中国科学 : 物理学 力学 天文学 2023 年 第 53 卷 第 4 期 : 240314
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文

一个高效的量子安全多方计算协议

林崧[1*], 王宁[1,2], 刘晓芬[1]

1. 福建师范大学计算机与网络空间安全学院, 福州 350100;
2. 郑州师范学院信息科学与技术学院, 郑州 450044
*联系人, E-mail: lins95@gmail.com

收稿日期: 2023-01-17; 接受日期: 2023-02-15; 网络出版日期: 2023-03-20
国家自然科学基金(编号: 62171131, 61976053, 61772134)和福建省自然科学基金(编号: 2022J01186)资助

摘要 安全多方计算是一类重要的密码原语, 在电子投票、数据挖掘、区块链、云计算等领域有着广泛的应用. 本文利用量子纠缠特性和欧拉定理, 提出了一个高效的量子安全多方计算协议. 协议中, 所有参与方在一个半可信第三方的帮助下实现多元多项式函数的安全计算. 性能分析表明该协议是正确的, 并且可以抵抗一些常见的外部和内部攻击. 此外, 本文所提协议不仅可提高粒子的检测效率, 还能有效降低协议所需的通信复杂度.

关键词 量子密码, 量子安全多方计算, 欧拉定理, 多项式函数

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud

1 引言

作为20世纪最重要的物理学成就之一, 量子力学理论极大地拓展和改变了人们认识世界的角度和方式, 信息安全领域也不例外. 量子密码是利用量子力学的基本原理建立了一种新的密码系统, 具有理论上的无条件安全. 自从1984年Bennett和Brassard [1]的开创性工作以来, 经过30年的研究, 量子密码在理论和实验方面均取得了长足的进展, 已成为量子信息领域的一个主要研究分支[2,3]. 安全多方计算(Secure Multiparty Computation, SMC)是密码学中最常见和最重要的问题之一, 它允许两个或多个参与者合作计算相关函数, 而不向对方透露各自的私有输入信息, 最终输出计算结果. 第一个有两个参与者的SMC协议是由Yao [4]于1982年提出的, 被称为百万富翁问题. 后来, Goldreich等人[5]将该问题扩展到具有n个参与者的场景中. 目前, 安全多方计算被广泛应用于电子交易、信息检索、数据挖掘等领域. 然而, 随着量子计算的发展, 基于计算复杂度的SMC协议的安全性受到了极大的挑战. 量子安全多方计算(Secure Multiparty Quantum Computation, SMQC) [6–8]是SMC在量子领域的扩展, 其克服了SMC在窃听检测方面的安全缺陷, 具有SMC无法达到的优势. 目前, 许多学者对SMQC进行了研究, 并提出了各种各样的SMQC协议来解决一些安全计算问题, 如保密比较[9–11]、保密查询[12–15]、集合计算[16–18]、几何计算[19,20]、多项式计算[21–38]等.

安全多项式计算是安全多方计算中的一个重要研究问题, 它可用来为其他复杂的多方计算构建安全体系, 是一种提供隐私保护的通用密码学原语协议. 2007年, Du 等人[21]提出了一个基于非正交态的量子

引用格式: 林崧, 王宁, 刘晓芬. 一个高效的量子安全多方计算协议. 中国科学: 物理学 力学 天文学, 2023, 53: 240314
Lin S, Wang N, Liu X-F. An efficient secure multiparty quantum computation protocol (in Chinese). Sci Sin-Phys Mech Astron, 2023, 53: 240314, doi: 10.1360/SSPMA-2023-0030

保密模加方案, 该方案允许n个用户把他们各自的私密输入保密地累加在一个未知数上, 并实现渐进安全. 随后, 人们利用不同量子特性设计了一些巧妙的量子安全多方求和协议[22–31]. 2013年, Li等人[32]基于纠缠态的量子相关性提出了一个SMQC协议, 该协议需要在第三方的协助下完成布尔函数的计算. 2016年, Shi等人[33]提出两个SMQC协议, 这些协议利用量子傅里叶变换、受控非(CNOT)门和oracle算子分别实现了模d的加法和乘法运算. 随后, 他们提出了一种适用于单边安全的两方经典计算的通用量子协议[34]. 2017年, Clementi等人[36]提出了一个计算非线性多变量函数的协议, 该协议通过线性经典计算和有限的量子操作实现一个特定布尔函数的计算. 然而, 该协议处于2维希尔伯特空间上, 存在一定的局限性. 最近, 利用相互无偏基(Mutually Unbiased Bases, MUBs)以及纠缠态, Lu等人[37]分别设计了两个计算多变量函数的协议, 这两个协议实现了有限域GF(d)上的加法和乘法运算.

受这些研究成果的启发, 本文提出了一个高效的量子安全多方计算协议. 协议中, n个参与者在一个半可信第三方的协助下完成对一个n元多项式函数的安全计算. 这里, 通过构造两个幺正操作实现GF(d)上的加减运算, 并将信息粒子和检测粒子纠缠起来达到窃听检测目的. 为了实现GF(d)上的乘法和除法运算, 利用欧拉定理设计另外两个存在对易关系的幺正操作, 进而实现多项式的四则运算. 由于协议中用d级粒子作为信息粒子来嵌入秘密输入, 而用2级粒子作为检测粒子进行窃听检测, 因此本文所提协议具有较高的检测效率.

2 n元多项式函数

在本节中, 对本文的研究对象, n元多项式函数, 进行简要介绍. 它是一个有限域GF(d)= $\{0,1,...,d-1\}$ (d为素数)上的一个带n个变量的多项式函数$f(x_1,x_2,\cdots,x_n)$, 为GF$(d)^n \to$ GF(d)上的一个映射. 这里, 多项式$f(\cdot)$只涉及n个变量的四则运算. 这就意味着, 要计算多项式$f(\cdot)$ 就要实现GF(d)域上的模d加、减、乘、除四个运算, 本文分别用$\oplus,\ominus,\odot,\oslash$四个符号来标记.

