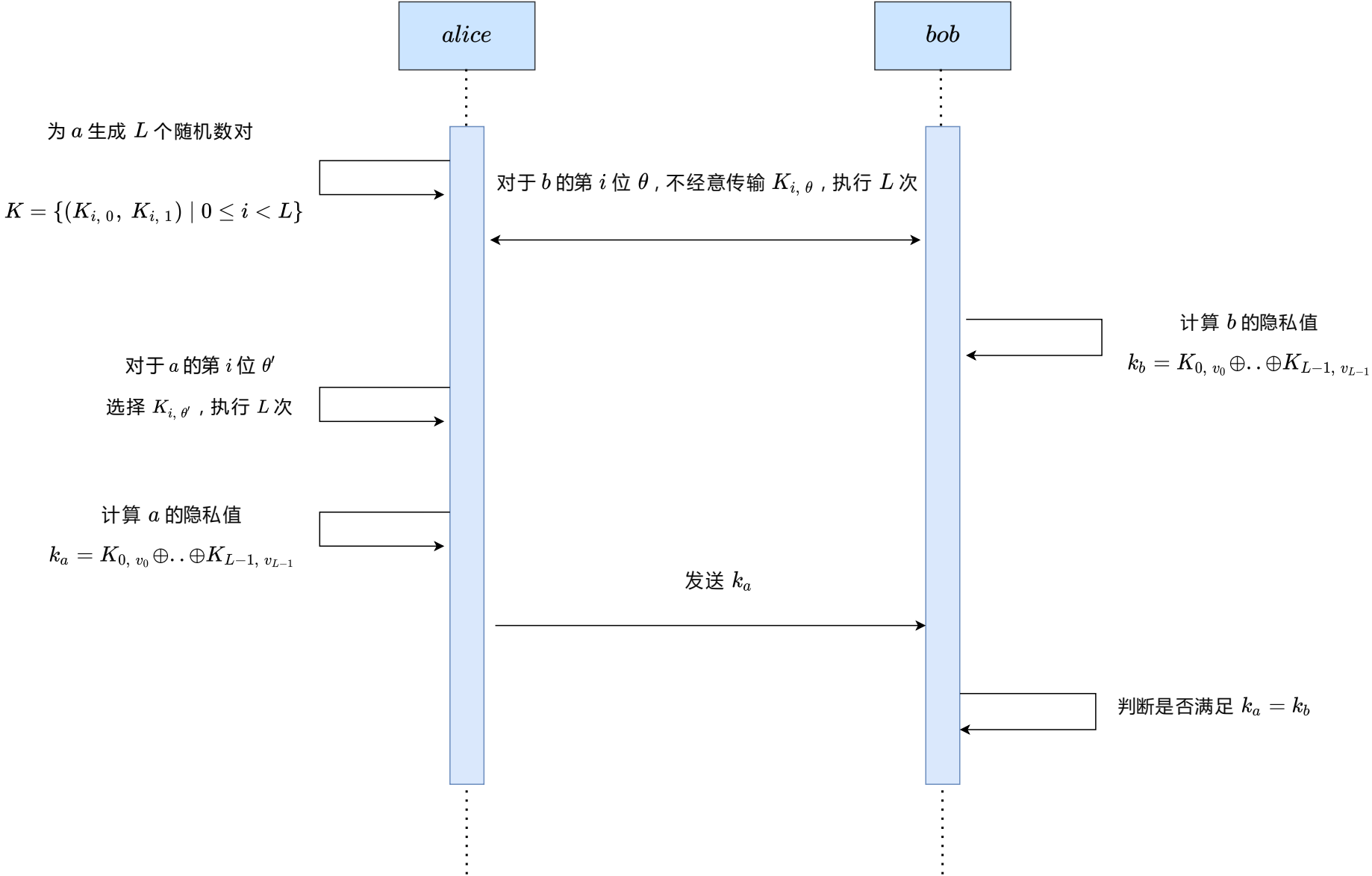
alice
bob
为 a 生成 L 个随机数对
$K = \{(K_{i,0}, K_{i,1}) \mid 0 \le i < L\}$
对于 b 的第 i 位 θ，不经意传输 $K_{i,\theta}$，执行 L 次
计算 b 的隐私值
$k_b = K_{0,v_0} \oplus .. \oplus K_{L-1,v_{L-1}}$
对于 a 的第 i 位 θ'
选择 $K_{i,\theta'}$，执行 L 次
计算 a 的隐私值
$k_a = K_{0,v_0} \oplus .. \oplus K_{L-1,v_{L-1}}$
发送 k_a
判断是否满足 $k_a = k_b$