第 56 卷 第 11 期 2007 年 11 月
1000-3290/2007/56(11)/6214-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.56,No.11,November,2007


# 保密多方量子求和*

杜建忠[1)2)3)†] 陈秀波[1)] 温巧燕[1)] 朱甫臣[4)]

1)(北京邮电大学理学院,北京 100876)

2)(北京科技大学信息工程学院,北京 100083)

3)(西安电子科技大学综合业务网国家重点实验室,西安 710071)

4)(现代通信国家重点实验室,成都 610041)

(2006 年 11 月 9 日收到;2007 年 1 月 23 日收到修改稿)

给出基于非正交态的量子保密模加法方案,允许累加者把一个数保密地累加在一个未知数上.提出的保密多方量子求和方案对于窃取者是渐进安全的,$n-1$ 方的共谋攻击不会使得另一方泄露全部信息.

**关键词**:量子多方计算,Grover 算子,非正交态,量子安全直接通信

**PACC**:0367,0365,0650

## 1. 引 言

在多方联合执行计算的任务中,计算可能发生在互相不信任、甚至互相竞争的多方中,保密每个参与者的输入变得重要.多方计算理论[1-3]使得这种任务被完成成为可能.文献[4—7]讨论了多方保密求和方案:$n$ 个参与者 $P_1,P_2,\cdots,P_n$ 各有一个秘密输入 $x_1,\cdots,x_n$,他们希望计算多元函数 $x_1+x_2+\cdots+x_n$,但不希望泄漏关于 $x_1,\cdots,x_n$ 进一步的信息.多方保密求和已经成为统计分析[6,7]、数据挖掘[8]等多方保密计算问题解决方案的一个基本模块.

对于迄今为止的经典多方保密求和方案[4—7],其技术可以概括为保密传输、显式加法和共享分割.设 Alice 和 $n-1$ 方进行保密求和,Alice 是第 $i$ 个参与者.保密传输的目的是仅仅针对窃取,$n-1$ 方的共谋总可以解密 Alice 传输的全部密文.求和者当然知道自己的加数,在显式加法中,求和者同时可以知道被加数.如果累加由别人完成,Alice 必需将自己的加数明文告诉别人.如果累加由 Alice 完成,Alice 公布和数后,利用减法,$n-1$ 方的共谋可以得到 Alice 的加数.共享分割使得一个加数分割为 $n$ 个共享,确保不能从 $n-1$ 个共享中推断出加数的任何信息.常用方法是将一个加数减去 $n-1$ 个随机数得到差数,这 $n-1$ 个随机数与差数构成 $n$ 个共享,即每个求和者将 $n-1$ 个共享分别传输给其他人,将收到别人共享累加到自己保留的一个共享,然后公布和数,显示加法使得 $n-1$ 方可以算出 Alice 保留的共享.这样的多方保密求和可以经受小于等于 $n-2$ 方的共谋攻击,不能经受 $n-1$ 方的共谋攻击.现有的 $n$ 方保密求和的经典方案中,$n-1$ 方的共谋攻击使得一方泄露全部信息.

多方保密求和方案改进的关键在于本文给出的隐式加法的设计,使得 Alice 可以将自己的加数 $x_i$ 累加到一个未知数上,共谋者不能准确读出和数.这样,Alice 不能知道其他参与者传给他的被加数,其他参与者也不能从和数中准确地得到 $x_i$.

量子力学的不确定原理、不可克隆原理和量子纠缠特性为信息处理提供了新的途径[9—12],也同时为解决经典难题提供了新的途径.Shor 给出多项式时间内的因式分解量子算法[13],Grover 给出 $O(\sqrt{N})$ 时间内的无序搜索量子算法[14],文献[15,16]讨论了量子多方计算.Cai 等在量子安全直接通信中[17]给出隐式模 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[16]中.模 2 加法不能记录进位信息,不能用于

* 国家高技术研究发展计划项目(863 计划)(批准号:2006AA01Z419);国家自然科学基金重大研究项目(批准号:90604023);高等学校博士学科点专项科研基金(批准号:20040013007);现代通信国家重点实验室基金(批准号:9140C1101010601);ISN 开放基金;国家自然科学基金(批准号:60373059)资助的课题.