另外, 不失一般性, 我们可设该多项式由一个线性单项$\bar{f}(\cdot)$和m个非线性单项$\tilde{f}_i(\cdot)$ $(i=1,2,\cdots,m)$组成, 即$f(\cdot)=\bar{f}(\cdot)\oplus\sum_{i=1}^{m}\tilde{f}_i(\cdot)$. 例如, 有限域GF(7)上一个三元多项式$f(x_1,x_2,x_3)=x_1\ominus x_2\oplus x_3\oplus x_1\odot x_2\oplus x_2\oslash x_3$. 它是由一个线性单项$\bar{f}(x_1,x_2,x_3)=x_1\ominus x_2\oplus x_3$和两个非线性单项组, $\tilde{f}_1(x_1,x_2,x_3)=x_1\odot x_2$和$\tilde{f}_2(x_1,x_2,x_3)=x_2\oslash x_3$组成.

由于减法和除法分别是加法和乘法的逆运算, 因此完成计算任务的关键是实现模d加法和乘法运算. 模d加运算在量子安全多方计算中是比较容易实现的, 目前已取得了一些研究成果, 如一些量子安全多方求和协议[22–26,28–31]. 模d乘运算则比较困难, 现有的一些量子协议大都效率偏低. 这里, 我们结合欧拉定理[39], 将模d乘转换为模$d-1$加(记为$\widehat{\oplus}$)运算来高效解决这一问题. 在数论中, 欧拉定理是一个关于同余的性质, 是费马小定理的加强推广, 具体描述如下. 假设有两个正整数a 和d且满足gcd$(a,d)=1$, 则有: $a^{\varphi(d)}\equiv 1(\mathrm{mod}\ d)$, 其中$\varphi(d)$(称为欧拉函数)表示与$d$互素的且小于$d$的正整数数目. 显然, 当$d$为素数时, $\varphi(d)=d-1$. 另外, 如果d是素数, 则GF$(d)^*$ = GF$(d)-\{0\}=\{1,2,...,d-1\}$对于乘法运算构成一个循环群. 这样, 我们就可在GF$(d)^*$上找到一个生成元g, 使得对于任意一个元素$x\in$ GF$(d)^*$, 存在一个$s\in$ R$(d-1)=\{0,1,\cdots,d-2\}$满足$x=g^s$. 进一步, 当$x_1=g^{s_1}$和$x_2=g^{s_2}$, 那么$x_1\odot x_2=g^{s_1\widehat{\oplus}s_2}$. 这样, 对于GF$(d)^*$上的乘法(除法)就可转换为环R$(d-1)$ 上的模$d-1$加法(减法)运算.

3 四个量子门操作

在本节中, 对本文所提协议所涉及的四个主要量子门操作进行介绍. 这里, 我们在Hilbert空间$\mathrm{H}^2\otimes\mathrm{H}^d$上设计两个特殊的编码操作$E_s$和$\widehat{E}_s$, 来实现上述的模$d$加和模$d-1$加的运算. 此外, 为了粒子传输的安全性, 构造了与这些编码操作可对易的两个置乱操作P_t^q和$\widehat{P}_t^q$.

在一个d级系统H^d中存在一个移位操作, 即$X=\sum_{i=0}^{d-1}|i\oplus 1\rangle\langle i|$, 其中$\oplus$为模$d$ 加. 在此基础上, 可构造一个受控CX操作, 即$CX=|0\rangle\langle 0|\otimes\sum_{i=0}^{d-1}|i\rangle\langle i|+|1\rangle\langle 1|\otimes\sum_{i=0}^{d-1}|i\oplus 1\rangle\langle i|$. 这里, 第一个控制粒子是一个qubit, 第二个目标粒子是一个qudit. 进一步, 就可得到如下3个量子门

操作:

$$X_t = \sum_{i=0}^{d-1} |i \oplus t\rangle\langle i|,$$
$$CX_t^0 = |0\rangle\langle 0| \otimes \sum_{i=0}^{d-1} |i\rangle\langle i| + |1\rangle\langle 1| \otimes \sum_{i=0}^{d-1} |i \oplus t\rangle\langle i|, \quad (1)$$
$$CX_t^1 = |0\rangle\langle 0| \otimes \sum_{i=0}^{d-1} |i \oplus t\rangle\langle i| + |1\rangle\langle 1| \otimes \sum_{i=0}^{d-1} |i\rangle\langle i|.$$

利用这些操作, 我们可构造$H^2 \otimes H^d$空间上的两个幺正操作:

$$E_s = I_2 \otimes X_s,\ P_t^q = CX_t^q (H \otimes I_d). \quad (2)$$

这里, I_2和I_d分别是Hilbert空间H^2和H^d上单位矩阵, $H = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]$是常见的hadamard算子. 经过简单计算可知, 这两个操作是可对易的, 即满足下述条件.

命题1: 若$E_s = I_2 \otimes X_s$, $P_t^q = CX_t^q (H \otimes I_d)$ $(s, t \in \mathrm{GF}(d), q \in \mathrm{GF}(2))$, 则$E_s P_t^q = P_t^q E_s$.

为了在d级系统中实现模$d-1$加运算, 我们构造了一个空间H^d上的幺正操作, $\widehat{X} = \sum_{i=0}^{d-2} |i \widehat{\oplus} 1\rangle\langle i| + |d-1\rangle\langle d-1|$, $\widehat{\oplus}(\widehat{\ominus})$为环R$(d-1)$上的模$d-1$加(减)运算, 进而可以得到相应的三个算子:

$$\widehat{X}_t = \sum_{i=0}^{d-2} |i \widehat{\oplus} t\rangle\langle i| + |d-1\rangle\langle d-1|,$$
$$\widehat{CX}_t^0 = |0\rangle\langle 0| \otimes \sum_{i=0}^{d-1} |i\rangle\langle i| + |1\rangle\langle 1| \otimes \left(\sum_{i=0}^{d-2} |i \widehat{\oplus} t\rangle\langle i| + |d-1\rangle\langle d-1| \right), \quad (3)$$
$$\widehat{CX}_t^1 = |0\rangle\langle 0| \otimes \left(\sum_{i=0}^{d-2} |i \widehat{\oplus} t\rangle\langle i| + |d-1\rangle\langle d-1| \right) + |1\rangle\langle 1| \otimes \sum_{i=0}^{d-1} |i\rangle\langle i|.$$

进而可设计两个编码操作:

$$\widehat{E}_s = I_2 \otimes \widehat{X}_s,\ \widehat{P}_t^q = \widehat{CX}_t^q (H \otimes I_d), \quad (4)$$

并且这两个操作也是可对易的, 即命题2成立.

命题2: 若$\widehat{E}_s = I_2 \otimes \widehat{X}_s$, $\widehat{P}_t^q = \widehat{CX}_t^q (H \otimes I_d)$, 则$\widehat{E}_s \widehat{P}_t^q = \widehat{P}_t^q \widehat{E}_s$.

