保密两方量子比较问题的研究*

刘 文† 王永滨

(中国传媒大学计算机学院,北京 100024)

(2010 年 4 月 16 日收到;2010 年 5 月 31 日收到修改稿)

保密两方比较问题用于两方在不泄漏自己保密数值的前提下判断两数值的大小,但现有的解决方案无法对抗强大的量子攻击. 设计了一个半诚实模型下的基于量子隐式模 $n+1$ 加法保密两方量子比较协议,并且详细地分析了该协议的安全性.

关键词: 保密两方计算, 保密两方比较问题, 量子隐式模 $n+1$ 加法

PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk

1. 引 言

两方保密计算要解决的问题是两个参与方 P_1, P_2 各自有一个秘密输入 x_1, x_2,它们希望在无可信第三方的情况下,保密计算这些秘密输入的一个约定函数 $f(x_1, x_2) = (y_1, y_2)$,参与方 P_1 得到输出 y_1, P_2 得到输出 y_2. 其中保密的含义是指对于任何一个参与方 P_i,除了 x_i 和 y_i 所隐含的信息,P_i 不能得到任何其他信息. 两方保密计算在电子选举、电子投票、电子拍卖、秘密共享、门限签名等场景中有着重要的作用. 一个保密两方计算协议,如果对于拥有无限计算能力的攻击者而言是安全的,则称作是信息论安全的或无条件安全的;如果对于拥有多项式计算能力的攻击者是安全的,则称为是密码学安全的或者条件安全的.

在文献[1]中提出了这样一个问题:两个百万富翁 Alice 和 Bob 想知道他们两个人谁更加富有,但他们都不想让对方知道自己财富的任何信息,这就是百万富翁问题(也称为保密两方比较问题). 保密两方比较问题是保密多方计算中一个基本问题. 近年来人们针对该问题利用传统的经典密码算法设计了各种能够提高效率的协议[2—8]. Cachin 等人[2]基于 ϕ-隐藏假设在茫然第三方的帮助下解决了保密两方比较问题;Lin 等人[3]利用 0,1 编码方案和具有乘法同态性的公钥加密体制提出了一个保密两方比较问题的解决方案;秦波等人[4]也利用公钥同态加密体制设计了一个常数复杂度的保密两方比较协议;Ioannidis 等人[5]利用 2 选 1 的不经意传输 OT_1^2 方案解决保密两方比较问题;李顺东等人[6]将 m 选 1 的不经意传输 OT_1^m 协议和单调不减的函数结合起来设计了一种新的保密比较两个数的大小的方案. 在文献[7,8]中,为了弥补公钥密码体制效率低下的问题提出了基于对称密码体制的保密两方比较大小协议. 然而这些方案(基于公钥密码体制或者基于对称密码体制)在强大的量子计算机面前不堪一击,无法保证安全性.

目前与经典密码学对应的许多方面在量子密码中都得到了研究,例如量子密钥分配协议[9,10],量子认证协议[11,12],量子秘密分享协议[13—16],量子安全多方计算协议[17—21]等. 量子安全多方计算问题首先由在文献[17]中提出来的,接着在文献[18,19]中讨论了量子安全多方计算. Cai 等在量子安全直接通信[20]中给出了隐式模 2 加法的量子算法,Tokunaga 等将量子隐式模 2 加法用在门限量子密码方案[19]中. 杜建忠等人[21]研究了基于量子 Grover 态的保密多方量子隐式模 $n+1$ 加法.

本文也同样致力于研究量子技术在安全多方计算领域的应用,研究在半诚实模型下的基于量子 Grover 态的隐式模 $n+1$ 加法的保密两方比较协议.

* 2009 年北京市文化创意产业发展专项资金项目"数字新媒体内容制作集成运营及监管平台"、国家"211 工程"项目、校级工科规划项目(批准号:XNG0925)资助的课题.

† E-mail:lw8206@gmail.com

该协议是量子技术在安全多方计算领域的应用,该协议克服了原有基于经典密码体制的安全两方比较协议的弱点,可以对抗强大的量子计算机的攻击. 这是量子力学在保密多方计算方向中一个新的尝试.

2. 预备知识

2.1. 量子隐式模 $n+1$ 加法[21]

令 $B^0=\{|i^0\rangle|i=0,1,\cdots,n\}$ 是 $n+1$ 维 Hilbert 空间上一组标准正交基,令 $\alpha=-1+\frac{2}{n+1}$,$\beta=\frac{2}{n+1}$,则 $B^1=\{|i^1\rangle=\alpha|i^0\rangle+\sum_{j=0,j\neq i}^{n}\beta|j^0\rangle,|i=0,1,\cdots,n\}$ 也是 $n+1$ 维 Hilbert 空间上一组标准正交基. 当 $j=i$ 时,$\langle i^0|j^1\rangle=\alpha$;否则 $\langle i^0|j^1\rangle=\beta$. 显然 $\langle i^0|j^1\rangle\neq 0$ 并且 $\langle i^0|j^1\rangle\neq 1$,对于 $i,j=0,1,\cdots,n$ 均成立,$|i^0\rangle$ 和 $|j^1\rangle$ 是非正交态. 算子 V^0 是 $n+1$ 阶单位算子,算子 V^1 为 $n+1$ 阶 Grover 算子:

$$V^0=\begin{bmatrix}1&0&\cdots&0\\0&1&\cdots&0\\\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&1\end{bmatrix},$$

$$V^1=\begin{bmatrix}-1+\frac{2}{n+1}&\frac{2}{n+1}&\cdots&\frac{2}{n+1}\\\frac{2}{n+1}&-1+\frac{2}{n+1}&\cdots&\frac{2}{n+1}\\\vdots&\vdots&\vdots&\vdots\\\frac{2}{n+1}&\frac{2}{n+1}&\cdots&-1+\frac{2}{n+1}\end{bmatrix}.$$

