一、布尔电路下的情形　例：5⊕3=6　101 ↩5, 011 ↩3, 110 →6

① 秘密X ⟶ 子秘密 x_1、x_2、x_3，且 $X=x_1\oplus x_2\oplus x_3$

具体方式：秘密分享者生成三个随机数 a_1、a_2、a_3

且 $a_1\oplus a_2\oplus a_3=0$

让 $x_1=a_3\oplus X$，$x_2=a_1\oplus X$，$x_3=a_2\oplus X$

有 $x_1\oplus x_2\oplus x_3=X$

让三者分别持有 (a_1,x_1)，(a_2,x_2)，(a_3,x_3)

（生成满足 $a_1\oplus a_2\oplus a_3=0$ 的方法：

A、B、C 随机生成 ρ_1、ρ_2、ρ_3

A $\xrightarrow{\rho_1}$ B $\xrightarrow{\rho_2}$ C，ρ_3 C→A

有 $a_1=\rho_1\oplus\rho_3$

$a_2=\rho_1\oplus\rho_2$

$a_3=\rho_2\oplus\rho_3$

易得 $a_1\oplus a_2\oplus a_3=0$ ）

（此时任意两个人合谋便可恢复秘密）

例：1与2合谋：x_2 与 a_1 合力得到 $x_2\oplus a_1=a_1\oplus X\oplus a_1=X$

② 多方加法

$$[z]=[x]+[y]$$

1、对1：持有 $x_1=a_3\oplus X$　$y_1=b_3\oplus y$　对2、3同理

$$x_1\oplus y_1=a_3\oplus X\oplus b_3\oplus y=(a_3\oplus b_3)\oplus(X\oplus y)=(a_3\oplus b_3)\oplus Z$$

2、将3者结合进行运算

有 $(x_1\oplus y_1)\oplus(x_2\oplus y_2)\oplus(x_3\oplus y_3)\oplus Z\oplus Z\oplus Z$

$=0\oplus0\oplus0\oplus0\oplus Z=Z$

③ 多方乘法

$$[z]=[x]\cdot[y]$$

引入三个随机数 $\alpha、\beta、\gamma$，且 $\alpha\oplus\beta\oplus\gamma=0$

Alice 计算 $r_1=x_1y_1\oplus a_1b_1\oplus\alpha$

发送

Bob 计算 $r_2=x_2y_2\oplus a_2b_2\oplus\beta$

Candy 计算 $r_3=x_3y_3\oplus a_3b_3\oplus\gamma$

（为何有发送操作？）

↓

进行 $r_1\oplus r_2\oplus r_3$ 的操作？

Alice 本地计算：$c_1=r_1\oplus r_3$

Bob：$c_2=r_2\oplus r_1$

Candy：$c_3=r_3\oplus r_2$

$\Rightarrow\begin{cases}r_1=z_1\\r_2=z_2\\r_3=z_3\end{cases}\Rightarrow r_1\oplus r_2\oplus r_3=z=xy$

证：

$x_1y_1=(a_3\oplus x)(b_3\oplus y)=a_3b_3\oplus a_3y\oplus xb_3\oplus xy$

$x_2y_2=(a_1\oplus x)(b_1\oplus y)=a_1b_1\oplus a_1y\oplus xb_1\oplus xy$

$x_3y_3\ (a_2\oplus x)(b_2\oplus y)=a_2b_2\oplus a_2y\oplus xb_2\oplus xy$

⇓

$x_1y_1\oplus x_2y_2\oplus x_3y_3=a_1b_1\oplus a_2b_2\oplus a_3b_3\oplus x(\underbrace{b_1\oplus b_2\oplus b_3}_{0})\oplus y(\underbrace{a_1\oplus a_2\oplus a_3}_{0})\oplus xy$

$=a_1b_1\oplus a_2b_2\oplus a_3b_3\oplus xy$

↓ 代入

$r_2\oplus r_2\oplus r_3=x_1y_1\oplus a_1b_1\oplus\alpha\oplus x_2y_2\oplus a_2b_2\oplus\beta\oplus x_3y_3\oplus a_3b_3\oplus\gamma$

$= (x_1y_1 \oplus x_2y_2 \oplus x_3y_3) \oplus (a_1b_1 \oplus a_2b_2 \oplus a_3b_3) \oplus (\alpha \oplus \beta \oplus r)$

$= (a_1b_1 \oplus a_2b_2 \oplus a_3b_3) \oplus xy \oplus (a_1b_1 \oplus a_2b_2 \oplus a_3b_3)$

$= xy$

$c_1 \oplus c_2 \oplus c_3 = (r_1 \oplus r_1) \oplus (r_2 \oplus r_2) \oplus (r_3 \oplus r_3) = 0$

有 $z_1 = c_3 \oplus xy$

$z_2 = c_1 \oplus xy$

$z_3 = c_2 \oplus xy$

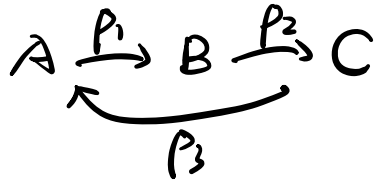
有 $z_1 \oplus z_2 \oplus z_3 = xy$ $c_1 \oplus c_2 \oplus c_3 = 0$

二、扩展至环 2^n 下的方式 (算秘享)

① 在环 2^n 下生成三个随机数 a_1, a_2, a_3

且 $a_1+a_2+a_3=0$

生成方法：A、B、C 分别生成 $\rho_1、\rho_2、\rho_3$



A: $\rho_1-\rho_3=a_1$

B: $\rho_2-\rho_1=a_2$

C: $\rho_3-\rho_2=a_3$

② 现在秘密 $x、y$

则 $x_1=a_3-x \qquad y_1=b_3-y$

$x_2=a_1-x \qquad y_2=b_1-y$

$x_3=a_2-x \qquad y_3=b_2-y$

A 持有 $(x_1,a_1),(y_1,b_1)$

B $(x_2,a_2),(y_2,b_2)$

C $(x_3,a_3),(y_3,b_3)$

③实现 $x+y$

先本地计算 $x_i+y_i=z_i$

如 $x_1+y_1=z_1=a_3-x+b_3-y$

三人合起来：

$$\sum_{i=1}^{3} z_i=-3(x+y)+(a_1+a_2+a_3)+(b_1+b_2+b_3)$$

$$\sum_{i=1}^{3} z_i=-3z$$

$\therefore z = -\frac{1}{3}(z_1+z_2+z_3)$

④ 实现乘法

再生成一组随机数 α, β, ρ (方法同上)

A: $r_1 = (x_1y_1 - a_1b_1 + \alpha)/3$

B: $r_2 = (x_2y_2 - a_2b_2 + \beta)/3$

C: $r_3 = (x_3y_3 - a_3b_3 + \rho)/3$

有: $r_1+r_2+r_3$

$$= \frac{1}{3}\left[x_1y_1 + x_2y_2 + x_3y_3 - \sum_{i=1}^{3} a_ib_i\right]$$

$$= \frac{1}{3}\left[(a_3-x)(b_3-y) + (a_1-x)(b_1-y) + (a_2-x)(b_2-y) - \sum_{i=1}^{3} a_ib_i\right]$$

$$= \frac{1}{3}\left[3xy - (\underbrace{b_1+b_2+b_3}_{0})x - (\underbrace{a_1+a_2+a_3}_{0})y\right]$$

$$= xy$$