关于这两个命题的证明, 我们将在附录中给出简要的证明过程. 利用这些量子门操作, 就可实现GF(d)域上的四则运算, 进而设计具体量子密码协议完成对多元多项式的安全计算任务.

4 量子安全多方计算协议

假设有n个参与者Bob$_i$ $(i = 1, 2, \cdots, n)$, 每个参与者分别拥有一个私密输入x_i $(x_i \in \mathrm{GF}(d)^* = \{1, 2, ..., d-1\})$, 其中$d$为素数. 他们希望安全计算出一个GF$(d)$上的多项式$f(x_1, x_2, ..., x_n)$. 这里, $f(x_1, x_2, ..., x_n) = \tilde{f}(x_1, x_2, ..., x_n) + \sum_{i=1}^{m} \tilde{f}_i(x_1, x_2, ..., x_n)$, 即它由一个线性单项$\tilde{f}(\cdot)$和$m$个非线性单项$\tilde{f}_i(\cdot)$组成. 如图 1所示, n个参与者通过执行下述步骤, 就可在一个半可信第三方Alice的帮助下实现这个安全多方计算任务.

(1) **初始化阶段**. n个参与者Bob$_i$事先约定好m个非线性单项$\tilde{f}_i(\cdot)$的计算顺序, 并保证该顺序的私密性. 第三方Alice选择$GF(d)^*$上的一个生成元g, 并公布$d-1$个对应关系$(s, x = g^s)$. 这样, Bob$_i$就可根据该对应关系, 得到他的秘密输入s_i, 满足$x_i = g^{s_i}$.

(2) **非线性单项计算**. n个参与者和Alice执行下述步骤m轮计算出m个非线性单项$\tilde{f}_j(\cdot)$的结果.

在第j轮中$(j = 1, 2, \cdots, m)$, n个参与者计算非线性单项$\tilde{f}_j(x_1, x_2, \cdots, x_n)$. 当该单项包含$x_i$, 则Bob$_i$本轮的输入为$s_i^j = s_i$. 当该单项不包含$x_i$, 则$s_i^j = 0$.

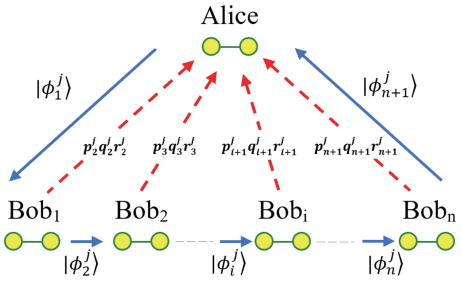

图 1 (网络版彩图) SMQC协议整体通信框架图. 该图中量子通信和经典通信分别用带箭头的实线和虚线来标记, 相连的两个圆表示该协议的信息载体, 即两粒子纠缠态

Figure 1 (Color online) The whole communication framework of the proposed SMQC protocol. In the figure, quantum communication and classical communication are marked with solid lines and dotted lines with arrows respectively, and the two connected circles represent the information carrier of the protocol, namely the two-particle entangled states.

(2.1) Alice制备初始量子态$|0\rangle|p_1^j\rangle$, 其中$p_1^j \in \mathrm{GF}(d)$是一个随机数. 然后, Alice生成两个随机数$q_1^j \in \{0,1\}$和$r_1^j \in \mathrm{GF}(d)^*$, 并根据该比特值对两个信号粒子进行置乱操作$\widehat{P}^{q_1^j}_{r_1^j}$. 最后, Alice将量子态$|\phi_1^j\rangle = \widehat{P}^{q_1^j}_{r_1^j}|0\rangle|p_1^j\rangle$发送给第一个参与者$\mathrm{Bob}_1$.

(2.2) 参与者Bob_1生成三个随机数p_2^j, q_2^j, r_2^j, 其中$p_2^j, r_2^j \in GF(d)^*$ $q_2^j \in GF(2)$. 在收到量子态$|\phi_2^j\rangle$后, Bob_1对两个粒子执行$\widehat{E}_{s_1^j \widehat{\oplus} p_2^j}$操作. 在编码操作后, Bob_1进行置乱操作, 即执行$\widehat{P}^{q_2^j}_{r_2^j}$操作. 最后, 他将量子态$|\phi_2^j\rangle = \widehat{P}^{q_2^j}_{r_2^j}\widehat{E}_{s_1^j \widehat{\oplus} p_2^j}|\phi_1^j\rangle$传给下一个参与者$\mathrm{Bob}_2$.

(2.3) 参与者Bob_i $(i = 2,3,\cdots,n)$执行与步骤(2.2)类似的过程. 具体来讲, 当Bob_i收到信号粒子后, 他对信号粒子先执行编码操作$\widehat{E}_{s_i^j \widehat{\oplus} p_{i+1}^j}$和置乱操作$\widehat{P}^{q_{i+1}^j}_{r_{i+1}^j}$. 然后, 他将量子态$|\phi_{i+1}^j\rangle = \widehat{P}^{q_{i+1}^j}_{r_{i+1}^j}\widehat{E}_{s_i^j \widehat{\oplus} p_{i+1}^j}|\phi_i^j\rangle$给下一个参与者$\mathrm{Bob}_{i+1}$. 这里, 最后一个参与者$\mathrm{Bob}_n$将信号粒子传回给Alice.

(2.4) 当Alice收到量子态$|\phi_{n+1}^j\rangle$后, 她要求n个参与者Bob_i按随机顺序公布他的随机数q_{i+1}^j和r_{i+1}^j. 然后, Alice对量子态$|\phi_{n+1}^j\rangle$执行相应的逆操作, $(\widehat{P}^{q_1^j}_{r_1^j})^{-1}(\widehat{P}^{q_2^j}_{r_2^j})^{-1}\cdots(\widehat{P}^{q_{n+1}^j}_{r_{n+1}^j})^{-1}$. 最后, 她对两个信号粒子分别进行计算基测量, 得到测量结果o_1^j和o_2^j. 经过简单计算可得, 在理想情况下, $o_1^j = 0$并且$o_2^j = (\widehat{\oplus}_{i=1}^{n+1} p_i^j)\widehat{\oplus}(\widehat{\oplus}_{i=1}^{n} s_i^j)$.

