# 基于量子不经意传输的PSI方案

# 1 背景及目标

不经意传输(Oblivious Transfer,OT) 是安全多方计算的基本构件之一，不经意传输的安全性对整体安全多方计算的安全性起重要作用。安全多方计算中的不经意传输协议其长期以来被认为需要依赖椭圆曲线上的离散对数、编码、格密码等假设，而不能仅依靠单向函数、哈希函数或对称加密来构建。但最近的研究表明，在量子世界中，安全多方计算仅需要单向函数就可以构建，通过哈希函数实例化协议中的单向函数即可得到天然抗量子的安全多方计算，这使得此种利用量子信息的安全多方计算天然就是抗量子的。研究基于量子信息的安全多方计算既是密码学前沿的课题，又为量子信息产业增添了一类全新的应用。

在理论方面，Bennett等人在CRYPTO 1991给出了最早的基于量子的不经意传输[1]。此后这些方案被不断地修正和改进[2][3]。之后提出了依赖经典承诺构造的量子不经意传输协议，并给出了安全证明[4]。最近在EUROCRYPT 2021和CRYPTO 2021分别出现了相关论文，给出了CRS模型下的UC安全的协议[5][6]，表明基于量子信息的安全多方计算在理论上已经较为成熟。而在实验方面，国内外尽管有一些不同协议的不经意传输的实验[7][8][9]，实验[7]基于noisy storage模型，实验[9]基于nonorthogonal states进行了不经意传输的实验，验证了量子不经意传输的可行性。但总体上这些工作还停留在理论阶段，尚未得到广泛的实验论证。

2023年国科量子与上海交大合作，完成了“基于量子信息的安全多方计算”课题。课题中，团队在已有的研究基础上，以离散变量量子通信方式设计了量子不经意传输协议（Quantum Oblivious Transfer,以下简称QOT），对此种QOT协议实现中可能存在的“延迟测量攻击”设计了攻击检测步骤。课题中，团队基于成熟的BB84协议量子密钥分发（Quantum Key Distribution，以下简称QKD）设备进行功能改造，利用BB84 QKD设备已有的量子态信息制备分发和接收测量功能，按照QOT协议步骤进行具体功能设计实现，完成了实现系统的开发和测试验证，证明了离散变量QOT系统的可行性，并对系统安全性进行了较充分的理论论证和功能实现。

本方案目标为在上述课题研究成果的基础上，将QOT系统应用于人行反欺诈系统，替换隐私集合求交（Private Set Intersection，以下简称PSI）功能中基于密码算法构建的不经意传输功能，使系统在OT功能上具备抵抗量子攻击的能力基础。

# 2 方案框架



图1

本方案整体框架如上图所示，QOT功能分为QOT传输设备和QOT经典协商两部分组成。QOT传输设备（以下简称QOTD）为专用基于离散变量量子传输方式的量子不经意传输硬件设备，分为发送端和接收端，经量子信息传输在两端生成的量子比特和基底信息。QOT经典协商为软件功能组件，基于QOTD提供的量子比特和基底信息计算得到二选一结果。

# 3 方案说明



图2

本方案所需硬件运行环境主要如下：

|  |  |  |
| --- | --- | --- |
| 名称 | 数量 | 说明 |
| QOTD-A | 1台 | QOTD设备发送端。 |
| QOTD-B | 1台 | QOTD设备接收端。 |
| 裸光纤 | 2芯 | 链接QOTD-A及QOTD-B，距离不超过40km，光衰小于10db。 |
| 信创服务器 | 2台 | 两数据中心各一台，运行QOT程序。 |

方案主要流程如下：

1、QOTD-A与QOTD-B采用离散变量量子通信方式，在QOTD-A及QOTD-B分别生成用于后续QOT协商的中间协议数据，包括量子比特及基底信息，其中QOTD-A侧数据记为和，QOTD-B侧数据记为和。

2、QOTD-A及QOTD-B对量子比特和基底信息抽取部分做误码率检测，检验会否存在中间窃听者Eve，并判断生成数据质量，若误码率高于或等于2%，则丢弃此轮生成数据，若低于2%，则丢弃被抽查数据，剩余数据留用，安全存储于设备内部。

