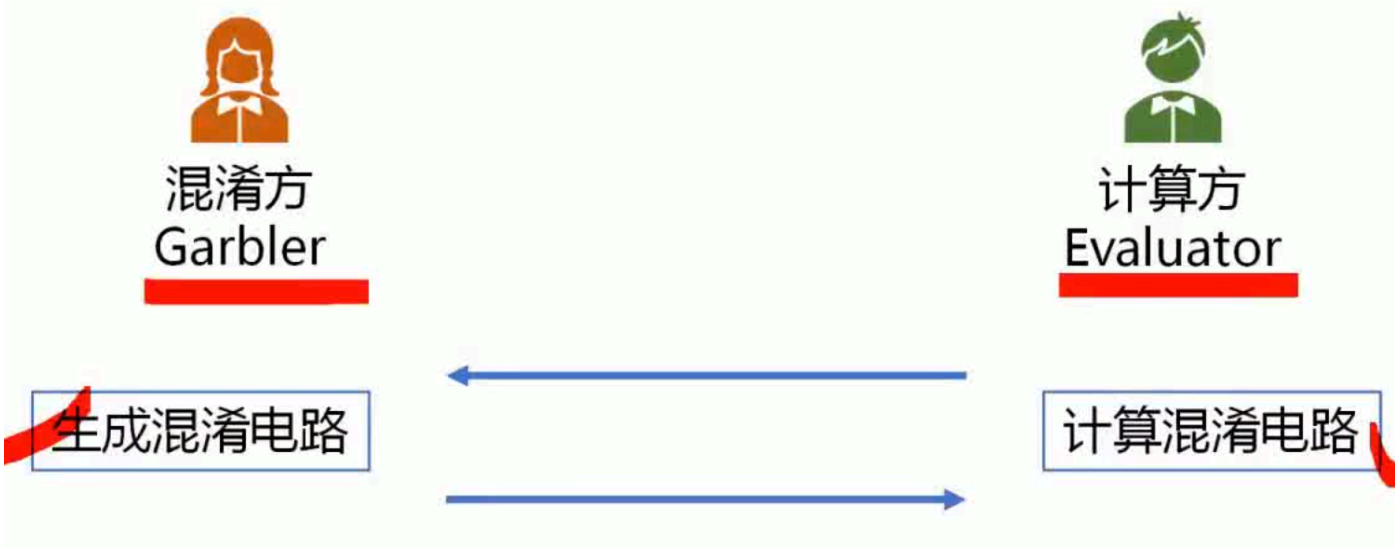
���ڂ·····İ·ő□Э··

···ɾ۶Ç

·····Ç····ő·····(2PC)Э·····Ʒ·····ص··溯······Ĺ··췽··

2PC·····Ï·····c··燔



□□□□□□□□MPC□□□□□0(1)□□□□□□□□

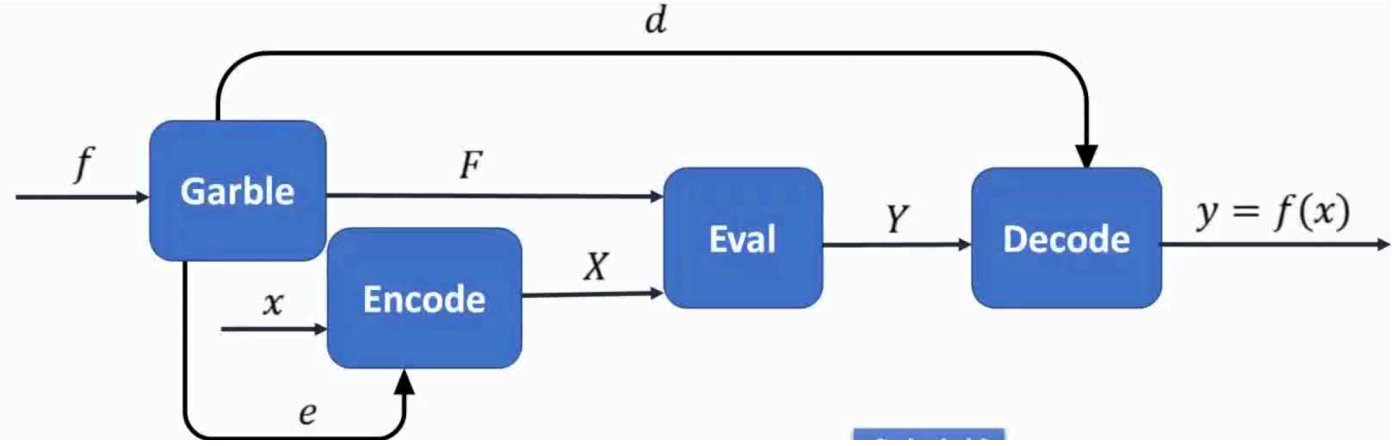
WRK类分布式混淆电路

- **非对称性**：只有一方能计算混淆电路
- 混淆电路大小：共发送 $4n(n-1)|C|\kappa$ 比特
