参与者：数据库持有者 Bob，第三方 TP，n个用户

数据库项N

1. Bob与预先共享一个2N个元素的密钥；
2. TP随机制备4N 个单光子乘积态，每个态属于，然后把这些态发送给Bob；
3. Bob收到态，从位置集合中随机选择2N个元素作为子集，然后Bob按对位置上的乘积态施加酉操作U;

其中酉操作

在经过上述酉操作后，V位置集上有各，重排至时，位置上的态分别为即可，

然后，Bob把所以乘积态序列划分为n 个长为 4N 的单光子态序列，分别发送给用户。随后Bob公布位置集V；

1. **用户认证Bob**

收到态序列后，根据以下规则对V位置上的态进行测量：

按解码得到，然后用与一一比较，若所有都相等，认证Bob成功，否则协议中止，认证Bob成功后把所有发送给Bob ；

1. Bob检测信道安全性，Bob将发回的态以制备时的基底测量，计算错误率，若高于预先设定的错误率阈值，则存在窃听，协议中止；
2. **Bob认证用户**

Bob根据的测量结果后以同样方式解码得到一系列二比特块并与中的元素一一顺序比较，若全部相等则Bob认证成功；

1. 用户丢弃用于认证的态，此时，用户还剩2N qubit 的一个序列，分别记为，用户