(3) **线性单项计算**. 与上述非线性单项计算类似, n个参与者和Alice通过一轮操作计算出线性单项$\tilde{f}(\cdot)$的结果. 不同之处在于, 编码操作(置乱操作)是$E_s(P_t^q)$而不是$\widehat{E}_s(\widehat{P}_t^q)$. 具体来讲, Alice制备量子态$|\phi_1^{m+1}\rangle = P^{q_1^{m+1}}_{r_1^{m+1}}|0\rangle|p_1^{m+1}\rangle$发送给$\mathrm{Bob}_1$. 每个参与者$\mathrm{Bob}_i(i = 1,2,\cdots,n)$在收到信号粒子后, 执行编码操作$E_{x_i \oplus p_{i+1}^{m+1}}$和置乱操作$P^{q_{i+1}^{m+1}}_{r_{i+1}^{m+1}}$, 并将操作后的量子态$|\phi_{i+1}^{m+1}\rangle = P^{q_{i+1}^{m+1}}_{r_{i+1}^{m+1}}E_{x_i \oplus p_{i+1}^{m+1}}|\phi_i^{m+1}\rangle$传给下一个参与者$\mathrm{Bob}_{i+1}$. 当Alice收到传回的量子态$|\phi_{n+1}^{m+1}\rangle$, 她根据参与者公布的随机数对粒子进行逆操作$(P^{q_1^{m+1}}_{r_1^{m+1}})^{-1}(P^{q_2^{m+1}}_{r_2^{m+1}})^{-1}\cdots(P^{q_{n+1}^{m+1}}_{r_{n+1}^{m+1}})^{-1}$. 最后, Alice对两个信号粒子进行计算基测量o_1^{m+1}和o_2^{m+1}.

(4) **窃听检测**. Alice利用$m+1$次的第一个测量结果来计算出错误率. 具体来讲, 若第i轮的第一个测量结果为$|1\rangle$, 则错误计数e加1. 这样就可得到错误率$\varepsilon = \frac{e}{m+1}$. 当错误率超过预先设定的阈值, 所有参与者放弃协议. 否则, Alice公布错误轮次, 所有参与者重新执行相应轮次的步骤.

(5) **公布计算结果**. Alice要求n个参与者Bob_i按随机顺序公布他的随机数串$\{p_{i+1}^1, p_{i+1}^2, \cdots, p_{i+1}^{m+1}\}$. 根据这些公开信息以及第二个测量结果, Alice就可推得所有非线性单项计算结果和线性单项结果. 进而, 她就得到多项式$f(x_1, x_2, ..., x_n)$的计算结果. 最后, Alice将计算结果告诉所有参与者, 这样就完成安全多方计算任务.

接下来, 我们通过一个简单例子来进一步阐述协议的执行过程. 以2.1节描述的例子为例, 三个参与者: Bob_1, Bob_2和Bob_3, 分别拥有秘密输入$x_1 = 2$, $x_2 = 5$和$x_3 = 4$, 他们想安全计算出域GF(7)上的多项式$f(x_1, x_2, x_3) = x_1 \ominus x_2 \oplus x_3 \oplus x_1 \odot x_2 \oplus x_2 \oslash x_3$. 假设Alice选择$\mathrm{GF}(7)^*$上的生成元$g = 5$, 并公布6个对应关系$(0, 1 = 5^0)$, $(1, 5 = 5^1)$, $(2, 4 = 5^2)$, $(3, 6 = 5^3)$, $(4, 2 = 5^4)$, $(5, 3 = 5^5)$. 这样, 三个参与者就可根据该对应关系, 分别得到$s_1 = 4$, $s_2 = 1$和$s_3 = 2$.

在第1轮计算非线性单项$\tilde{f}_1(x_1, x_2, x_3) = x_1 \odot x_2$过程中, 假设Alice和三个参与者的随机数分别为$(p_1^1 = 3, q_1^1 = 0, r_1^1 = 1)$, $(p_2^1 = 4, q_2^1 = 1, r_2^1 = 5)$, $(p_3^1 = 0, q_3^1 = 1, r_3^1 = 0)$, $(p_4^1 = 5, q_4^1 = 0, r_4^1 = 2)$. 首先, Alice制备两个信号粒子处于量子态$|\phi_1^1\rangle = \widehat{P}_1^0|0\rangle|p_1^1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|3\rangle + |1\rangle|4\rangle)$, 并将其传给$\mathrm{Bob}_1$. Bob_1执行他的编码操作$\widehat{E}_{s_1^1 \widehat{\oplus} p_2^1}$ $(s_1^1 = s_1 = 4)$和置乱操作$\widehat{P}^{q_2^1}_{r_2^1}$, 得到量子态$|\phi_2^1\rangle = \widehat{P}_5^1\widehat{E}_2|\phi_1^1\rangle = \frac{1}{2}(|0\rangle|4\rangle + |1\rangle|5\rangle + |0\rangle|5\rangle - |1\rangle|0\rangle)$. 接着, Bob_2执行他的编码操作$\widehat{E}_{s_2^1 \widehat{\oplus} p_3^1}$ $(s_2^1 = s_2 = 1)$和置乱操作$\widehat{P}^{q_3^1}_{r_3^1}$, 得到量子态$|\phi_3^1\rangle = \widehat{P}_0^1\widehat{E}_1|\phi_2^1\rangle = \frac{1}{2\sqrt{2}}(|0\rangle|5\rangle + |1\rangle|5\rangle + 2|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle)$. 然后, Bob_3执行他的编码操作$\widehat{E}_{s_3^1 \widehat{\oplus} p_4^1}$ $(s_3^1 = 0)$和置乱操作$\widehat{P}^{q_4^1}_{r_4^1}$, 得到量子态$|\phi_4^1\rangle = \widehat{P}_2^0\widehat{E}_5|\phi_3^1\rangle = \frac{1}{2}(|0\rangle|4\rangle + |0\rangle|5\rangle + |1\rangle|1\rangle - |1\rangle|2\rangle)$. 最后, Alice对量子态$|\phi_4^1\rangle$执行操作$(\widehat{P}^{q_1^1}_{r_1^1})^{-1}(\widehat{P}^{q_2^1}_{r_2^1})^{-1}(\widehat{P}^{q_3^1}_{r_3^1})^{-1}(\widehat{P}^{q_4^1}_{r_4^1})^{-1}$, 得到量子态$|0\rangle|5\rangle$. 因此, 对这两个粒子进行计算基测量, Alice得到测量结果$o_1^1 = 0$和$o_2^1 = 5$, 进而推得$\tilde{f}_1(x_1, x_2, x_3) = 5^{o_2^1 \ominus (\widehat{\oplus}_{i=0}^{3} p_i^1)} = 3$.