- 在线轮数：2-4 轮

[YWZ20]：$(4n-6)(n-1)|C|\kappa$ 比特

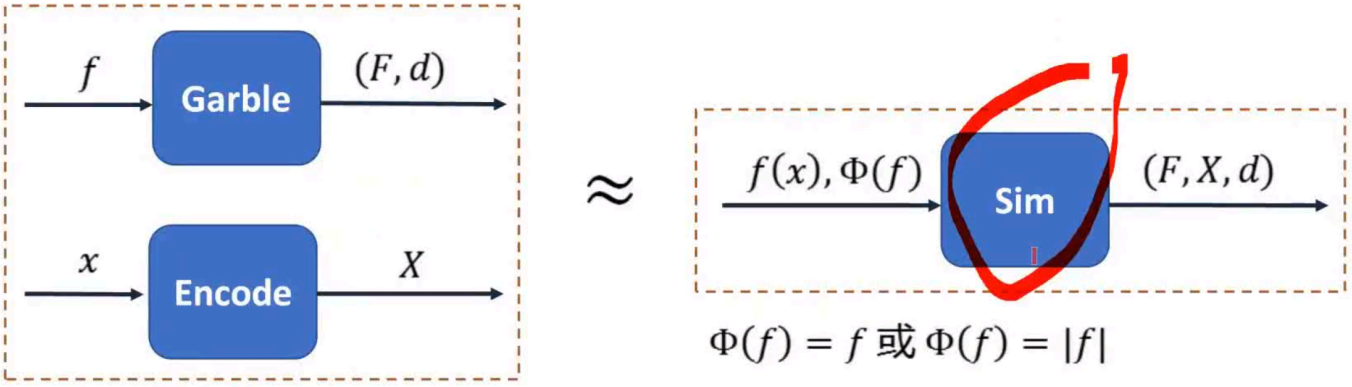
Yao�İ��ˈ��ŏ����Ɜ��

������·�������壺



- fÏ��·��FÏ������·
- e������Ш��d������Ш
- x��·���룬y��·���
- X������룬Y�������
- Garble�����燦
- Encode�����燦
- Eval�����燦
- Decode�����燦