† E-mail:ddddjjjjzzzz@tom.com

多方求和中.本文中给出基于 Grover 态的隐式模 $n+1$ 加法的量子算法,模 $n+1$ 加法能够记录二进制加法进位信息.

为了清楚地讨论多方求和方案,我们作如下假设：

1)每一方的输入都是一个长度为 $m$ 的二进制随机数.

2)求和的参与人数 $n$ 大于 3 方,每一方都能够正确地执行协议,输入自己的加数.每一方都不会直接地或间接地将自己的输入泄露给共谋的同伴.同时,共谋 $n-1$ 方中不会有人攻击另外一个人.

3)方案中引入一个测量人 $P_1$,为方便有时称为 $P_{n+1}$,只要求他如实地测量和宣布结果,测量人可以和 $n-1$ 方共谋攻击 Alice.

4)量子操作是无错的.量子信道本身不产生差错,但允许受到攻击.经典信道是认证的.

假设 1)使得窃取信息只依赖对求和方案的攻击,假设 2)使得基于加减法规则的平凡攻击不能被利用,假设 3)使得求和有解,引入测量人是为了叙述方便,其中一个参与者可以充当这一角色.假设 4)简化模型.

## 2. 隐式模 $n+1$ 加法

令 $B^0=\{|i^0\rangle \mid i=0,1,2,\cdots,n\}$ 是一组标准正交基,$\alpha=-1+\frac{2}{n+1}$,$\beta=\frac{2}{n+1}$,则 $B^1=\{|i^1\rangle \mid |i^1\rangle=\alpha|i^0\rangle+\sum_{j=0,j\neq i}^{n}\beta|j^0\rangle, i=0,1,2,\cdots,n\}$ 也是一组标准正交基.有 $\langle i^0|j^1\rangle\neq 0$ 并且 $\langle i^0|j^1\rangle\neq 1$ 对于 $i,j=0,1,2,\cdots,n$ 均成立,$|i^0\rangle$ 和 $|i^1\rangle$ 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[14],算子 $U$ 为置换算子 $U|i^0\rangle=|(i+1)^0 \bmod n+1\rangle$.有 $V^0|i^0\rangle=|i^0\rangle$,$V^0|i^1\rangle=|i^1\rangle$,$V^1|i^0\rangle=|i^1\rangle$,$V^1|i^1\rangle=|i^0\rangle$,$U|i^1\rangle=|(i+1)^1 \bmod n+1\rangle$,$V^1U=UV^1$,这里 $i=0,1,2\cdots,n$.

给出 Bob 的加数 $i$ 和 Alice 的加数 $j$ 作隐式模 $n+1$ 加法,$i,j=0,1,2,\cdots,n$.Bob 将 $i$ 随机地编码为量子态 $|i^a\rangle(a=0,1)$ 发送给 Alice.Alice 在量子态上执行 $j$ 次 $U$ 操作,将 $j$ 累加到量子态上.Alice 随机地选择操作 $V^b(b=0,1)$ 作用在量子态上,将量子态传出去.

Alice 累加 $j$ 之前不需要知道 Bob 提供的加数 $i$ 值.如果 Bob 不告诉 Alice 所选择的 $a$ 值,由不确定原理,Alice 不能准确地知道 $i$ 值.同样,只有知道 $a\oplus b$,才能用基 $B^{a\oplus b}$ 准确地测得求和的结果 $i+j \bmod (n+1)$.

## 3. 保密多方量子求和协议

对 $c=1,2,\cdots,n$,令 $x_c=(x^c(1),x^c(2),\cdots,x^c(m))$ 是 $P_c$ 由低位到高位的二进制表示的加数,$P_c$ 作三元组集合 $\{z,w^c(z),x^c(z)\mid z=1,2,\cdots,m,w^c(z)\in\{0,1\}\}$,$w^c(z)$ 表示选择 $V^0$ 或 $V^1$ 操作.$\{w^c(z)\}$ 是随机序列.

对 $c=0,1,2,\cdots,n$,参与方 $P_c$ 作三元组集合 $\{(d,e^c(d),f^c(d))\mid d=1,2,\cdots,m+ngm,e^c(d)\in\{0,1\}f^c(d)\in\{0,1,\cdots,n\}\}$,这里 $d$ 是序号,$e^c(d)$ 表示选择 $V^0$ 或 $V^1$ 操作,$f^c(d)$ 表示累加的数,$\{e^c(d)\}$ 和 $\{f^c(d)\}$ 均是随机序列.$g$ 是一个与控制有关的数,后面详细介绍.