在第2轮计算非线性单项$\tilde{f}_2(x_1, x_2, x_3) = x_2 \oslash x_3 = x_2 \odot (x_3)^{-1}$过程中, Alice和三个参与者的随机数分别为$(p_1^2 = 2, q_1^2 = 1, r_1^2 = 1)$, $(p_2^2 = 3, q_2^2 = 0, r_2^2 = 1)$, $(p_3^2 = 1, q_3^2 = 1, r_3^2 = 4)$, $(p_4^2 = 2, q_4^2 = 0, r_4^2 = 3)$. 最后, Alice根据测量结果推得$\tilde{f}_2(x_1, x_2, x_3) = 3$, 具体过程请见表1.

表 1 一个三方量子安全计算例子

Table 1 An example of the three-party quantum security computation

	第1轮	第2轮	第3轮
子函数	$\tilde{f}_1(x_1,x_2,x_3)=x_1\odot x_2$	$\tilde{f}_2(x_1,x_2,x_3)=x_2\oslash x_3$	$\bar{f}(x_1,x_2,x_3)=x_1\ominus x_2\oplus x_3$
Alice	$\|\phi_1^1\rangle=\widehat{P}_1^0\|0\rangle\|p_1^1\rangle=\frac{1}{\sqrt{2}}(\|0\rangle\|3\rangle+\|1\rangle\|4\rangle)$	$\|\phi_1^2\rangle=\widehat{P}_1^1\|0\rangle\|p_1^2\rangle=\frac{1}{\sqrt{2}}(\|0\rangle\|3\rangle+\|1\rangle\|2\rangle)$	$\|\phi_1^3\rangle=P_1^0\|0\rangle\|p_1^3\rangle=\frac{1}{\sqrt{2}}(\|0\rangle\|6\rangle+\|1\rangle\|0\rangle)$
Bob_1	$\|\phi_2^1\rangle=\widehat{P}_5^1\widehat{E}_2\|\phi_1^1\rangle=\frac{1}{2}(\|0\rangle\|4\rangle+\|1\rangle\|5\rangle$ $+\|0\rangle\|5\rangle-\|1\rangle\|0\rangle)$	$\|\phi_2^2\rangle=\widehat{P}_1^0\widehat{E}_3\|\phi_1^2\rangle=\frac{1}{2}(\|0\rangle\|0\rangle+\|1\rangle\|1\rangle$ $+\|0\rangle\|5\rangle-\|1\rangle\|0\rangle)$	$\|\phi_2^3\rangle=P_3^0E_4\|\phi_1^3\rangle=\frac{1}{2}(\|0\rangle\|3\rangle+\|1\rangle\|6\rangle$ $+\|0\rangle\|4\rangle-\|1\rangle\|0\rangle)$
Bob_2	$\|\phi_3^1\rangle=\widehat{P}_0^1\widehat{E}_1\|\phi_2^1\rangle=\frac{1}{2\sqrt{2}}(\|0\rangle\|5\rangle+\|1\rangle\|5\rangle$ $+2\|0\rangle\|0\rangle-\|0\rangle\|1\rangle+\|1\rangle\|1\rangle)$	$\|\phi_3^2\rangle=\widehat{P}_4^1\widehat{E}_2\|\phi_2^2\rangle=\frac{1}{2\sqrt{2}}(2\|1\rangle\|2\rangle+\|0\rangle\|1\rangle$ $-\|1\rangle\|3\rangle+\|0\rangle\|5\rangle+\|1\rangle\|1\rangle)$	$\|\phi_3^3\rangle=P_1^1E_6\|\phi_2^3\rangle=\frac{1}{2\sqrt{2}}(\|0\rangle\|3\rangle+\|1\rangle\|2\rangle$ $+\|0\rangle\|6\rangle-\|1\rangle\|5\rangle+\|0\rangle\|4\rangle+\|1\rangle\|3\rangle-\|0\rangle\|0\rangle$ $+\|1\rangle\|6\rangle)$
Bob_3	$\|\phi_4^1\rangle=\widehat{P}_2^0\widehat{E}_5\|\phi_3^1\rangle=\frac{1}{2}(\|0\rangle\|4\rangle+\|0\rangle\|5\rangle$ $+\|1\rangle\|1\rangle-\|1\rangle\|2\rangle)$	$\|\phi_4^2\rangle=\widehat{P}_3^0\widehat{E}_0\|\phi_3^2\rangle=\frac{1}{4}(2\|0\rangle\|2\rangle-2\|1\rangle\|5\rangle$ $+2\|0\rangle\|1\rangle-\|0\rangle\|3\rangle+\|1\rangle\|0\rangle+\|0\rangle\|5\rangle+\|1\rangle\|2\rangle)$	$\|\phi_4^3\rangle=P_4^0E_5\|\phi_3^3\rangle=\frac{1}{4}(2\|0\rangle\|1\rangle+\|0\rangle\|0\rangle$ $-\|1\rangle\|4\rangle+2\|0\rangle\|4\rangle-\|0\rangle\|3\rangle+\|1\rangle\|0\rangle+\|0\rangle\|2\rangle$ $+\|1\rangle\|6\rangle-\|0\rangle\|5\rangle-\|1\rangle\|2\rangle)$
Alice测量结果	$o_1^1=0, o_2^1=5$	$o_1^2=0, o_2^2=1$	$o_1^3=0, o_2^3=0$
运算结果	$\tilde{f}_1(x_1,x_2,x_3)=5^{o_2^1\widehat{\ominus}(\widehat{\oplus}_{i=0}^3p_i^1)}=3$	$\tilde{f}_2(x_1,x_2,x_3)=5^{o_2^2\widehat{\ominus}(\widehat{\oplus}_{i=0}^3p_i^2)}=3$	$\bar{f}(x_1,x_2,x_3)=o_2^3\ominus(\oplus_{i=0}^3p_i^3)=1$

同理, 在最后一轮中, Alice和三个参与者分别制备相应的随机数($p_1^3=6, q_1^3=0$), ($p_2^3=2, q_2^3=0, r_2^3=3$), ($p_3^3=4, q_3^3=1, r_3^3=1$), ($p_4^3=1, q_4^3=0, r_4^3=4$), 进而计算出线性单项$\bar{f}(x_1,x_2,x_3)=1$. 在协议结束时, Alice将三个计算结果求和得到$f(x_1,x_2,x_3)=3\oplus3\oplus1=0$, 并将该结果告知3个参与者.