3、若上层PSI应用发起调用QOT功能，则有QOT-A从Alice侧PSI获取原始消息m0、m1。

4、QOT-A发起向QOTD-A获取和，并通知QOTD-B推送和至QOT-B。

5、QOT-A及QOT-B对获取的量子比特和基底信息进行“延时测量攻击”检测。

6、QOT-A向QOT-B发送基底信息。

7、QOT-B将与进行比较，因两个都是二进制随机序列，因此按照概率，有50%基底信息一致。一致和不一致的序列位信息分别按顺序分为两个集合和，其中，按照基底一致的比特位选取对应位，得到b。

8、QOT-B向QOT-A发送。

9、QOT-A按照对量子比特进行划分，并按划分后结果与QOT-B按照正向协商方式进行纠错和隐私放大处理。

10、QOT-A使用某种加密算法，将x0和x1作为密钥分别对m0、m1进行加密，以异或为例，f为与密钥等长的截取函数，计算，发送给QOT-B。

11、QOT-B使用b可以解密得到mb，向上层PSI应用输出QOT最终选择信息结果mb。

对PSI来说，QOT替换其他OT实现方式的功能，与PSI的BaseOT组件完成以下功能：

1、QOT-A向PSI-A获取被选信息m0、m1；

2、QOT-B向PSI-B获取随机选择项b∈(0,1)，并向PSI-B输出选择结果。

# 4 性能优化方案

QOT性能主要受限于以下两点：

1、QOTD设备成码率限制，光衰10db条件下，QOTD理论成码率为60kbps。QOTD做量子信息传输生成量子比特和基底信息的过程与QOT程序经典协商过程为异步处理，即QOTD按照其设置的数据存储空间大小，按能力随时做量子信息传输生成量子比特和基底，安全存储于设备，等待QOT程序调用，因此，当QOTD存储备用数据使用完毕后，实际的成码率将影响QOT获取量子比特和基底信息的效率。

2、QOT向QOTD申请量子比特和基底数据响应在实验阶段性能较低，是实际整体QOT性能的关键瓶颈。

为避免PSI调用OT功能时，实时向QOTD获取量子比特及基底数据，并进行QOT协议运算耗时较大的问题，本方案尝试参考预计算的方案[10]：

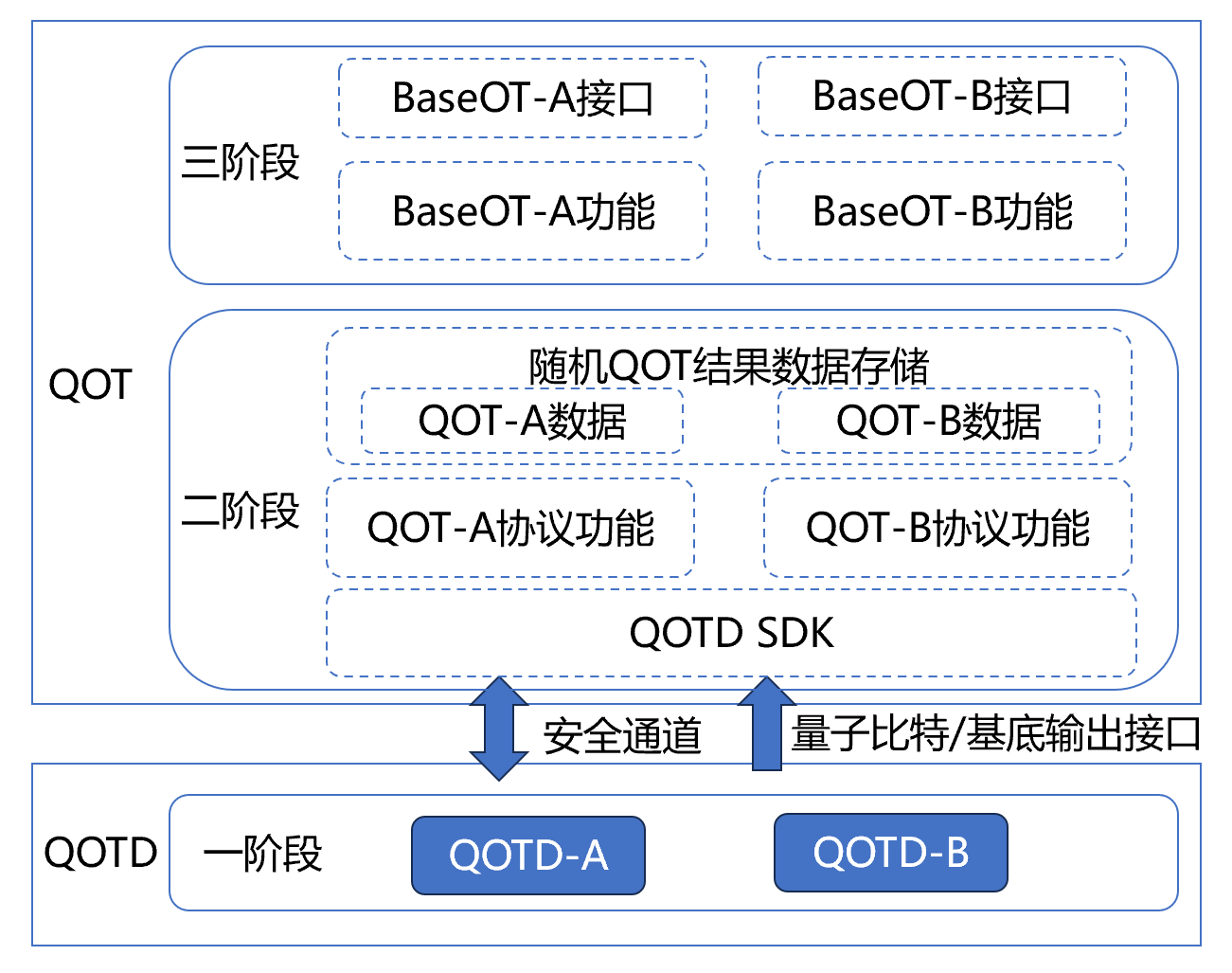
1、在未知PSI-A输入的情况下，由QOT做随机不经意传输，QOT-A得到、，QOT-B得到、，QOT-A和QOT-B分别对应存储提前生成备用的数据。

