

总结：1.算数电路中只用了一个加法门，用了一个乘法门（需要一组三元组）

**P0拥有a0 b0 c0** **P1拥有a1 b1 c1**

**满足(a0+a1)(b0+b1)=(c0+c1)**

**P0公开x0+a0，y0+b0**

**P1公开x1+a1，y1+b1**

**双方均可计算获得e=x+a,f=y+b**

**P0本地计算：z0=-fa0-eb0+c0mod2k**

**P1本地计算：z1=ef-fa1-eb1+c1mod2k**

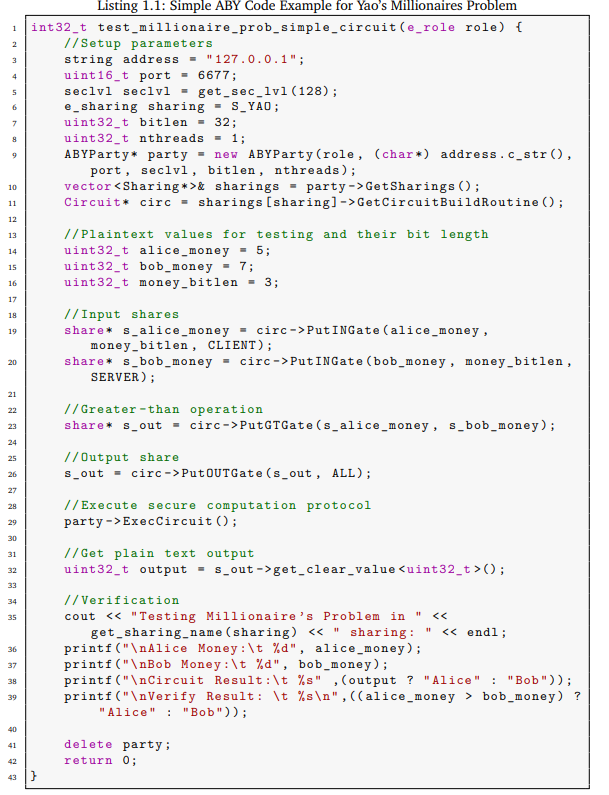
2.算数电路转布尔电路底层是利用加掩码在输出放入另外一个电路之中，所以会有加法门损耗。

3.算数电路转布尔电路会进行一个32位的比较门

也可以直接用布尔电路去做：

首先会用到一个32位加法器

然后会用到一个32位的乘法器

最后会用到一个32位比较门