5 协议性能分析

5.1 正确性

通过上述例子可以看出, 在理想情况下所有参与者执行协议后获得正确的计算结果. 下面, 本文利用命题1和命题2的结论对协议的正确性进行严格证明. 具体证明过程如下.

首先, 对线性项的计算结果进行分析. 在第$m+1$轮, Alice制备的量子初态可设为$|\phi_1^{m+1}\rangle=P_{r_1^{m+1}}^{q_1^{m+1}}|0\rangle|p_1^{m+1}\rangle$. 在理想情况(没有信道噪声和敌手攻击)下, 经过n次操作后回到Alice手上的两粒子所处的状态为

$$|\phi_{n+1}^{m+1}\rangle=P_{r_{n+1}^{m+1}}^{q_{n+1}^{m+1}}E_{x_n\oplus p_{n+1}^{m+1}}\cdots P_{r_2^{m+1}}^{q_2^{m+1}}E_{x_1\oplus p_2^{m+1}}P_{r_1^{m+1}}^{q_1^{m+1}}|0\rangle|p_1^{m+1}\rangle. \quad (5)$$

根据命题1, 可得

$$|\phi_{n+1}^{m+1}\rangle=P_{r_{n+1}^{m+1}}^{q_{n+1}^{m+1}}\cdots P_{r_2^{m+1}}^{q_2^{m+1}}P_{r_1^{m+1}}^{q_1^{m+1}}E_{x_n\oplus p_{n+1}^{m+1}}\cdots E_{x_1\oplus p_2^{m+1}}|0\rangle|p_1^{m+1}\rangle. \quad (6)$$

因此, 在Alice执行$(P_{r_1^{m+1}}^{q_1^{m+1}})^{-1}(P_{r_2^{m+1}}^{q_2^{m+1}})^{-1}\cdots(P_{r_{n+1}^{m+1}}^{q_{n+1}^{m+1}})^{-1}$操作后, 两个信号粒子所处的量子态就为

$$\begin{aligned}&E_{x_n\oplus p_{n+1}^{m+1}}\cdots E_{x_1\oplus p_2^{m+1}}|0\rangle|p_1^{m+1}\rangle\\&=|0\rangle|p_1^{m+1}\oplus\cdots\oplus p_{n+1}^{m+1}\oplus x_1\oplus\cdots\oplus x_n\rangle.\end{aligned} \quad (7)$$

在这种情况下, 对两粒子进行计算基测量, 测量结果就为$o_1^{m+1}=0$和$o_2^{m+1}=p_1^{m+1}\oplus\cdots\oplus p_{n+1}^{m+1}\oplus x_1\oplus\cdots\oplus x_n$. 那么, Alice就可得到线性项的正确计算结果, 即下述公式成立:

$$o_2^{m+1}\ominus(p_1^{m+1}\oplus\cdots\oplus p_{n+1}^{m+1})=x_1\oplus\cdots\oplus x_n=\bar{f}(x_1,\cdots,x_n). \quad (8)$$

类似地, 利用命题2和欧拉定理, 我们很容易证明Alice就可得到非线性项的正确计算结果, 即

$$g^{o_2^j\widehat{\ominus}(p_1^j\widehat{\oplus}\cdots\widehat{\oplus}p_{n+1}^j)}=\tilde{f}_j(x_1,\cdots,x_n). \quad (9)$$

根据式(8)和(9), 不难看出Alice公布的结果就是多项式$f(x_1,\cdots,x_n)$的计算结果. 因此, 协议是正确的. 另外, 从式(7)可知, 在理想情况下所有第一个信号粒子(即检测粒子)的测量结果都应该是0. 因此, 协议可以利用这个测量结果计算错误率, 实现窃听检测.

5.2 安全性

本节将对所提的量子安全多方计算协议的安全性

进行分析. 这里, 主要对一些常见的攻击策略[40]进行分析, 考虑两种情形: 一个是外部攻击者的窃听行为, 二是内部参与者的攻击行为. 本协议所涉及的参与者与半可信的第三方都有可能是不诚实的, 因此在分析协议的安全性时, 应着重考虑多个不诚实参与者的共谋攻击以及半可信第三方的主动攻击.

5.3 外部攻击

假设存在一个外部攻击者Eve, 她的目的是窃取参与者的秘密信息x_i或s_i. Eve窃取s_i的情形和x_i相似, 故这里只讨论窃取x_i的情形. 由于秘密信息被编码到旅行粒子中, 因此Eve只能通过攻击旅行粒子来获得Bob_i秘密信息. 这里, 考虑两种常见的攻击策略, 即截获重发攻击和纠缠附加粒子攻击[2,40].

(1) 截获重发攻击

截获重发攻击是指窃听者截获信道中传输的粒子并进行测量, 然后根据测量结果发送适当的量子态给合法接收者. 在所提协议中, 为了成功地执行拦截重发攻击, Eve可以拦截Bob_{i-1}在第j轮发送的量子态$|\phi_i^j\rangle$, 并重新发送一个假量子态给Bob_i. 由于量子态的第一个粒子被用来进行窃听检测, 而制备的假量子态的第一个粒子将不可避免地会引入错误, 这将在步骤(4)中被Alice检测到. 尽管如此, Eve依然试图窃取Bob_i的秘密信息. 然而, 这仍是不成功的. 具体分析如下.

假设Eve发送给Bob_i的假量子态为$|\psi_1\rangle = |0\rangle|0\rangle$, Bob_i对其执行操作$P_{r_{i+1}^j}^{q_{i+1}^j} E_{x_i \oplus p_{i+1}^j}$, 得到量子态$|\psi_2\rangle = P_{r_{i+1}^j}^{q_{i+1}^j} |x_i \oplus p_{i+1}^j\rangle$. 然后, Eve再次拦截由$\mathrm{Bob}_i$发送给$\mathrm{Bob}_{i+1}$量子态$|\psi_2\rangle$. 根据公开信息$q_{i+1}^j$和$r_{i+1}^j$, Eve对$|\psi_2\rangle$执行操作$(P_{r_{i+1}^j}^{q_{i+1}^j})^{-1}$, 得到量子态$|\psi_3\rangle = |x_i \oplus p_{i+1}^j\rangle$. 由于Eve不知道随机数$p_{i+1}^j$, 所以她不能计算出$\mathrm{Bob}_i$的秘密信息$x_i$. 综上, 提出的协议可以抵抗截获重发攻击.