算子 U 为置换算子

$$U=\begin{bmatrix}0&0&\cdots&0&1\\1&0&\cdots&0&0\\0&1&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&\cdots&0&1\end{bmatrix}.$$

有 $V^0|i^0\rangle=|i^0\rangle$,$V^0|i^1\rangle=|i^1\rangle$,$V^1|i^0\rangle=|i^1\rangle$,$V^1|i^1\rangle=|i^0\rangle$,$U|i^0\rangle=|((i+1)\bmod(n+1))^0\rangle$,$U|i^1\rangle=|((i+1)\bmod(n+1))^1\rangle$,$V^1U=UV^1$,这里 $i=0,1,2,\cdots,n$. 这里算子 V^0 和 V^1 决定是否将基向量变换到另外一组向量上,利用非正交态的不可完全区分性实现保密目的. 算子 U 可以在两组不同的基 B^0 和基 B^1 上实现加 1 操作.

2.2. 保密两方计算安全性[22]

半诚实模型:本文方案中所有参与者都是半诚实或诚实的,即在协议的执行过程中,半诚实参与者完全按照协议的要求完成协议的各个步骤,同时可能将自己的所有输入、输出及中间结果泄漏给攻击者.

符号约定:首先我们假设有两个参与方,他们分别为 P_1 和 P_2,要计算的函数为 $f:\{0,1\}^*\times\{0,1\}^*\mapsto\{0,1\}^*\times\{0,1\}^*$,函数 $f(x,y)$ 的第一个元素记为 $f_1(x,y)$,第二个元素记为 $f_2(x,y)$. 计算函数 f 的两方协议为 Π. 运行协议 Π 的过程中 $P_1(P_2)$ 所得的信息记为 $\mathrm{VIEW}_1^{\Pi}(x,y)=(x,r,m_1,\cdots,m_t)$ ($\mathrm{VIEW}_2^{\Pi}(x,y)=(y,r,m_1,\cdots,m_t)$),其中,$r$ 表示 P_1 和 P_2 两方共同产生的随机数,m_i 表示他们接收到的第 i 个信息. 运行协议 Π 后,$P_1(P_2)$ 的输出结果记为 $\mathrm{OUTPUT}_1^{\Pi}(x,y)$ ($\mathrm{OUTPUT}_2^{\Pi}(x,y)$). 显然,$\mathrm{OUTPUT}_1^{\Pi}(x,y)$ 含于 $\mathrm{VIEW}_1^{\Pi}(x,y)$,($\mathrm{OUTPUT}_2^{\Pi}(x,y)$ 含于 $\mathrm{VIEW}_2^{\Pi}(x,y)$).

半诚实模型两方保密计算:对于一个确定的函数 f,我们称 Π 保密计算 f,若存在多项式时间算法(或者模拟器)S_1 和 S_2,使下面两式成立:

$$\begin{aligned}&\{S_1(x,f_1(x,y)),f_2(x,y)\}_{x,y\in\{0,1\}^*,s.t.|x|=|y|}\\&\overset{C}{\equiv}\{\mathrm{VIEW}_1^{\Pi}(x,y),\\&\quad\mathrm{OUTPUT}_2^{\Pi}(x,y)\}_{x,y\in\{0,1\}^*,s.t.|x|=|y|},\end{aligned}\tag{1}$$

$$\begin{aligned}&\{f_1(x,y),S_2(y,f_2(x,y))\}_{x,y\in\{0,1\}^*,s.t.|x|=|y|}\\&\overset{C}{\equiv}\{\mathrm{OUTPUT}_1^{\Pi}(x,y),\\&\quad\mathrm{VIEW}_2^{\Pi}(x,y)\}_{x,y\in\{0,1\}^*,s.t.|x|=|y|},\end{aligned}\tag{2}$$

其中,$\mathrm{VIEW}_1^{\Pi}(x,y)$,$\mathrm{VIEW}_2^{\Pi}(x,y)$,$\mathrm{OUTPUT}_1^{\Pi}(x,y)$ 和 $\mathrm{OUTPUT}_2^{\Pi}(x,y)$ 都是相关的随机变量,$\equiv$ 表示计算上不可区分,则认为 Π 保密地计算 f.

要证明一个两方计算方案是保密的,就必须构造满足(1)和(2)式的模拟器 S_1 和 S_2.