2、当PSI-A有明确的m0、m1输入QOT-A，PSI-B有选择比特位b输入QOT-B，QOT-B将c=b⊕发送给QOT-A。即当b=，c=0，当b≠，c=1；

3、QOT-A收到c后，若c=0，则向QOT-B发送⊕m0、⊕m1，若c=1，则向QOT-B发送⊕m0、⊕m1；

4、QOT-B收到m0、m1的密文消息后，使用解密，得到mc。

按照以上思路，QOT方案功能框架示意图如下，三阶段即上述2-4步骤，因执行的是异或操作，性能比执行完整QOT过程要快很多，为保证协议安全，QOT二阶段的QOT运算结果数据，只能按一次一密的方式执行三阶段异或操作。



引用文献

1. Bennett C H, Brassard G, Crépeau C, et al. Practical quantum oblivious transfer[C]//Annual international cryptology conference. Springer, Berlin, Heidelberg, 1991: 351-366.
2. Mayers D. Unconditionally secure quantum bit commitment is impossible[J]. Physical review letters, 1997, 78(17): 3414.
3. Lo H K. Insecurity of quantum secure computations[J]. Physical Review A, 1997, 56(2): 1154.
4. Ivan Damgård et al. “Improving the Security of Quantum Protocols via Commit-and-Open”. In: 2009, pp. 408–427. doi: 10.1007/978-3- 642-03356-8\\_24.
5. Grilo A B, Lin H, Song F, et al. Oblivious transfer is in miniqcrypt[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2021: 531-561.
6. Bartusek J, Coladangelo A, Khurana D, et al. One-way functions imply secure computation in a quantum world[C]//Annual International Cryptology Conference. Springer, Cham, 2021: 467-496.
7. Erven C, Ng N, Gigov N, et al. An experimental implementation of oblivious transfer in the noisy storage model[J]. Nature communications, 2014, 5(1): 1-11.
8. Amiri R, Stárek R, Reichmuth D, et al. Imperfect 1-out-of-2 quantum oblivious transfer: bounds, a protocol, and its experimental implementation[J]. PRX Quantum, 2021, 2(1): 010335.
9. Chou Y H, Zeng G J, Kuo S Y. One-out-of-two quantum oblivious transfer based on nonorthogonal states[J]. Scientific Reports, 2018, 8(1): 1-12.
10. Beaver D. Efficient Multiparty Protocols Using Circuit Randomization[C]. CRYPTO 1991.