

- $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$ 
  - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
  - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
  - Yao 的  $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
  - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$ 
    - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
    - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
    - Textbook Yao 的  $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$ 
      - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
      - $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$
- MPC 的  $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$

$\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$

$\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$

$\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$

2PC 的  $\mathbb{Z}_p$  上的乘法逆元  $a^{-1}$  满足  $aa^{-1} \equiv 1 \pmod{p}$



## 计算混淆电路

♠ J ♣ ? ♡ ? ♢ ? ♤ ? ♧ ? ♨ ? ♩ MPCЭ ♪ ? ♫ ? ♬ ? ♭ ? ♮ ? ♯ ? ♰ ? ♱ ? ♲ ? ♳ ? ♴ ? ♵ ? ♶ ? ♷ ? ♸ ? ♹ ?

◆◆◆◆◆◆ MPCЭ◆◆

- 
- 

## BMR类分布式混淆电路

- **对称性**：所有参与方都能计算混淆电路
- **混淆电路大小**：共发送  $4n^2|C|\kappa$  比特
- **在线轮数**：2 轮

$|C|$  表示 AND 门数量,  $n$  表示参与方数量

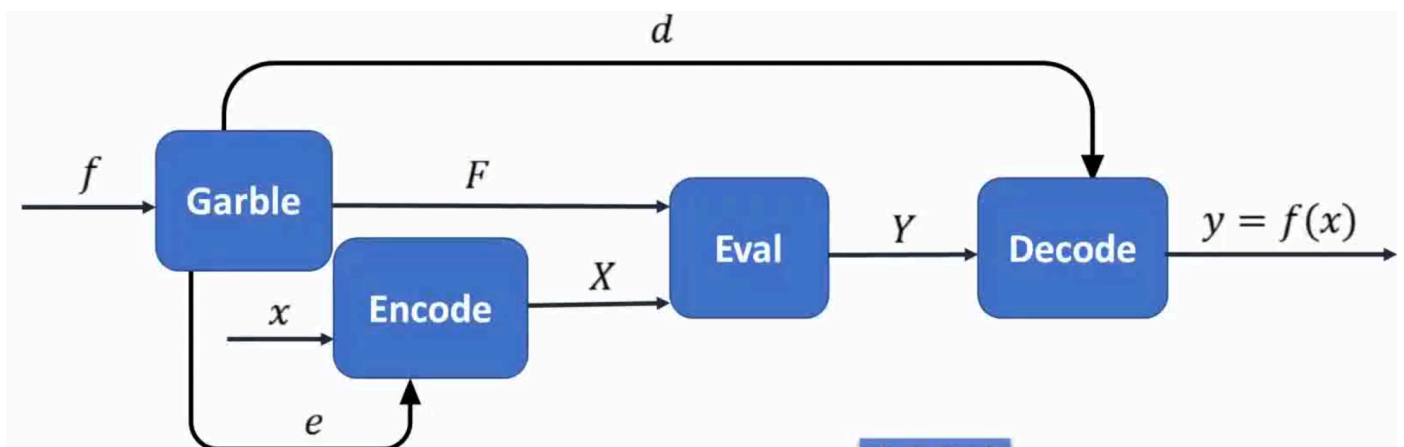
## WRK类分布式混淆电路

- **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?i??ʻ??ö????E??

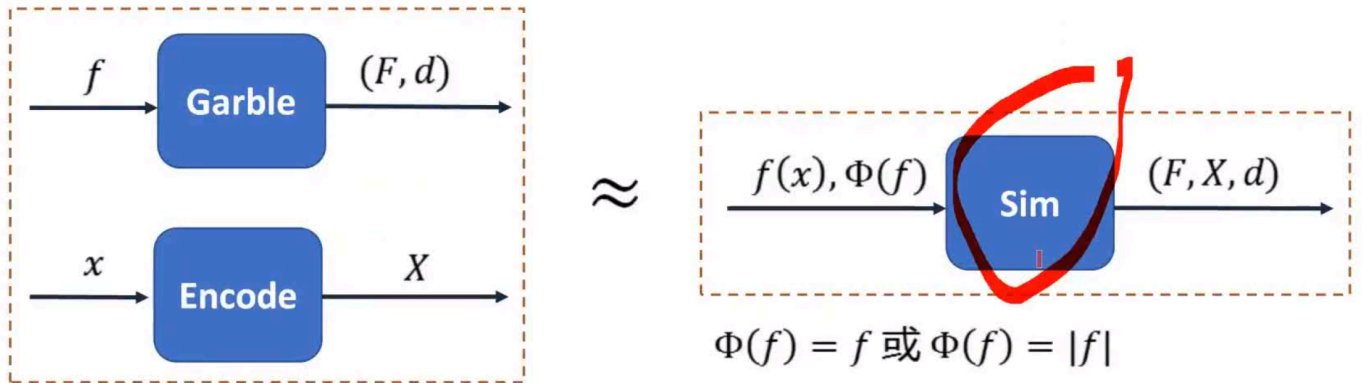
**? ? ? ? ? ? · ? ? ? ? ? ? ?**



- fi???.Fï?????
- e?????y???d?????y
- x???.륜y??.
- X?????륜Y?????
- Garble????燐
- Encode????燐
- Eval????燐
- Decode????燐

◆ ◆ ◆ ◆ ◆ · ◆ ◆ ḡ ◆ ʘ ö ◆ ◆ ◆ 壺

??L?A?????????????c?????????????g?º?  
 ???壺



Yao?????ö?????É?????í?????은?????z=f(x,y)?i?ö?????得  
 ???IJ?????£?