### 3.1. 预备操作

参与方 $P_0$ 产生一个量子态序列,$|F0\rangle=|F(e^0(1),f^0(1))\rangle\otimes\cdots\otimes|F(e^0(d),f^0(d))\rangle\otimes\cdots\otimes|F(e^0(m+ngm),f^0(m+ngm))\rangle$,这里 qudit $|F(e^0(d),f^0(d))\rangle$ 是 $2(n+1)$ 个态之一,$|F(0,0)\rangle=|0^0\rangle$,$|F(0,1)\rangle=|1^0\rangle,\cdots|F(0,n)\rangle=|n^0\rangle$,$|F(1,0)\rangle=|0^1\rangle$,$|F(1,1)\rangle=|1^1\rangle$,$|F(1,n)\rangle=|n^1\rangle$.每个 qudit 的位置 $d$ 称为初始位置.$P_0$ 将 $|F0\rangle$ 传给参与方 $P_1$.

### 3.2. 控制模式

对每个 $c=1,2,\cdots,n$,参与方 $P_c$ 收到 $P_{c-1}$ 的量子态序列,称为 $|Fc\rangle$.

$P_c$ 根据 $|Fc\rangle$ 中每个 qudit 的相对位置,结合前面 $c-1$ 个人宣布的已测量 qudit 初始位置,算出 $|Fc\rangle$ 中每个 qudit 的初始位置.

$P_c$ 的测量操作.$P_c$ 随机地取 $gm$ 个 qudit 准备测量,设这些 qudit 初始位置是 $h_L(L=1,2,\cdots,gm)$,用经典信道给其他 $n$ 方宣布这些初始位置值.$P_c$ 要求前面 $c$ 个参与者 $P_s(s=0,1,\cdots,c-1)$ 宣布 $e^s(h_L)$,$f^s(h_L)$ 的值.$P_c$ 计算

$$e[L]=\bigoplus_{s=0}^{c-1}e^s(h_L),\quad f[L]=\sum_{s=0}^{c-1}f^s(h_L)\bmod(n+1),$$

$\oplus$ 表示模 2 加.用基 $B^{e[L]}$ 投影测量初始位置为 $h_L$ 的 qudit.若有一个测量结果不为为 $f[L]$,认为有窃取者,终止求和.否则,抛弃被测量 qudit,继续执行.

$P_c$ 的演化操作.现在$|Fc\rangle$中有 $m+(n-c)gm$ 个 qudit,设其 qudit 初始位置是 $k_q$($q=1,2,\cdots,m+(n-c)gm$). $P_c$ 在初始位置 $k_q$ 的 qudit 上执行 $f^c(k_q)$次 $U$ 操作,再执行 $V^{e^c(k_q)}$操作. $P_c$ 将演化后的量子态序列传给 $P_{c+1}$.

### 3.3. 消息模式

$P_0$ 收到 $P_n$ 的长度为 $m$ 量子态序列后转发给 $P_1$.每个参与方根据此量子态序列中 qudit 的相对位置,结合所有人宣布的已测量 qudit 初始位置.算出此量子态序列每个 qudit 的初始位置 $y_p$($p=1,2,\cdots,m$).

对每个 $c=1,2,\cdots,n$, $P_c$ 在初始位置为 $y_p$ 的 qudit 上执行 $x^c(p)-f^c(y_p)\bmod n+1$ 次 $U$ 操作,再执行 $V^{w^c(p)}$操作, $P_c$ 将演化后的 qudit 序列传给 $P_{c+1}$.

### 3.4. 测量结果

$P_0$ 收到 $P_n$ 的量子态序列,要求每个 $P_c$ 宣布二元组$(y_p, e^c(y_p)\oplus w^c(p))$的值,这里 $c=1,2,\cdots,n$, $p=1,2,\cdots,m$. $P_0$ 计算 $w[p]=e^0(y_p)\oplus\{\bigoplus_{c=1}^{n}[e^c(y_p)\oplus w^c(p)]\}$,用基 $B^{w[p]}$ 测量初始位置为 $y_p$ 的 qudit,设结果为 $T_p$, $P_0$ 公布 $m$ 个值 $s_p=T_p-f^0(y_p)\bmod n+1$.每一个 $P_c$ 计算$s_1+s_2\cdot 2^1+s_3\cdot 2^2+\cdots+s_m\cdot 2^{m-1}$,得到十进制多方和.