3. 保密两方量子比较协议

假设有两个参与方 P_1,P_2,P_1 拥有一个保密整数 m_1 和 P_2 拥有一个保密整数 m_2(其中 $1\leqslant m_1,m_2\leqslant N$),他们希望在不泄露自己的保密数值的情况下比较两个保密数值的大小. 该协议的执行过程如下:

3.1. P_1, P_2 数据准备阶段

1) P_1 利用自己的保密数值 m_1 (其中 $1 \leqslant m_1 \leqslant N$) 构造一个长度为 N 的向量 $V_1 = (v_1, v_2, \cdots, v_N)$, 构造的方法如下: 当 $1 \leqslant j < m_1$ 时, $v_j = 0$; 当 $m_1 \leqslant j \leqslant N$ 时, $v_j = 1$, 其中 $j = 1, 2, \cdots, N$.

2) P_1 生成一个长度为 N 的随机向量 $R_1 = (r_1^1, r_2^1, \cdots, r_N^1)$, 其中 r_j^1 是随机选择的, $r_j^1 \in \{0, 1\}$, $j = 1, 2, \cdots, N$.

3) P_1 生成 N 个长度为 N 的二元组向量, 每个长度为 N 的二元组向量表示为

$$R_i^{1'} = ((r_1^{i1'}, v_1^{i1'}), (r_2^{i1'}, v_2^{i1'}), \cdots, (r_N^{i1'}, v_N^{i1'})),$$

其中 $r_j^{i1'}, v_j^{i1'}$ 是随机选择的, $r_j^{i1'} \in \{0, 1\}$, $v_j^{i1'} \in \{0, 1, \cdots, n\}$, $i, j = 1, 2, \cdots, N$.

4) P_1 生成 N 个长度为 N_1 的二元组向量, 每个长度为 N_1 的二元组向量表示为

$$R_i^{1''} = ((r_1^{i1''}, v_1^{i1''}), (r_2^{i1''}, v_2^{i1''}), \cdots, (r_{N_1}^{i1''}, v_{N_1}^{i1''})),$$

其中 $r_j^{i1''}, v_j^{i1''}$ 是随机选择的, $r_j^{i1''} \in \{0, 1\}$, $v_j^{i1''} \in \{0, 1, \cdots, n\}$, $i = 1, 2, \cdots, N, j = 1, 2, \cdots, N_1$.

5) P_2 生成一个长度为 N 的二元组向量, 该向量表示为

$$R^{2'} = ((r_1^{2'}, v_1^{2'}), (r_2^{2'}, v_2^{2'}), \cdots, (r_N^{2'}, v_N^{2'})),$$

其中 $r_j^{2'}, v_j^{2'}$ 是随机选择的, $r_j^{2'} \in \{0, 1\}$, $v_j^{2'} \in \{0, 1, \cdots, n\}$, $j = 1, 2, \cdots, N$.

6) P_2 生成一个长度为 N_2 的二元组向量, 长度为 N_2 的二元组向量表示为

$$R^{2''} = ((r_1^{2''}, v_1^{2''}), (r_2^{2''}, v_2^{2''}), \cdots, (r_{N_2}^{2''}, v_{N_2}^{2''})),$$

其中 $r_j^{2''}, v_j^{2''}$ 是随机选择的, $r_j^{2''} \in \{0, 1\}$, $v_j^{2''} \in \{0, 1, \cdots, n\}$, $j = 1, 2, \cdots, N_2$.

7) P_2 生成一个长度为 N_3 的二元组向量, 长度为 N_3 的二元组向量表示为

$$R^{2'''} = ((r_1^{2'''}, v_1^{2'''}), (r_2^{2'''}, v_2^{2'''}), \cdots, (r_{N_3}^{2'''}, v_{N_3}^{2'''})),$$

其中 $r_j^{2'''}, v_j^{2'''}$ 是随机选择的, $r_j^{2'''} \in \{0, 1\}$, $v_j^{2'''} \in \{0, 1, \cdots, n\}$, $j = 1, 2, \cdots, N_3$.

3.2. P_1 预备阶段

1) P_1 利用每个长度为 N 的二元组向量 $R_i^{1'}$ ($i = 1, 2, \cdots, N$) 分别产生一个包含 N 个量子态的序列

$$L_i^{1'} = |(v_1^{i1'})^{r_1^{i1'}}\rangle \otimes |(v_2^{i1'})^{r_2^{i1'}}\rangle \otimes \cdots \otimes |(v_N^{i1'})^{r_N^{i1'}}\rangle,$$

其中每个量子态 $|(v_j^{i1'})^{r_j^{i1'}}\rangle$ ($j = 1, 2, \cdots, N$) 是 B^0, B^1 中的 $2(n+1)$ 个态之一.

2) P_1 利用每个长度为 N_1 的二元组向量 $R_i^{1''}$ ($i = 1, 2, \cdots, N$) 分别产生一个包含 N_1 个量子态的序列

$$L_i^{1''} = |(v_1^{i1''})^{r_1^{i1''}}\rangle \otimes |(v_2^{i1''})^{r_2^{i1''}}\rangle \otimes \cdots \otimes |(v_{N_1}^{i1''})^{r_{N_1}^{i1''}}\rangle,$$

其中每个量子态 $|(v_1^{i1''})^{r_1^{i1''}}\rangle$ ($j = 1, 2, \cdots, N$) 是 B^0, B^1 中的 $2(n+1)$ 个态之一. P_1 将 $L_i^{1''}$ 中的各个量子态, 随机插入序列 $L_i^{1'}$ 中得到的新序列记为 L_i^1, 并记录下 $L_i^{1''}$ 中的各个量子态在 L_i^1 中的位置, 该位置序列记为 P_i^1. P_1 将量子态的序列 $L_1^1, L_2^1, \cdots, L_N^1$ 发送给 P_2.

