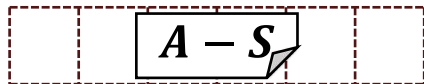


发送方

集合 $\{x_i\}_{i \in [1, n]}$

B, Δ



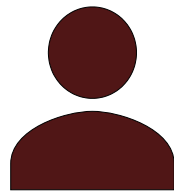
解码

$\{f'(x_1), f'(x_2), \dots, f'(x_n)\}$

B, Δ

VOLE 协议

A, C



接收方

构建 $\{y_i, f(y_i)\}_{i \in [1, n]}$

编码



比对 $\{H(f'(x_i))\}_{i \in [1, n]}$
与 $\{f(y_i)\}_{i \in [1, n]}$

$A - S$

$\{H(f'(x_i))\}_{i \in [1, n]}$