## 4. 协议对窃取者是渐进安全的

为了窃取 Alice 的输入 $x_i$,Eve 必须攻击控制模式和消息模式.消息模式不检测 Eve,我们假设 Eve 可以窃取到所有消息模式信息.把 $x_i$ 看作明文,则 Alice 消息模式的累加数就是 $x_i$ 的密文,控制模式的累加数就是 $x_i$ 的密钥,这是一次密码.我们只考虑控制模式对窃取者是渐进安全的即可.

如果 Eve 没有破坏量子态,对于每个 qudit,Alice 操作前, Eve 的信息熵是 $\log(n+1)$,Alice 操作后, Eve 的信息熵也是 $\log(n+1)$,Eve 没有获得信息.因此,Eve 获得信息量,前提是破坏量子态,这将导致被检测.沿着文献[18,19]中的轮廓但有差异,我们给出证明.

考虑窃取者 Eve 的纠缠攻击.Eve 在第 $i-1$ 参与者和第 $i$ 个参与者 Alice 之间的量子信道上,让传输量子态和他的辅助态$|\varepsilon\rangle$发生纠缠.我们写出 Eve 最一般的纠缠操作

$$|i^0\rangle|\varepsilon\rangle\rightarrow a_{i0}|0^0\rangle|\varepsilon_{i0}\rangle+a_{i1}|1^0\rangle|\varepsilon_{i1}\rangle+\cdots+a_{in}|n^0\rangle|\varepsilon_{in}\rangle,$$

$a_{ij}$为实数,$i,j=1,2,\cdots,n$.同样的纠缠操作使得

$$\begin{aligned}|i^1\rangle|\varepsilon\rangle\rightarrow\sum_{j=0}^{n}|j^1\rangle[&\alpha^2 a_{ij}|\varepsilon_{ij}\rangle\\&+\alpha\beta\sum_{k=0,k\neq i}^{n}a_{kj}|\varepsilon_{kj}\rangle\\&+\alpha\beta\sum_{k=0,k\neq j}^{n}a_{ik}|\varepsilon_{ik}\rangle\\&+\beta^2\sum_{p=0,p\neq i}^{n}\sum_{q=0,q\neq j}^{n}a_{pq}|\varepsilon_{pq}\rangle].\end{aligned}$$

辅助态$|\varepsilon_{ij}\rangle$是规一的,$a_{ij}$是实数.不失一般性[18],可设$\langle\varepsilon_{ij}|\varepsilon_{ik}\rangle=\delta_{jk}$,$\langle\varepsilon_{ji}|\varepsilon_{ki}\rangle=\delta_{jk}$, $i,j,k=0,1,\cdots,n$.幺正性条件要求 $a_{i0}^2+a_{i1}^2+\cdots+a_{in}^2=1$.

Eve 逃避检测的概率是

$$\begin{aligned}P_{nd}=&\frac{1}{2(n+1)}\Big(\sum_{i=0}^{n}a_{ii}^2\Big)\\&+\frac{1}{2(n+1)}\Big[\Big(\sum_{i=0}^{n}\alpha^2 a_{ii}\langle\varepsilon_{ii}|+\alpha\beta\sum_{k=0,k\neq i}^{n}a_{ki}\langle\varepsilon_{ki}|\\&+\alpha\beta\sum_{k=0,k\neq i}^{n}a_{ik}\langle\varepsilon_{ik}|+\beta^2\sum_{p=0,p\neq i}^{n}\sum_{q=0,q\neq i}^{n}a_{pq}\langle\varepsilon_{pq}|\Big)\\&\Big(\sum_{i=0}^{n}\alpha^2 a_{ii}|\varepsilon_{ii}\rangle+\alpha\beta\sum_{k=0,k\neq i}^{n}a_{ki}|\varepsilon_{ki}\rangle\\&+\alpha\beta\sum_{k=0,k\neq i}^{n}a_{ik}|\varepsilon_{ik}\rangle\\&+\beta^2\sum_{p=0,p\neq i}^{n}\sum_{q=0,q\neq i}^{n}a_{pq}|\varepsilon_{pq}\rangle\Big)\Big].\end{aligned}$$

