

发送方

集合 $\{x_i\}_{i \in [1, n]}$



解码

$\{s_1^*, s_2^*, \dots, s_n^*\}$

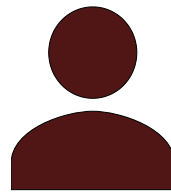
集合 $\{x_i\}_{i \in [1, n]}$

$\{s_i^*\}_{i \in [1, n]}$

VODE 协议

OT 协议

D



接收方

s 的 n 个密文: $\{s_i\}_{i \in [1, n]}$



编码 $\{y_i, s_i\}_{i \in [n]}$



加密密钥 k , 明文 s

判断结果 $\{b_i\}_{i \in [1, n]}$

$\{b_i\}_{i \in [1, n]}$ 且 $b_i = 0$

集合 $X \setminus (X \cap Y)$