3) 在确定 P_2 收到所有的量子态序列 $L_1^1, L_2^1, \cdots, L_N^1$ 之后, P_1 公开宣布位置序列 $P_1^1, P_2^1, \cdots, P_N^1$ 和二元组向量 $R_1^{1''}, R_2^{1''}, \cdots, R_N^{1''}$.

3.3. P_2 操作阶段

1) P_2 从收到的量子态序列 $L_1^1, L_2^1, \cdots, L_N^1$ 和公开宣布位置序列 $P_1^1, P_2^1, \cdots, P_N^1$ 和二元组向量 $R_1^{1''}, R_2^{1''}, \cdots, R_N^{1''}$ 中选出第 m_2 列量子态序列 $L_{m_2}^1$、第 m_2 列位置序列 $P_{m_2}^1$ 和第 m_2 个二元组向量 $R_{m_2}^{1''}$. 首先让第 m_2 列量子态序列中所有光子通过特殊滤光器, 通过使用特殊滤光器, 滤掉所有窃听者的不可见光子, 阻止不可见光子进入他的操作系统. 然后他随机选取位置序列 $P_{m_2}^1$ 中 N_1' 个代表位置的数, 按照这 N_1' 个数从量子态序列 $L_{m_2}^1$ 中取出相应位置的量子态作为窃听检查的样品, 从二元组向量 $R_{m_2}^{1''}$ 中取出相应位置的二元组. 用半透半反光子数分裂器 (PNS: 50/50) 来分裂每一个样品光子信号, 随后使用向量 $R_{m_2}^{1''}$ 中对应二元组信息来选用 B^0 或者 B^1 测量每一个分裂后的样本光子信号. 显然, 如果在一个信号中探测到两个或更多的光子, P_2 终止该次量子比较过程, 重新开始. 如果仅测到一个光子, P_2 利用对应二元组中信息与测得光子信息比较, 分析这些样本错误率. 如果错误率高于 P_1, P_2 选定的临界值, 则 P_2 放弃量子通信, 否则进行下步.

2) P_2 抛弃 $L_{m_2}^1$ 中与位置序列 $P_{m_2}^1$ 中相对位置的量子态, 得到量子态序列

$$L_{m_2}^{1'} = |(v_1^{m_2 1'})^{r_1^{m_2 1'}}\rangle \otimes |(v_2^{m_2 1'})^{r_2^{m_2 1'}}\rangle \otimes \cdots \otimes |(v_N^{m_2 1'})^{r_N^{m_2 1'}}\rangle,$$

并对该序列的各个量子态 $j = 1, 2, \cdots, N$ 执行 $v_j^{2'}$ 次 U 操作, 再执行 $V^{r_j^{2'}}$ 操作. P_2 得到的新的量子态序列

表示为

$$L_2' = |((v_1^{m_2 1'} + v_1^{2'}) \bmod (n+1))^{r_1^{m_2 1'} \oplus r^{2'}}\rangle \otimes |(v_2^{m_2 1'} + v_2^{2'}) \bmod (n+1))^{r_2^{m_2 1'} \oplus r_2^{2'}}\rangle \otimes \cdots \otimes |(v_N^{m_2 1'} + v_N^{2'}) \bmod (n+1))^{r_N^{m_2 1'} \oplus r_N^{2'}}\rangle .$$

P_2 利用长度为 N_2 的二元组向量 $R^{2''}$ 产生一个包含 N_2 个量子态的序列

$$L_2'' = |(v_1^{2''})^{r_1^{2''}}\rangle \otimes |(v_2^{2''})^{r_2^{2''}}\rangle \otimes \cdots \otimes |(v_{N_2}^{2''})^{r_{N_2}^{2''}}\rangle,$$

其中每个量子态 $|(v_j^{2''})^{r_j^{2''}}\rangle (j=1,2,\cdots,N)$ 是 B^0, B^1 中的 $2(n+1)$ 个态之一. P_2 将 L_2'' 中的各个量子态，随机插入序列 L_2' 中得到的新序列记为 L_2，并记录下 L_2'' 中的各个量子态在 L_2' 中的位置，该位置序列记为 P^2，P_2 将 L_2 发送给 P_1.

在确定 P_2 收到所有的量子态序列 L_2 之后，P_1 公开宣布位置序列 P^2 和二元组向量 $R^{2''}$.

3.4. P_1 操作阶段

1) P_1 首先让量子态序列 L_2 中所有光子通过特殊滤光器，通过使用特殊滤光器，滤掉所有窃听者的不可见光子，阻止不可见光子进入他的操作系统. 然后他随机选取位置序列 P^2 中 N_2' 个代表位置的数，按照这 N_2' 个数从量子态序列 L_2 中取出相应位置的量子态作为窃听检查的样品，从二元组向量 $R^{2''}$ 中取出相应位置的二元组. 用半透半反光子数分裂器(PNS:50/50)来分裂每一个样品光子信号，随后使用对应二元组中信息来选用 B^0 或者 B^1 测量每一个分裂后的样本光子信号. 显然，如果在一个信号中探测到两个或更多的光子，P_1 终止该次量子比较过程，重新开始. 如果仅测到一个光子，P_1 利用对应二元组中信息与测得光子信息比较，分析这些样本错误率. 如果错误率高于 P_1，P_2 选定的临界值，则 P_2 放弃量子通信，否则进行下步.