利用条件极值可知,只有在 $a_{ij}=\delta_{ij}$下, $P_{nd}$才可能取得最大值,这样

$$|i^0\rangle|\varepsilon\rangle\rightarrow|i^0\rangle|\varepsilon_i\rangle.$$

因为每个参与者的输入是二进制信息,窃取者只需知道每种模式下 Alice 累加数的奇偶即可,我们可设

$$|i^0\rangle|\varepsilon\rangle\rightarrow|i^0\rangle|\varepsilon_0\rangle,\ i\text{ 为奇数},$$

$$|i^0\rangle|\varepsilon\rangle\rightarrow|i^0\rangle|\varepsilon_1\rangle,\ i\text{ 为偶数}.$$

Eve 被检测的概率是

$$P_d=\frac{2n(-2+n+n^2)}{(1+n)^4}(1-\cos x),\ n\text{ 为偶数},$$

$$P_d=\frac{2(-1+n)}{(1+n)^2}(1-\cos x),\ n\text{ 为奇数}.$$

这里,精心选择$|\varepsilon_0\rangle$和$|\varepsilon_1\rangle$使得

$\langle\varepsilon_0|\varepsilon_1\rangle=\langle\varepsilon_1|\varepsilon_0\rangle=\cos x, 0\leqslant x\leqslant\pi/2$.

因为从两个随机数的和不能推断出加数的任何信息，所以当 Eve 逃避 Alice 的检测，在下一个参与者累加之前，他必须测量通信者载体粒子和辅助粒子．用基 $B^0=\{|i^0\rangle|i=0,1,2,\cdots,n\}$ 测量载体粒子是最自然的选择．根据量子态认证理论[20,21]，可以构造一组 POVM 操作 $\{E_0,E_1,E_2\}$ 测量辅助态，测量 $|\varepsilon_0\rangle(|\varepsilon_1\rangle)$ 依最大概率 $1-\cos x$ 获得测量结果 0 (1)，依概率 $\cos x$ 获得测量结果 2.

为计算 Eve 和 Alice 的互信息 $I(x;y)$，需要计算概率 $p(x,y)$，令 $z$ 表示载体粒子测量结果，$w$ 表示辅助粒子测量结果，$x=0(1)$ 表示 Alice 作了偶数(奇数)次加 1 操作，$y=0$ 表示 $z$ 为偶数并且 $w$ 为 0，或者 $z$ 为奇数并且 $w$ 为 1，$y=1$ 表示 $z$ 为偶数并且 $w$ 为 1，或者 $z$ 为奇数并且 $w$ 为 0，$y=2$ 表示 $w$ 为 2．我们以 $n$ 为奇数时 Alice 前面一个参与者发送 $|0^1\rangle$ 并且 Alice 累加 0 为例给出 $p(x,y)$ 的计算方法．Eve 纠缠后，系统态为 $(\alpha|0^0\rangle+\beta|2^0\rangle+\cdots+\beta|(n-1)^0\rangle)|E_0\rangle+(\beta|1^0\rangle+\beta|3^0\rangle+\cdots+\beta|n^0\rangle)|E_1\rangle$．Alice 执行操作 $V^0$ 累加 0 后，Eve 测量，以概率 $\alpha^2+\frac{n-1}{2}\beta^2(1-\cos x)$ 测得 $z$ 为偶数并且 $w$ 为 0，以 $\frac{n+1}{2}\beta^2(1-\cos x)$ 测得 $z$ 为奇数并且 $w$ 为 1，以 $\cos x$ 测得 $w$ 为 2，因此有 $P(0,0)=1-\cos x$，$P(0,2)=\cos x$．Alice 执行操作 $V^1$ 累加 0 后，系统态为