1. ??????Garble?燐?????f(x, y)  
 n?????·F?????ye?????yd
2. ??????□□□μ??燐???F??d?????ü?H?????ye
3. ??????OTЭ?養???燐  
 ??????ïy?????ie?????n??燐  
 ??????y?????Y
4. ??????ḡ?????e?????x?????X
5. ??????□□□λ?????X?????□?????燐
6. ???燐?????Eval?燐?????İF??X??Y?????İz?ı?????Z
7. ???n??燐?ḡ?????Decode?燐?????İd??Z?????İz

?????燐  
 ??????i?????ö?????Э?養  
 ı?????X?????̄?h?????n?????c??燐  
 ???ü?????i?????ö?????Э?養  
 ??????š?????Yao?????ö?????Э?????Ч??p?????¸????  
 ???·ij'磳

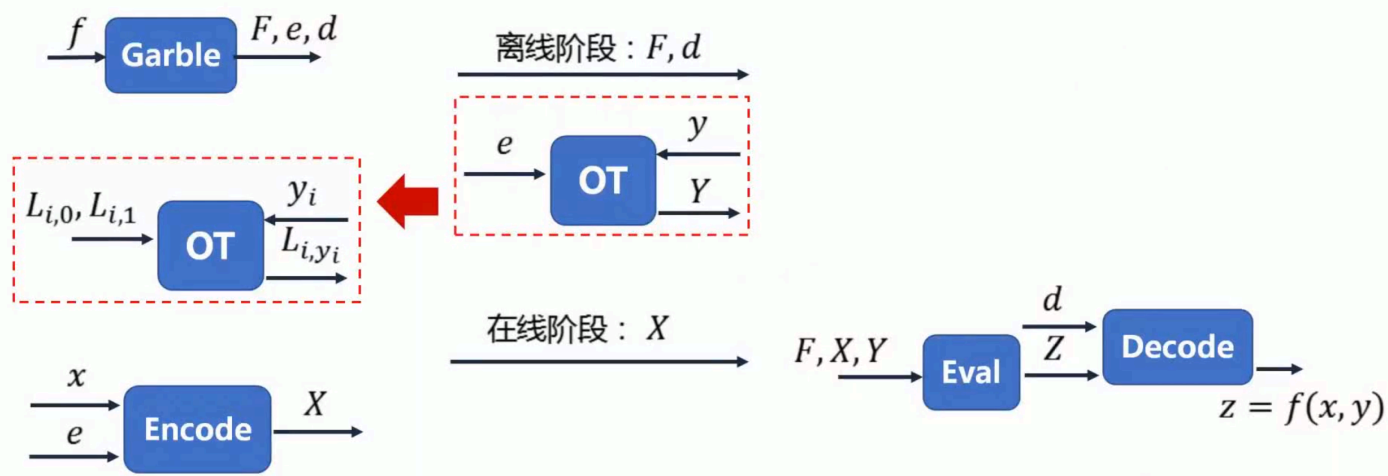


混淆方

$$z = f(x, y)$$



计算方



???.?·?L???.?4?4L?

????·?L????

Garble????燐

- ????yhh????·?1?wd,???( $K_0^i, K_1^i$ )
- ????yhh????·?t?
  - ??????????( $L_0, L_1$ )
  - ??????????( $R_0, R_1$ )
  - ??????????( $Z_0, Z_1$ )
  - ??????????  $gg \leftarrow Gb(g, L_0, L_1, R_0, R_1, Z_0, Z_1)$
- ?·????,?????m????e =  $\{(K_0^i, K_1^i)\}$
- ?·????,?????d =  $(Y_0, Y_1)$
- ????л????Z???.F =  $\{gg^i\}$

1730444518108

Encode燐

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

??? e =  $\{(K_0^i, K_1^i)\}$  ?? x =  $(x_1, \dots, x_m)$

???? X =  $(K_{x_1}^1, \dots, K_{x_m}^m)$

Decode燐

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

$$d = \{Y_0, Y_1\} Y$$

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

$$\perp$$

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

1730450082245

•

wd ŭ ± · ŵ

1730450136598

1730450191170

TextbookYao•

1730450228927

H() İ ç ö

ℳ H() ç õ C<sub>ab</sub>

ḡ ü ' õ Z

ف ' Eval 烽 ñ W ı a b

Щ ѡ ѣ

h ℳ 𐄀

û ı Ÿ t □ ж Ĺ . j

h•K-bit 0

ı Dz H Z

Æ Z c h K-bit 0 β

ôûÿΧ<sup>c</sup>υβ  
0жрJ

Çj∞цJЉ

<sup>c</sup>ƒε

1730450673078

j.ûŽ

„Dz0İ<sup>ä</sup>β<sup>a</sup>Dz1-bit  
bitûbitİж

α,β,γ  
өгİ„óυ  
bitİûİβ

Çυæûbitج·<sup>ñ</sup>'

ÑEval $a \oplus \alpha, b \oplus \beta$

⊥□a?b?c?уc=ab

1730450790740

1730450902142

1730450911704

1730450920998

ØTûbit□漣υ

1730451109217

•ЧκЉ

HκЉ

1730451204135

ℳXƒAES燿!eHash

 1730451786156