2) P_1 抛弃 L_2 中与位置序列 P^2 中相对位置的量子态，得到量子态序列

$$L_2' = |((v_1^{m_2 1'} + v_1^{2'}) \bmod (n+1))^{r_1^{m_2 1'} \oplus r_1^{2'}}\rangle \otimes |((v_2^{m_2 1'} + v_2^{2'}) \bmod (n+1))^{r_2^{m_2 1'} \oplus r_2^{2'}}\rangle \otimes \cdots \otimes |((v_N^{m_2 1'} + v_N^{2'}) \bmod (n+1))^{r_N^{m_2 1'} \oplus r_N^{2'}}\rangle .$$

P_1 对序列 L_2' 的各个量子态 $j=1,2,\cdots,N$ 执行 $(v_j - v_j^{j1'}) \bmod (n+1)$ 次 U 操作，再执行 $V^{j'}$ 操作. P_1 得到的新量子态的序列表示为

$$L_2' = |((v_1^{m_2 1'} + v_1^{2'} + v_1 - v_1^{11'}) \bmod (n+1))^{r_1^{m_2 1'} \oplus r_1^{2'} \oplus r_1^{1'}}\rangle \otimes |(v_2^{m_2 1'} + v_2^{2'} + v_2 - v_2^{21'}) \bmod (n+1))^{r_2^{m_2 1'} \oplus r_2^{2'} \oplus r_2^{1'}}\rangle \otimes \cdots \otimes |(v_N^{m_2 1'} + v_N^{2'} + v_N - v_N^{N1'}) \bmod (n+1))^{r_N^{m_2 1'} \oplus r_N^{2'} \oplus r_N^{1'}}\rangle .$$

P_1 利用长度为 N_3 的二元组向量 $R^{2'''}$ 产生一个包含 N_3 个量子态的序列

$$L_2''' = |(v_1^{2'''})^{r_1^{2'''}}\rangle \otimes |(v_2^{2'''})^{r_2^{2'''}}\rangle \otimes \cdots \otimes |(v_{N_3}^{2'''})^{r_{N_3}^{2'''}}\rangle,$$

其中每个量子态 $|(v_j^{2'''})^{r_j^{2'''}}\rangle (j=1,2,\cdots,N)$ 是 B^0, B^1 中的 $2(n+1)$ 个态之一. P_1 将 L_2''' 中的各个量子态，随机插入序列 L_2' 中得到的新序列记为 L_2，并记录下 L_2''' 中的各个量子态在 L_2' 中的位置，该位置序列记为 $P^{2'}$，P_2 将 L_2 和序列 $(r_1^{m_2 1'} \oplus r_1^{1'}, r_2^{m_2 1'} \oplus r_2^{1'}, \cdots, r_N^{m_2 1'} \oplus r_N^{1'})$ 发送给 P_2.

在确定 P_2 收到所有的量子态序列 L_2 和序列 $(r_1^{m_2 1'} \oplus r_1^{1'}, r_2^{m_2 1'} \oplus r_2^{1'}, \cdots, r_N^{m_2 1'} \oplus r_N^{1'})$ 之后，P_1 公开宣布位置序列 $P^{2'}$ 和二元组向量 $R^{2'''}$.

3.5. P_2 测量结果阶段

1) P_2 首先让量子态序列 L_2 中所有光子通过特殊滤光器，通过使用特殊滤光器，滤掉所有窃听者的不可见光子，阻止不可见光子进入他的操作系统. 然后他随机选取位置序列 $P^{2'}$ 中 N_3' 个代表位置的数，按照这 N_3' 个数从量子态序列 L_2 中取出相应位置的量子态作为窃听检查的样品，从二元组向量 $R^{2'''}$ 中取出相应位置的二元组. 用半透半反光子数分裂器(PNS:50/50)来分裂每一个样品光子信号，随后使用对应二元组中信息来选用 B^0 或者 B^1 测量每一个分裂后的样本光子信号. 显然，如果在一个信号中探测到两个或更多的光子，P_1 终止该次量子比较过程，重新开始. 如果仅测到一个光子，P_1 利用对应二元组中信息与测得光子信息比较，分析这些样本错误率. 如果错误率高于 P_1，P_2 选定的临界值，则 P_2 放弃量子通信，否则进行下步.

2) P_2 抛弃 L_2 中与位置序列 $P^{2'}$ 中相对位置的量子态，得到量子态序列

$$L_2' = |(v_1^{m_2 1'} + v_1^{2'} + v_1 - v_1^{11'}) \bmod (n+1))^{r_1^{m_2 1'} \oplus r_1^{2'} \oplus r_1^{1'}}\rangle \otimes |(v_2^{m_2 1'} + v_2^{2'} + v_2 - v_2^{21'}) \bmod (n+1))^{r_2^{m_2 1'} \oplus r_2^{2'} \oplus r_2^{1'}}\rangle \otimes \cdots \otimes |(v_N^{m_2 1'} + v_N^{2'} + v_N - v_N^{N1'}) \bmod (n$$

$+1))^{r_N^{m_2 1'} \oplus r_N^{2'} \oplus r_N^{1'}}\rangle$.