$$\begin{aligned}&(\alpha|0^1\rangle+\beta|2^1\rangle+\cdots+\beta|(n-1)^1\rangle)|E_0\rangle\\&+(\beta|1^1\rangle+\beta|3^1\rangle+\cdots+\beta|n^1\rangle)|E_1\rangle\\=&\Big[\Big(\alpha^2+\frac{n-1}{2}\beta^2\Big)|0^0\rangle\\&+\Big(2\alpha\beta+\frac{n-3}{2}\beta^2\Big)(|2^0\rangle+|4^0\rangle\\&+\cdots+|(n-1)^0\rangle)\\&+\Big(\alpha\beta+\frac{n-1}{2}\beta^2\Big)(|1^0\rangle+|3^0\rangle\\&+\cdots+|n^0\rangle)\Big]|E^0\rangle\\&+\Big[\frac{n+1}{2}\beta^2(|0^0\rangle+|2^0\rangle+\cdots+|(n-1)^0\rangle)\\&+\Big(\alpha\beta+\frac{n-1}{2}\beta^2\Big)(|1^0\rangle+|3^0\rangle\\&+\cdots+|n^0\rangle)\Big]|E^1\rangle.\end{aligned}$$

Eve 执行测量操作，以概率

$$\Big[\Big(\alpha^2+\frac{n-1}{2}\beta^2\Big)^2+\frac{n-1}{2}\Big(2\alpha\beta+\frac{n-3}{2}\beta^2\Big)^2\Big](1-\cos x)$$

测得 $z$ 为偶数并且 $w$ 为 0，以

$$\frac{n+1}{2}\Big(\alpha\beta+\frac{n-1}{2}\beta^2\Big)^2(1-\cos x)$$

测得 $z$ 为奇数并且 $w$ 为 0，以

$$\frac{n+1}{2}\Big(\frac{n+1}{2}\beta^2\Big)^2(1-\cos x)$$

测得 $z$ 为偶数并且 $w$ 为 1，以概率

$$\Big[\frac{n+1}{2}\Big(\alpha\beta+\frac{n-1}{2}\beta^2\Big)^2\Big](1-\cos x)$$

测得 $z$ 为奇数并且 $w$ 为 1，以 $\cos x$ 测得 $w$ 为 2，因此有

$$\begin{aligned}P(0,0)&=\frac{-1+n}{1+n}(1-\cos x),\\P(0,1)&=\frac{2}{1+n}(1-\cos x),\\P(0,2)&=\cos x.\end{aligned}$$

依据这种计算方法，可以计算 Alice 前面参与者发送任一态并且 Alice 累加任意数对应的 $p(x,y)$．利用全概率公式，可得 $n$ 为奇数时有

$$\begin{aligned}p(0,0)&=\Big(\frac{1}{2}-\frac{1}{2(n+1)}\Big)(1-\cos x),\\p(0,1)&=\frac{1}{2(n+1)}(1-\cos x),\\p(0,2)&=\frac{1}{2}\cos x,\\p(1,0)&=\frac{1}{2(n+1)}(1-\cos x),\\p(1,1)&=\Big(\frac{1}{2}-\frac{1}{2(n+1)}\Big)(1-\cos x),\\p(1,2)&=\frac{1}{2}\cos x,\end{aligned}$$

互信息 $I(\text{Alice};\text{Eve})$ 为

$$(1-\cos x)\Big(1-H\Big(1-\frac{1}{n+1},\frac{1}{n+1}\Big)\Big).$$

$n$ 为偶数时，为了简便运算，我们假设 Eve 可以区分态 $|(0+0)^0\rangle$ 和态 $|(n+1)^0\rangle$，放大了 Eve 的窃取能力，有

$$\begin{aligned}p(0,0)&=\Big(\frac{1}{2}-\frac{n}{2(n+1)^2}\Big)(1-\cos x),\\p(0,1)&=\frac{n}{2(n+1)^2}(1-\cos x),\\p(0,2)&=\frac{1}{2}\cos x,\\p(1,0)&=\frac{n}{2(n+1)^2}(1-\cos x),\\p(1,1)&=\Big(\frac{1}{2}-\frac{n}{2(n+1)^2}\Big)(1-\cos x),\end{aligned}$$

$$p(1,2) = \frac{1}{2}\cos x,$$

互信息 $I$(Alice ;Eve)为

$$(1-\cos x)\left(1 - H\left(1 - \frac{n}{(n+1)^2}, \frac{n}{(n+1)^2}\right)\right).$$

纠缠和测量操作引入的错误会进一步扩散到随后量子态序列,会被随后的其他参与者检测.因此,Eve 攻击第 $n$ 个参与者被检测的概率最低.对于第 $n$ 个参与者,他的量子态序列中每一个量子被当作控制量子的概率是 $g/(1+g)$.根据量子安全直接通信理论[22,23],本协议对于窃取者是渐进安全的.

