# PSI-QOT测试报告

# 改进点说明：

1. 离线的部分的OT+ROT生成部分，建议与在线PSI比较部分分离，前者为异步生成；

解决方案：将离线部分分离出来作为一个服务生成ROT的基础数据。

1. 建议baseOT部分分离出来，对比一下量子改造过后的PSI以及原版PSI的效率；

解决方案：文件接口使用原版应用程序的接口，完成了控制变量的比对测试。

1. 在测试两端流量阶段，建议可通过划分Vlan的方式区分开PSI纯两端的通信流量。

解决方案：该部分暂未改造。

# 测试用例和结果

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 类别 | 测试点 | 测试用例 | 抗量子PSI（改进前）  测试结果 | 抗量子PSI（改进后）  测试结果 | 原始非抗量子PSI  测试结果 | 备注 |
| QOTD | 中间数据生成基础功能 |  | 通过 | 通过 |  |  |
| 中间数据生成性能 | 实际环境量QOTD-A和B之间2-3km，成码率 |  | 50kbps |  |  |
| 实验室环境QOTD-A和B之间多种距离成码率测试：1、尾纤1km，2、10km，3、30km，4、50km |  | 1km(0.34dB)：66.666664Kbps  10km(1.88dB): 66.666664Kbps  30km(5.44dB): 62.253333Kbps  50km(9.03dB): 45.740740Kbps |  | 实验室测试 |
| QOT | QOT与QOTD安全通道建立 | QOT与QOTD安全通道建立 | 通过 | 通过 |  |  |
|  | 执行QOT获取QOTD中间数据，执行一次基础QOT协议，测试一轮QOT时间 | 通过 | 通过 |  |  |
|  | 持续测试QOT，把QOTD存储的中间数据消耗完，测实时生成中间数据时，执行一次QOT的性能 |  |  |  | 待修改配置参数再跑 |
|  | ROT-mdata的生成及存储基础功能，128组ROT-mdata的生成时间 |  | 275ms |  |  |
|  | ROT基础功能，即一轮ROT执行时间 |  | 0.0078s |  |  |
| PSI | QOT+ROT:一轮PSI基础功能测试 | 数据提供方1W，查询端2K进行求交，交集数量为1172，比对测试结果和测试数据，确认是否能正确求交。 | 时间：  离线：70.1012s  在线：0.0228s  Recv:13.23M  Send:8.34M  测试结果：通过 | 时间：  0.0417s  OT：0.0078s  带宽：  Recv：2.94M  Send：  334.75kb | 时间：  0.0422s  OT：0.0109s  带宽：  Recv：863.22kb  Send：  232.28kb |  |
| QOT+ROT:不同数据量级的性能测试 | 查询方：1k数据提供方：1w | 时间：  离线：70.1017s  在线：0.0227s  带宽：  Send：8.47M  Recv：12.63M | 时间：  0.0417s  OT：0.0084s  带宽：  Recv：2.08M  Send：  195.69kb | 时间：  0.0418s  OT：0.0111s  带宽：  Recv：860.57kb  Send：130.50kb |  |
|  | 查询方：1k数据提供方：10w | 时间：  离线：70.1024s  在线：0.1208s  带宽：  Send：18.08M  Recv：30.34M | 时间：  0.3121s  OT：0.0079s  带宽：  Recv：11.31M  Send：  382.45kb | 时间：  0.3098s  OT：0.0110s  带宽：  Recv：8.36M  Send：240.08kb |  |
|  | 查询方：1k数据提供方：100w | 时间：  离线：70.1037s  在线：1.1535s  带宽：  Send：119.64M  Recv：15.61M | 时间：  3.1377s  OT：0.0080s  带宽：  Recv：85.57M  Send：  1.25M | 时间：  3.1046s  OT：0.0111s  带宽：  Recv：84.41M  Send：1.19M |  |
|  | 查询方：1k数据提供方：1k | 时间：  离线：70.1045s  在线：0.0148s  带宽：  Send：6.31M  Recv：14.14M | 时间：  0.0147s  OT：0.0112s  带宽：  Recv：161.89kb  Send：123.76kb | 时间：  0.0140s  OT：0.0109s  带宽：  Recv：99.90kb  Send：119.93kb |  |
|  | 查询方：1w数据提供方：1w | 时间：  离线：70.1051s  在线：0.0469s  带宽：  Send：10.83M  Recv：17.53M | 时间：  0.0469s  OT：0.0078s  带宽：  Recv：1.10M  Send：0.98M | 时间：  0.0468s  OT：0.0109s  带宽：  Recv：869.88kb  Send：955.48kb |  |
|  | 查询方：10w数据提供方：10w | 时间：  离线：70.1015s  在线：0.3727s  带宽：  Send：18.70M  Recv：38.98M | 时间：  0.3614s  OT：0.0077s  带宽：  Recv：9.29M  Send：9.43M | 时间：  0.3637s  OT：0.0109s  带宽：  Recv：8.44M  Send：9.37M |  |
|  |  | 查询方：100w数据提供方：100w | 时间：  离线：70.1017s  在线：4.0558s  带宽：  Send：126.32M  Recv：101.94M | 时间：  3.8195s  OT：0.0079s  带宽：  Recv：96.10M  Send：96.02M | 时间：  3.8584s  OT：0.0109s  带宽：  Recv：85.26M  Send：95.21M |  |
| 业务测试 | 黑名单查询 | 人行作为数据提供方提涉案账户，民丰银行作为查询方提供7天内开卡数据，民丰发起求交任务获取求交结果。  人行端：10312  民丰银行端：765 | 通过，能正确查得结果  时间：  离线：70.1017s  在线：0.0231s  带宽：  Send：7.75M  Recv：12.31M | 时间：  0.0229s  OT：0.0077s  带宽：  Recv：600.87kb  Send：  946.09kb | 时间：  0.0227s  OT：0.0109s  带宽：  Recv：78.90kb  Send：  878.67kb |  |
| 人行作为数据提供方提供高危数据，民丰银行作为查询方提供7天内开卡数据，民丰发起求交任务获取求交结果。  人行端：80261  民丰银行端：765 | 通过，能正确查得结果  时间：  离线：70.1023s  在线：0.0974s  带宽：  Send：20.83M  Recv：17.97M | 时间：  0.0971s  OT：0.0077s  带宽：  Recv：656.59kb  Send：  7.14M | 时间：  0.0958s  OT：0.0110s  带宽：  Recv：139.15kb  Send：  7.07M |  |