P_2 取出量子态的序列 L_2' 中的第 m_2 个量子态执行 $(1-v_{m_2}^{2'}) \bmod (n+1)$ 次 U 操作,再执行 $V^{r_{m_2}^{2'}}$ 操作. 此时第 m_2 个量子态可表示为 $|((v_1^{m_2 1'} + v_{m_2}^{2'} + v_{m_2} - v_{m_2}^{m_2 1'} + 1 - v_{m_2}^{2'}) \bmod (n+1))^{r_{m_2}^{m_2 1'} \oplus r_{m_2}^{2'} \oplus r_{m_2}^{1'} \oplus r_{m_2}^{2'}}\rangle$. P_2 用 $B^{r_{m_2}^{m_2 1'} \oplus r_{m_2}^{2'} \oplus r_{m_2}^{1'} \oplus r_{m_2}^{2'}}$ 测量上述量子态,设测得的结果表示为 R:如果 $R=1$,则 P_2 知道 $m_1 > m_2$;如果 $R=2$,则 P_2 知道 $m_1 \leqslant m_2$. P_2 将结果通知 P_1.

4. 安全性分析

定理 1 保密两方量子比较协议判断 m_1 和 m_2 之间的大小关系(其中 $1 \leqslant m_1, m_2 \leqslant N$)在半诚实模型下是安全的.

证明 我们构造两个满足(1),(2)式的模拟器 S_1, S_2 来证明定理 1.

注意在我们设计的协议中 $f_1(f_2)(x,y) = f_1(f_2)(m_1,m_2) = (m_1 \leqslant m_2)$ 或者 $f_1(f_2)(x,y) = f_1(f_2)(m_1,m_2) = (m_1 > m_2)$;$P_1$ 的 view 定义为 $(m_1, r_{P_1}, m_1^{P_1})$,其中 m_1 是 P_1 的输入,r_{P_1} 是 P_1 的内部掷币结果,$m_1^{P_1}$ 是 P_1 在步骤 3.3 之后从 P_2 得到的信息包括量子态序列 L_2、位置序列 P^2 和二元组向量 $R^{2''}$;P_2 的 view 定义为 $(m_2, r_{P_2}, m_1^{P_2}, m_2^{P_2})$,其中 m_2 是 P_2 的输入,r_{P_2} 是 P_2 的内部掷币结果,$m_1^{P_2}$ 是 P_2 在步骤(2)之后从 P_1 得到的信息;$m_2^{P_2}$ 是 P_2 在步骤 3.4 之后从 P_1 得到的信息.

4.1. 模拟器 S_1 利用输入 $(m_1, f_1(m_1,m_2))$ 模拟 P_1 的 view 的执行过程

1)根据 $(m_1, f_1(m_1,m_2))$,S_1 首先随机选择一个整数 m_2' $(1 \leqslant m_2' \leqslant N)$ 满足 $f_1(m_1,m_2') = f_1(m_1,m_2)$,这样如果 $f_1(m_1,m_2) = m_1 \leqslant m_2$,$S_1$ 选择 $m_1 \leqslant m_2'$;否则 S_1 选择 $m_1 > m_2'$.

P_1 生成一个长度为 N 的二元组向量,该向量表示为

$$(R^{2'})' = (((r_1^{2'})', (v_1^{2'})'), ((r_2^{2'})', (v_2^{2'})'), \cdots, ((r_N^{2'})', (v_N^{2'})')),$$

其中 $(r_j^{2'})'$,$(v_j^{2'})'$ 是随机选择的,$(r_j^{2'})' \in \{0,1\}$,$(r_j^{2'})'$,$(v_j^{2'})'$ 是随机选择的,$(r_j^{2'})' \in \{0,1\}$,$(v_j^{2'})' \in \{0,1,\cdots,n\}$,$j=1,2,\cdots,N$.

P_1 生成一个长度为 N_2 的二元组向量,长度为 N_2 的二元组向量表示为

$$(R^{2''})' = (((r_1^{2''})', (v_1^{2''})'), ((r_2^{2''})', (v_2^{2''})'), \cdots, ((r_{N_2}^{2''})', (v_{N_2}^{2''})'),$$

其中 $(r_j^{2''})'$,$(v_j^{2''})'$ 是随机选择的,$(r_j^{2''})' \in \{0,1\}$,$(v_j^{2''})' \in \{0,1,\cdots,n\}$,$j=1,2,\cdots,N_2$;

P_1 生成一个长度为 N_3 的二元组向量,长度为 N_3 的二元组向量表示为

$$(R^{2'''})' = (((r_1^{2'''})', (v_1^{2'''})'), ((r_2^{2'''})', (v_2^{2'''})'), \cdots, ((r_{N_3}^{2'''})', (v_{N_3}^{2'''})')),$$

其中 $(r_j^{2'''})'$,$(v_j^{2'''})'$ 是随机选择的,$(r_j^{2'''})' \in \{0,1\}$,$(v_j^{2'''})' \in \{0,1,\cdots,n\}$,$j=1,2,\cdots,N_3$.