## 5. $n-1$ 方参与者的共谋攻击不会使得一方泄露全部信息

设 $n-1$ 方参与者共谋攻击 Alice. $n-1$ 方传送给 Alice 合法量子,共谋攻击不会被检测,但量子态的非正交性保证不会使得 Alice 信息全部泄露. $n-1$方必需测量量子才能得到信息,测量的时机应在 Alice 操作之后,否则 Alice 的加数和其他参与者的加数累加后,因其他参与者不会泄露加数,而不能从和中计算出 Alice 加数.用基 $B^0 = \{|i^0\rangle \mid i = 0,1,2,\cdots,n\}$ 测量载体粒子是最自然的选择.

考虑 $n-1$ 方的共谋攻击获得的信息量,$n$ 为奇数时有

$$p(0,0) = \frac{n}{2(n+1)},$$

$$p(0,1) = \frac{1}{2(n+1)},$$

$$p(1,0) = \frac{1}{2(n+1)},$$

$$p(1,1) = \frac{n}{2(n+1)},$$

互信息 $I$(Alice ;$n-1$ 方共谋者)为

$$1 - H\left(1 - \frac{1}{n+1}, \frac{1}{n+1}\right);$$

$n$ 为偶数时有

$$p(0,0) = \frac{1+n+n^2}{2(n+1)^2},$$

$$p(0,1) = \frac{n}{2(n+1)^2},$$

$$p(1,0) = \frac{n}{2(n+1)^2}(1-\cos x),$$

$$p(1,1) = \frac{1+n+n^2}{2(n+1)^2},$$

互信息 $I$(Alice ;$n-1$ 方共谋者)为

$$1 - H\left(1 - \frac{n}{(n+1)^2}, \frac{n}{(n+1)^2}\right).$$

这里 $p(x,y)$的意义是 :$x=0(1)$表示 Alice 作了偶数(奇数)次加 1 操作,$y=0(1)$表示 $n-1$ 方参与者利用测量结果推测 Alice 作了偶数(奇数)次加 1 操作.

## 6. 结论与讨论

我们给出一种量子保密加法,累加者可以把一个数保密地累加在一个未知数上.我们提出保密多方量子求和方案,$n-1$ 方参与者的共谋攻击不会使得一方泄露全部信息,同时对于窃取者是渐进安全的.

当 $n$ 较小时,窃取者逃避检测后获得的信息量较小,$n-1$ 方的共谋攻击获得信息量也较小.特别地,当 $n=4$ 时,Alice 测量一个粒子,Eve 被发现的概率是 $144(1-\cos x)/625$.一旦逃避检测,在一个二进制比特上互信息 $I$(Alice ;Eve) $= 0.36569(1-\cos x)$ 比特. $n-1$ 方的共谋攻击在一个二进制比特上获得的信息量是 0.36569 比特.当 $n=5$ 时,Alice 测量一个粒子,Eve 被发现的概率是 $2(1-\cos x)/9$.一旦逃避检测,在一个二进制比特上互信息 $I$(Alice ;Eve) $=0.35(1-\cos x)$ 比特. $n-1$ 方的共谋攻击在一个二进制比特上获得的信息量是 0.35 比特.

当 $n$ 趋于无穷大时,Alice 测量一个粒子,Eve 被发现的概率是 $O(1/n)$,协议仍然可以对窃取者渐进安全,只是 $g$ 的取值为 $O(n)$.一旦逃避检测,在一个二进制比特上互信息 $I$(Alice ;Eve)趋向 $1-\cos x$ 比特.而 $n-1$ 方的共谋攻击在一个二进制比特上获得的信息量趋向 1 比特,不能有效地抵御 $n-1$ 方的共谋攻击.

当 $n$ 较小时,参与者遭受 $n-1$ 方的共谋攻击的可能性较大,本方案可以被利用.当 $n$ 较大时,参与者遭受 $n-1$ 方共谋攻击的可能性变小,基于共享分割的经典方案可以被利用,它可以抵御小于等于 $n-2$ 方的共谋攻击.