������·��ǵ᪥ŏ���壺



Yao的混淆器定义为：$z=f(x,y)$，即混淆器输入为函数f和输入x，输出为混淆电路F和编码信息d

1. 混淆器Garble输入函数$f(x,y)$
   的电路表示F和编码信息d

2. 混淆器输入安全参数1^λ

3. 混淆器OT协议传输
   输入y的编码信息d

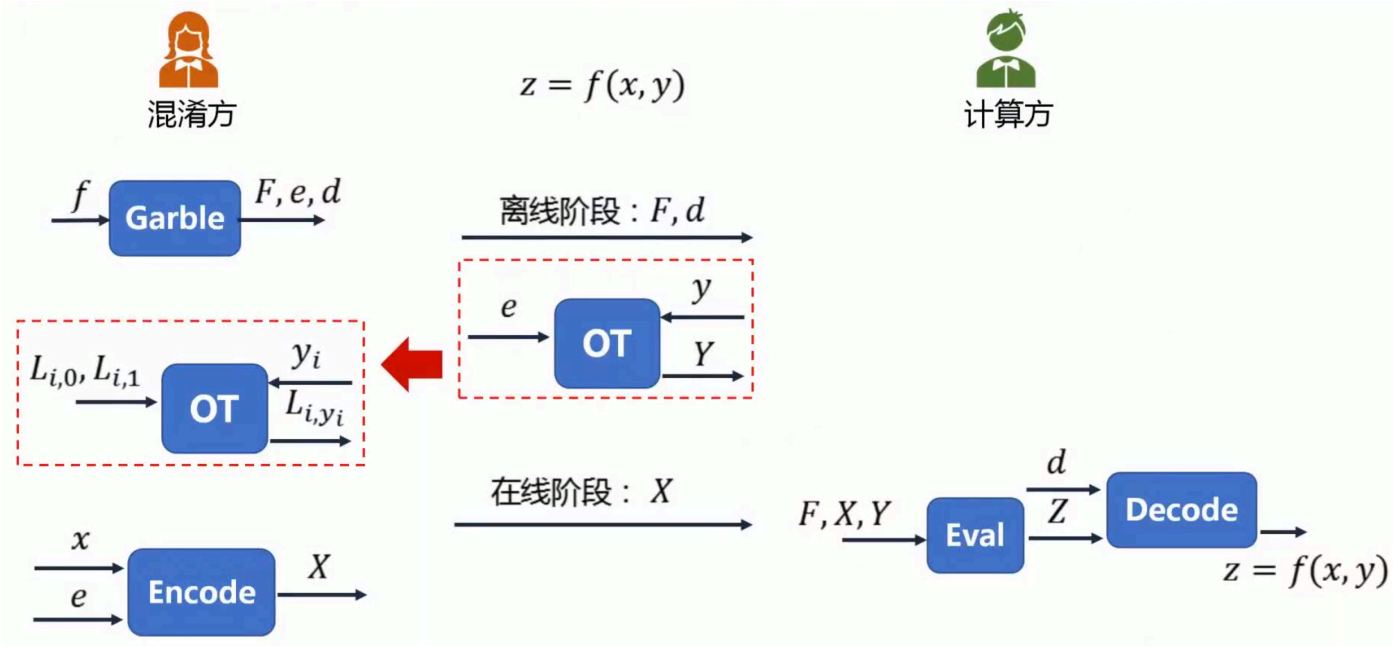
4. 混淆器输入布尔电路f

5. 混淆器输出1^λ

6. 混淆器输入Eval、F、X、Y输出z

7. 混淆器输入Decode、d、Z输出Z

   混淆器输入函数f
   的电路表示F和编码信息d
   混淆器输入X、F和d输出Z
   混淆器输入1^λ、F和d
   混淆器输入Yao的混淆器定义$z=f(x,y)$
   z：F和d



⬚⬚⬚⬚⬚⬚·⬚Ĺ⬚⬚⬚⬚Ч⬚ЧŁ⬚

⬚⬚⬚⬚⬚·⬚Ļ⬚⬚⬚⬚⬚

Garble⬚⬚⬚⬚⬚

- ⬚⬚⬚⬚ÿh⬚⬚⬚⬚·⬚Ղ⬚wqฺ⬚⬚Ч($K_0^i,\ K_1^i$)
- ⬚⬚⬚⬚ÿh⬚⬚⬚⬚·⬚ţ⬚
  - ⬚⬚⬚⬚⬚⬚⬚⬚⬚Ч($L_0,\ L_1$)
  - ⬚⬚⬚⬚⬚⬚⬚⬚⬚Ч($R_0,\ R_1$)
  - ⬚⬚⬚⬚⬚⬚⬚Ч($Z_0,\ Z_1$)
  - ⬚⬚⬚⬚⬚⬚⬚⬚$gg \leftarrow Gb(g, L_0, L_1, R_0, R_1, Z_0, Z_1)$
- ⬚⬚·⬚⬚⬚⬚‘⬚⬚⬚Ч⬚⬚⬚ɱ⬚⬚⬚⬚⬚ɯ$e = \{(K_0^i,\ K_1^i)\}$
- ⬚⬚·⬚⬚⬚⬚‘⬚⬚⬚Ч⬚⬚⬚ɾ⬚⬚⬚⬚⬚ɯ$d = (Y_0, Y_1)$
- ⬚⬚⬚л⬚⬚⬚⬚Ź⬚⬚ɻ⬚⬚⬚⬚⬚·$F = \{gg^i\}$

Encode⬚⬚

$$X \leftarrow Encode(e, x)$$

⬚⬚⬚ⱥ $e = \{(K_0^i, K_1^i)\}$⬚⬚$x = (x_1, ..., x_m)$

⬚⬚⬚⬚⬚$X = (K_{x_1}^1, ..., K_{x_m}^m)$

Decode⬚⬚

$$y \leftarrow Decode(d, Y)$$

���륜$d = \{Y_0, Y_1\}$��Y

$Y = Y_0$$y = 0$$Y = Y_1$$y = 1$

$$Y \leftarrow Eval(F, X)$$

TextbookYao

$H()$$Ï$$\bar{o}$

$H()$$C_{ab}$

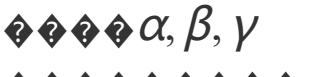
Z

Eval$\bar{W}$a$b

Ш$Ш$й¶

h$

$K-bit 0$



Χ���h���ў��ţ��(AES-NI)���ᵡ�������·��Ч��p����ᶜ�ſ���

********Ł**********Чw**кĽ**

wḍZ0ḍ̈́*H(L0,R0)

Free XOR********ƺ****ż***кĽ**

****.**ΧÑ*****Ч**wḍ**********ᵡ̃**脥
ᶜõ*****Чdelta**********

*****ḭ***õ*******H()**w****Ç****h****ó*******

ڇ**ƺ**ᶜ*****ḛ*********Ɛ***XOR****Ç̌ţ***ᵡ̃*****ɹ*****

Ż*****

h*Ż***

MPC**********5***