三元组制备：

1. Server 生成随机数 a_0,b_0，并利用 paillier 同态加密为 $E(a_0)$和 $E(b_0)$，发送给 Client
2. Client 生成随机数 a_1,b_1,c_1，并计算 $E(b_0)$的 a_1 次方，$E(a_0)$的 b_1 次方,以及加密数据 $E(a_1 \times b_1 - c_1)$，并将三者相乘，发送给 Server
3. Server 将结果解密，并加上 $a_0 \times b_0$，即得到 c_0
4. Server 拥有 a_0,b_0,c_0，Client 拥有 a_1,b_1,c_1，满足$(a_0,a_1)\times(b_0,b_1)=(c_0,c_1)$

三元组使用：

1. Server 拥有数据 x_0,y_0，Client 拥有数据 x_1,y_1
2. Server 公开 x_0+a_0 和 y_0+b_0，Client 公开 x_1+a_1 和 y_1+b_1
3. 双方各自计算：

   $e = (x_0+a_0)+(x_1+a_1) = (x_0+x_1)+(a_0+a_1) = x+a$

   $f = (y_0+b_0)+(y_1+b_1) = (y_0+y_1)+(b_0+b_1) = y+b$
4. Server 本地计算 $z_0=-f\times a_0-e\times b_0+c_0$

   Client 本地计算 $z_1=-f\times a_1-e\times b_1+c_1+e\times f$
5. Server 拥有乘法门结果 z_0，Client 拥有乘法门结果 z_1