(2) 纠缠附加粒子攻击

纠缠附加粒子攻击是指窃听者在截获信道中的粒子后, 通过幺正操作将自己的附加粒子与合法粒子纠缠起来, 然后将合法粒子重发给接收者, 随后从自己的附加粒子中窃取信息. 协议中, Eve可截获Bob_i在第j轮发送的量子态$|\phi_{i+1}^j\rangle$, 并制备一个附加粒子$|e\rangle$, $e \in GF(d)^*$. 然后, 她把$|\phi_{i+1}^j\rangle$的第二个粒子(用$|c\rangle$表示)作为控制粒子, 把附加粒子$|e\rangle$作为目标粒子来执行一个纠缠操作$U(|c\rangle, |e\rangle) = (|c\rangle, |c \oplus e\rangle)$. 此后, 如果Eve对附加粒子进行测量, 她将得到$c \oplus e$, 并推算出c, c由$\oplus_{k=1}^{i+1} p_k^j$, $\oplus_{k=1}^{i+1} x_k$以及$r_1^j, r_2^j, \cdots, r_{i+1}^j$组成. 由于Eve不知道随机数$p_1^j$的值, 所以她不能根据公开信息$r_k^j$从$c$中推断出关于$x_i$的信息. 进一步地, 如果Eve把攻击后的信号粒子发送给Bob_{i+1}, Bob_{i+1}则对该量子态执行操作$P_{r_{i+2}^j}^{q_{i+2}^j} E_{x_{i+1} \oplus p_{i+2}^j}$, 这对附加粒子$|c \oplus e\rangle$将不产生任何影响. 同样地, Eve测量该附加粒子也得不到关于参与者Bob_{i+1}的任何秘密信息. 简言之, 本文所提协议可抵抗纠缠附加粒子攻击.

5.4 内部攻击

在量子安全多方计算中, 参与者并不一定是诚实的, 其目的是窃取其他参与者的秘密输入. 与外部攻击者不同, 内部参与者参与协议的执行. 因此, 一般来讲他们拥有更大的便利攻击协议, 更具有破坏性[40,41]. 下面, 将对本文所提协议在一些常见的内部攻击下的情形进行分析.

(1) 不诚实参与者的共谋攻击[42]

协议中, 可能存在一个或多个不诚实的参与者想要窃取其他诚实参与者的秘密信息而不被检测到. 在只有一个不诚实参与者的情形中, 他的攻击行为会像外部攻击者Eve一样在步骤(4)中被检测到. 接下来, 我们将讨论一种比较普遍的情况. 在多方量子密码协议中, 多个不诚实参与者可以联合起来, 通过执行一系列的攻击操作来窃取诚实参与者的秘密, 这就是不诚实参与者的共谋攻击. 显然, 该攻击比单个不诚实参与者的攻击更具破坏性. 这里, 我们假设Bob_{i-1}和Bob_{i+1}是不诚实的参与者, 他们被标记为Bob_{i-1}^*和Bob_{i+1}^*. 显然, 他们共谋窃取Bob_i的秘密信息要比其他诚实参与者的更容易. Bob_{i-1}^*和Bob_{i+1}^*共谋攻击Bob_i的情形被讨论如下.

这里, 考虑一种比较常见的攻击策略. 假设Bob_{i-1}^*拦截量子态$|\phi_i^j\rangle$并保存在自己手中, 然后他发送一个假粒子$|\omega_1\rangle = |0\rangle|0\rangle$给$\mathrm{Bob}_i$. Bob_i对假粒子执行操作$P_{r_{i+1}^j}^{q_{i+1}^j} E_{x_i \oplus p_{i+1}^j}$, 得到量子态$|\omega_2\rangle = P_{r_{i+1}^j}^{q_{i+1}^j} |x_i \oplus p_{i+1}^j\rangle$, 将其发送给$\mathrm{Bob}_{i+1}^*$. 尽管$\mathrm{Bob}_{i-1}^*$和$\mathrm{Bob}_{i+1}^*$根据公开信息$q_{i+1}^j$和$r_{i+1}^j$可以确定$\mathrm{Bob}_i$执行的置乱操作, 但因为不知道$\mathrm{Bob}_i$的随机数$p_{i+1}^j$, 故他们无法从测量结果中推算

出Bob_i的秘密信息x_i.

最后, 我们对一种极端情况进行讨论, 即只有一个参与者是诚实的. 假设Bob_1是诚实的, 那么剩余$n-1$不诚实参与者根据公开的信息q_2^j和r_2^j共谋可以得到量子态$P_{r_1^j}^{q_1^j}|0\rangle|\oplus_{i=1}^{n+1}p_i^j\oplus\oplus_{i=1}^{n}x_i\rangle$. 由于剩余$n-1$不诚实参与者不知道Alice 的随机数$q_1^j$, r_1^j以及p_1^j, 所以他们共谋不能计算出诚实参与者Bob_1的秘密信息x_1. 通过上述分析可知, 共谋攻击对提出的协议是无效的.

(2) 半可信第三方的攻击 [43]

文献[43]从理性角度出发, 对量子安全多方计算中半可信第三方的能力进行规范. 除了不能与参与者合谋外, 半可信第三方可采取任何的主动和被动攻击策略来获得参与者的秘密信息. 在本文所提出的协议中, Alice是半可信的, 她试图利用参与协议的便利条件来窃取参与者Bob_i的秘密信息x_i. 为了达到这个目的, Alice可以拦截Bob_{i-1}发送的粒子, 并发送一个假粒子给Bob_i. 和外部攻击者Eve一样, Alice的这种攻击行为不仅无法获得Bob_i的秘密信息, 还会引入错误, 并在步骤(4)中被检测到. 因此, 提出的协议可以抵抗半可信第三方的攻击.