2)P_1 从收到的量子态序列 $L_1^1, L_2^1, \cdots, L_N^1$ 和公开宣布位置序列 $P_1^1, P_2^1, \cdots, P_N^1$ 和二元组向量 $R_1^{1''}, R_2^{1''}, \cdots, R_N^{1''}$ 中选出第 m_2' 列量子态序列 $L_{m_2'}^1$、第 m'_2 列位置序列 $P_{m_2'}^1$ 和第 m_2' 个二元组向量 $R_{m_3'}^{1''}$. P_1 抛弃 $L_{m_2'}^1$ 中与位置序列 $P_{m_2'}^1$ 中相对位置的量子态,得到量子态序列

$$L_{m_2}^{1'} = |(v_1^{m_2 1'})^{r_1^{m_2 1'}}\rangle \otimes |(v_2^{m_2 1'})^{r_2^{m_2 1'}}\rangle \otimes \cdots \otimes |(v_N^{m_2 1'})^{r_N^{m_2 1'}}\rangle,$$

并对该序列的各个量子态 $j=1,2,\cdots,N$ 执行 $(v_j^{2'})'$ 次 U 操作,再执行 $V^{(r_j^{2'})'}$ 操作. P_2 得到的新的量子态序列表示为

$$(L_2')' = |((v_1^{m_2 1'} + (v_1^{2'})') \bmod (n+1))^{r_2^{m_2 1'} \oplus (r_2^{2'})'}\rangle \otimes |(v_2^{m_2 1'} + (v_2^{2'})') \bmod (n+1))^{r_2^{m_2 1'} \oplus (r_2^{2'})'}\rangle \otimes \cdots \otimes |((v_N^{m_2 1'} + (v_N^{2'})') \bmod (n+1))^{r_N^{m_2 1'} \oplus (r_N^{2'})'}\rangle.$$

P_1 利用长度为 N_2 的二元组向量 $(R^{2''})'$ 产生一个包含 N_2 个量子态的序列

$$(L_2'')' = |((v_1^{2''})')^{(r_1^{2''})'}\rangle \otimes |((v_2^{2''})')^{(r_2^{2''})'}\rangle \otimes \cdots \otimes |((v_{N_2}^{2''})')^{(r_{N_2}^{2''})'}\rangle,$$

其中每个量子态 $|((v_j^{2''})')^{(r_j^{2''})'}\rangle$ $(j=1,2,\cdots,N)$ 是 B^0, B^1 中的 $2(n+1)$ 个态之一. P_2 将 $(L_2'')'$ 中的各个量子态,随机插入序列 $(L_2')'$ 中得到的新序列记为 $(L_2)'$,并记录下 $(L_2)'$ 中的各个量子态在 $(L_2)'$ 中的位置,该位置序列记为 $(P^2)'$.

此时

$$S_1(m_1, f_1(m_1,m_2)) = \{m_1, r'_{P_1}, (L_2')', (P^2)', (R^{2''})'\},$$

而

$$\{(L_2')', (P^2)', (R^{2''})'\} \overset{c}{\equiv} \{L_2, P^2, R^{2''}\},$$

可得

$$\{(S_1(m_1, f_1(m_1, m_2)), f_2(m_1, m_2))\}$$
$$\stackrel{c}{\equiv}\{\mathrm{view}_1^{\Pi}(m_1, m_2), \mathrm{output}_2^{\Pi}(m_1, m_2))\}.$$

同理模拟器 S_2 利用输入$(m_2, f_2(m_1, m_2))$模拟 P_2 的 view,可以得到

$$\{(f_1(m_1, m_2), S_2(m_2, f_2(m_1, m_2)))\}$$
$$\stackrel{c}{\equiv}\{\mathrm{output}_1^{\Pi}(m_1, m_2), \mathrm{view}_2^{\Pi}(m_1, m_2))\}.$$

4.2. 补充分析该协议可以对抗的针对量子技术的特有的窃听攻击

4.2.1. 不可见光子攻击和特洛伊马攻击

在我们现有的保密两方量子比较协议中,由于 P_2 在子步骤 3.3 的 1),3.5 的 1),P_1 在子步骤 3.4 的 1)中使用了特殊的滤光器来避免不可见光子进入他们的操作系统,因此窃听者的不可见光子可被这一特殊的滤光器滤掉. 如果窃听者的窃听光子不能被过滤掉,P_1,P_2 的光子探测装置所探测到. 如果窃听者应用特洛伊马攻击,他将在子步骤 3.1 的 1),3.4 的 1)和 3.5 的 1)中被光子束分裂器(PNS:50/50)所探测到. 因此,此协议对不可见光子攻击和特洛伊马攻击时安全的.

4.2.2. 截取-重放攻击

我们现有的保密两方量子比较协议是使用子步骤 3.3 的 1),3.4 的 1)和 3.5 的 1)中的随机抽样来避免截取—重放攻击.

P_1,P_2 发送的量子态序列中每一个量子态随机的出于 B^0 或者 B^1 两组标准正交基之一. 例如在子步骤 3.3 的 1)之前,窃听者如果要采用截取-重放攻击的话,他首先需要猜测量子态序列 $L_1^1, L_2^1, \cdots, L_N^1$ 中 P_2 会选取哪一列量子态序列,其次由于没有二元组向量 $R_{m_2}^{1'}, R_{m_2}^{1''}$ 中的信息,窃听者只能通过猜测的方式重构量子态,这样全部猜测正确的概率为$(1/2nN)^{N+N_1}$. 另外由于样本光子的插入位置和量子态本身的随机性,窃听者仅通过猜测不被检测到的概率为$(1/2nN)^{N'_1}$(如果样本光子数为 N'_1).

