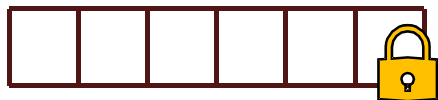


发送方

集合  $X = \{x_i\}_{i \in [1, n]}$

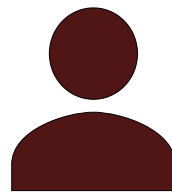
查询



$\{c_1, c_2, \dots, c_n\}$

发送加密过滤器

返回查询结果



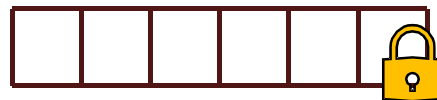
接收方

集合  $Y = \{y_i\}_{i \in [1, n]}$

插入



同态加密



$\{c_1, c_2, \dots, c_n\}$

解密

$\{e_1, e_2, \dots, e_n\}$