一个公开问题是当 $n$ 趋于无穷大时,是否可以构造更为安全的保密多方量子求和算法.一个思路是找两组可以作隐式加法的标准正交基 $\{|i^0\rangle \mid i = 0,1,2,\cdots,n\}$ 和 $\{|i^1\rangle \mid i = 0,1,2,\cdots,n\}$,使得 $|i^1\rangle = \sum_{j=0}^{n} \alpha_{ij} |i^0\rangle$ 中 $|\alpha_{ij}|$ 均接近于 $1/\sqrt{n+1}$.

[1] Yao A C 1982 *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science* (Chicago: IEEE Computer Society Press) p160

[2] Goldreich O, Micali S, Wigderson A 1987 *Proceedings of the 19th annual ACM symposium on Theory of Computing* (New York: ACM Press) p218

[3] Goldwasser S 1997 *Proceedings of the 16th annual ACM symposium on Principles of distributed computing* (New York: ACM Press) p2

[4] Benaloh J 1987 *Advances in Cryptology, Proceedings of CRYPTO '86* (New York: Springer-Verlag) p251

[5] Schneier B 1996 *Applied Cryptography Second Edition* (New York: John Wiley & Sons) p94

[6] Sanil A P, Karr A F, Lin X, Reiter J P 2004 *Proceedings of the 2004 ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (New York: ACM Press) p677

[7] Atallah M, Bykova M, Li J, Frikken K, Topkara M 2004 *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society* (New York: ACM Press) p103

[8] Kantarcioglu M, Clifton C 2004 *IEEE Transactions on Knowledge and Data Engineering* 16 1026

[9] Song K H 2005 *Acta Phys. Sin.* **54** 4730 (in Chinese) [宋克慧 2005 **物理学报 54** 4730]

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

[11] Chen X Bo, Wen Q Y, Zhu F C 2006 *Chin. Phys.* **15** 2240

[12] Guo F Z, Gao F, Wen Q Y, Zhu F C 2006 *Chin. Phys.* **15** 1690

[13] Shor P W 1994 *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (Los Alamitos: IEEE Computer Society Press) p124

[14] Grover L 1997 *Phys. Rev. Lett.* **79** p325

[15] Crepeau C, Gottesman D, Smith A 2002 *Proceedings of 34th Annual ACM Symposium on Theory of Computing* (Montreal: ACM press) p643

[16] Tokunaga Y, Okamoto T, Imoto N 2005 *Phys. Rev.* A **71** 012314

[17] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601

[18] Gisin N, Ribordy G, Tittel W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[19] Lucamarini M, Mancini S 2005 *Phys. Rev. Lett.* **94** 140501

[20] Duan L M, Guo G C 1998 *Phys. Rev. Lett.* **80** 4999

[21] Nielsen M A, ChuangI L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) p90

[22] Boström K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[23] Deng F G, Long G L, Liu X S 2003 *Phys. Rev.* A **68** 042317

# Secure multiparty quantum summation *

Du Jian-Zhong[1)2)3)†] Chen Xiu-Bo[1)] Wen Qiao-Yan[1)] Zhu Fu-Chen[4)]

1) (*School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

2) (*School of Information Engineering, University of Science & Technology Beijing, Beijing* 100083, *China*)

3) (*State Key Laboratory of Integrated Services Network, Xidian University, Xi'an* 710071, *China*)

4) (*National Laboratory for Modern Communications, Chengdu* 610041, *China*)

(received 9 November 2006; revised manuscript received 23 January 2007)

Abstract

A novel scheme of secure quantum addition module $n+1$ ($n \geqslant 2$) is proposed, based on non-orthogonal states, which allows a number to be added to an unknown number secretly. A proposed protocol for secure $n$-parity quantum summation is quasisecure to Eve. The collusive attack performed by $n$-1 legitimate participators cannot eavesdrop all the input information of the other participator in the protocol.

**Keywords**: secure multiparty quantum computation, Grover operator, non-orthogonal states, secure direction quantum communication

**PACC**: 0367, 0365, 0650

* Project supported by the National High Technology Research and Development Program of China (Grant No. 2006AA01Z419); the Major Research Plan of the National Natural Science Foundation of China (Grant No. 90604023); the National Research Foundation for the Doctoral Program of Higher Education of China (Grant No. 20040013007); the National Laboratory for Modern Communications Science Foundation of China (Grant No. 9140C1101010601); the ISN Open Foundation; and the National Natural Science Foundation of China, (Grant No. 60373059).

† E-mail: ddddjjjjzzzz@tom.com