可以采用同样的手段分析子步骤 3.4 的 1),3.5 的 1)之前可能出现的截取-重放攻击.

5. 结 论

本文设计了一个半诚实模型下的基于量子隐式模 $n+1$ 加法保密两方量子比较协议,并且详细地分析了该协议的安全性和防量子窃听攻击.

需要指出的是我们所设计的保密两方量子比较协议是基于量子技术的,比目前所有的基于经典密码体制的保密两方比较协议都要安全,可以抵抗强大的量子计算机的攻击.

在以后的工作中,我们希望可以研究出更多的可以对抗强大量子计算机攻击的保密多方计算协议.

[1] Yao A C 1982 *Proceeding of the 23th IEEE Symposium on Foundations of Computer Science* Los Alamitos, CA, November 3—5, 1982 p160

[2] Cachin C 1999 *Proceedings of the 6th ACM Conference on Computer and Communications Security* Kent Ridge Digital Labs, Singapore November 3—5, 1999 p120

[3] Lin H Y, Tzeng W G 2005 *Proceedings of the 4th International Conference on Applied Cryptography and Networks Security* Singapore, June 6—9, 2006 p456

[4] Qin B, Qin H, Zhou K F, Wang X F, Wang Y M 2005 *Journal of Xi'an University of Technology* **21** 149 (in Chinese) [秦 波、秦 慧、周克复、王晓峰、王育民 2005 西安理工大学学报 **21** 149]

[5] Ioannidis I, Grama A 2003 *Proceedings of the 36th Annual Hawaii International Conference on System Sciences* Big Island, HI, USA, January 6—9, 2003 p2005

[6] Li S D, Dai Y Q, You Q Y 2005 *Acta Electronica Sinica* **33** 769 (in Chinese) [李顺东、戴一奇、游启友 2005 电子学报 **33** 769]

[7] Li S D, Wang D S, Dai Y Q, Luo P 2008 *Information Sciences* **178** 244

[8] Li S D, Wang D S, Dai Y Q 2009 *Science in China Series* F: *Information Sciences* **52** 974

[9] Shi B S, Jiang Y K, Guo G C 2000 *Appl. Phys.* B: *Laser Opt.* B **70** 415

[10] Xue P, Li C F, Guo G C 2002 *Phys. Rev.* A **65** 022317

[11] Zhang Y S, Li C F, Guo G C arXIV: quant-Ph/ 0008044

[12] Yang Y G, Wen Q Y, Zhu F C 2005 *Acta Phys. Sin.* **54** 3995 (in Chinese) [杨宇光、温巧燕、朱甫臣 2005 物理学报 **54** 3995]

[13] Chen P, Deng F G, Long G L 2006 *Chin. Phys.* **15** 2228

[14] Yang Y G, Wen Q Y, Zhu F C 2006 *Acta Phys. Sin.* **55** 3255 (in Chinese) [杨宇光、温巧燕、朱甫臣 2006 物理学报 **55** 3255]

[15] Gu B, Li C Q, Xu F, Chen Y L 2009 *Chin. Phys.* B **18** 4690
[16] Wang C, Zhang Y 2009 *Chin. Physi.* B **18** 3238
[17] J. Mueller Quade, H. Imai 2000 quant-ph/0010112
[18] Crepeau C, Gottesman D, Smith A 2002 *Proceedings of 34th Annual ACM Symposium on Theory of Computing* Montréal, Québec, Canada, May 19—21, 2002 p643
[19] Tokunaga Y, Okamoto T, Imoto N 2005 *Phys. Rev.* A **71** 012314
[20] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601
[21] Du J Z, Chen X B, Wen Q Y, Zhu F C 2007 *Acta Phys. Sin.* **56** 6214 (in Chinese) [杜建忠、陈秀波、温巧燕、朱甫臣 2007 物理学报 **56** 6214]
[22] Goldreich O 2004 *Fountions of Cryptography: Basic Applications* (London: Cambridge University Press) p599

Research of secure two-party quantum comparing protocol*

Liu Wen† Wang Yong-Bin
(*School of Computer, Communication University of China, Beijing* 100024, *China*)
(Received 16 April 2010; revised manuscript received 31 May 2010)

Abstract

Secure two-party comparing problem is used to compare two private integer without further leaking of information. But in case of the quantum computer the currently available solutions become useless. A secure two-party quantum comparing protocol in semi-honest model is presented based on the a quantum implicit module $n+1$ addition. The security of the protocol is analyzed.

Keywords: secure two-party computation, secure two-party vector dominance statistic problem, quantum implicit module $n+1$ addition
PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk

* Project supported by the "Digital New Media Content Production, Integration, Operation and Monitoring(2009)" of Beijing Municipal Special Fund for Cultural and Creative Industries; the National "211" Development Fund for Key Engineering Program; the Engineering Course Programming Project of Communication University of China, (Grant No. XNG0925).
† E-mail: lw8206@gmail.com