5.5 效率比较

在安全多方计算协议中, 一般存在两个影响其效率的主要因素, 即通信复杂度(Communication Complexity, CC)和循环复杂度(Round Complexity, RC). SMC协议的通信复杂度是指协议执行过程中传输的最大比特数, 循环复杂度是执行协议所需的最大轮数. 本节将所提协议与一些相关的协议进行比较, 如表2所示. 在所提协议中, 对于每个线性(非线性)单项, 第三方只需制备一个量子态, 然后依次把该量子态传递给每个参与者, 所以协议的通信复杂度为$O(m+1)$, 其中, m表示多项式函数中非线性单项的个数. 由于提出的协议执行一轮就可以实现多项式函数的计算, 因此循环复杂度为1. 此外, 在文献[44] 中, Cabello对量子密钥分发协议的密钥生成率E定义为$E=\frac{b_s}{q_t+b_t}$. 这里, b_s为秘密信息比特, q_t和b_t为需要传输的量子比特和经典比特. 在本文所提协议中, n个参与者共同计算得到一个d级输出, 即$b_s=d$. 协议利用一个qudit作为信息粒子在n个参与者之间传输, 故而$q_t=nd$. 由于协议中每个参与者需公布q_i, r_i和p_i, 所以协议需要传输的经典信息有$b_t=nd+nd+2n$. 综上, 所提协议的效率$E=\frac{d}{3nd+2n}$. 从表2可以看出, 由于提出的协议大大降低了协议的通信复杂度和循环复杂度, 因此它与协议 [35,37,38]相比具有明显的效率优势.

值得注意的是, 与其他协议使用qudit进行窃听检测不同, 本协议采用qubit作为检测粒子, 因此该协议具有更高的检测效率. 此外, 提出的协议实现了有限域GF(d)上n元变量多项式的加、减、乘、除四则混合运算, 且无需量子存储(除第三方外)和事先共享密钥, 因此相比于协议 [35,37,38]来说, 所提协议的通用性和实用性更强.

6 结论

本文基于欧拉定理和量子纠缠特性, 构造两对可对易的量子门操作, 并在此基础上设计了一个高效的量子安全多方计算协议. 在该协议中, 半可信第三方制备两个粒子纠缠态作为信息粒子, 在参与者之间进行环型传输. 首先, 第三方根据自己的随机数对传输粒子执行置乱操作. 然后, 每个参与者依次将秘密输入信息编码到粒子中, 并对该粒子执行置乱操作. 最后, 半可信第三方根据测量结果和公开信息推出多项式的计算结果, 并将该结果告知所有参与者. 协议的性能分析表明, 提出的协议正确, 并且可以抵抗一些常见的攻

表 2 提出的协议与相关协议的比较

Table 2 Comparison of the proposed protocol and related protocols

协议	量子态	函数类型	运算类型	CC	RC	效率E
Sutradhar等人 [35]的协议	单粒子态	模2的布尔函数	$+,\times$	$O(n^2)$	3	$\frac{d}{n(n+3)d}$
Lu等人 [37]的协议Γ_2	纠缠态	模d的多项式函数	$+,\times$	$O(m\times n^2)$	3	$\frac{d}{2n(n-1)d+4nd}$
Zhang等人 [38]的协议Γ_2	纠缠态	模d的多项式函数	$+,\times$	$O(m\times n^2)$	2	$\frac{d}{n^2d+nr}$
本文所提协议	两粒子纠缠态	模d的多项式函数	$+,-,\times,\div$	$O(m+1)$	1	$\frac{d}{3nd+2n}$

击, 如拦截重发攻击、纠缠测量攻击、不诚实参与方的共谋攻击以及半可信第三方的主动攻击. 由于提出的协议执行一轮就可以实现多项式函数的计算, 而且无需事先共享密钥, 这大大降低了协议的通信复杂度和循环复杂度, 因此协议获得较高的效率. 此外, 协议将一个d级粒子作为信息载体保存秘密输入信息, 用一个2级粒子进行窃听检测, 因此本文所提协议的检测效率高.

另一方面, 从实用性角度出发, 与一些使用多粒子纠缠态的量子安全多方计算协议相比, 本文所提协议仅使用两粒子纠缠态, 在现有技术条件这显然是更易于实现的. 此外, 除第三方外的所有参与者都仅要求具备常见的两粒子量子门操作的能力, 而无需存储信号粒子, 这也进一步提高协议的实用性. 然而, 随着d的增大, 制备d级粒子将变得越来越困难, 这就大大限制了协议的实际应用. 为了解决该问题, 可以借鉴文献[45]的方法, 利用中国剩余定理加以解决. 具体来讲, 先选择几个互素的数值较小的正整数$d_1, d_2, \cdots, d_v$, 满足$d_1 \times d_2 \times \cdots \times d_v > d$. 然后, 对每个$d_i$通过执行本文所提协议, 即利用$d_i$级粒子得到$f(\cdot) \bmod d_i$的数值. 最后, 根据这$v$个结果, 通过中国剩余定理就可安全计算出$f(\cdot) \bmod d$.

参考文献

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Theor Comput Sci, 2014, 560: 7–11
2 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
3 Long G L, Wang C, Li Y S, et al. Quantum secure direct communication (in Chinese). Sci Sin-Phys Mech Astron, 2011, 41: 332–342 [龙桂鲁, 王川, 李岩松, 等. 量子安全直接通信. 中国科学: 物理学 力学 天文学, 2011, 41: 332–342]
4 Yao A C. Protocols for secure computations. In: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). Los Alamitos: IEEE, 1982. 160–164
5 Goldreich O, Micali S, Wigderson A. How to play any mental game. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing. ACM, 1987: 218–229
6 Chau H F. Quantum-classical complexity-security tradeoff in secure multiparty computations. Phys Rev A, 2000, 61: 032308
7 Ben-Or M, Crépeau C, Gottesman D, et al. Secure multiparty quantum computation with (only) a strict honest majority. In: Proceedings of the 47th Annual IEEE Symposium on Found Computer Science (FOCS'06). New York: IEEE, 2006. 249–260
8 Loukopoulos K, Browne D E. Secure multiparty computation with a dishonest majority via quantum means. Phys Rev A, 2010, 81: 062336
9 Yang Y G, Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A-Math Theor, 2010, 43: 209801
10 Chen X B, Xu G, Niu X X, et al. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt Commun, 2010, 283: 1561–1565
11 Li Q, Li P, Xie L, et al. Security analysis and improvement of a semi-quantum private comparison protocol with three-particle G-like states. Quantum Inf Process, 2022, 21: 127
12 Giovannetti V, Lloyd S, Maccone L. Quantum private queries. Phys Rev Lett, 2008, 100: 230502
13 Jakobi M, Simon C, Gisin N, et al. Practical private database queries based on a quantum-key-distribution protocol. Phys Rev A, 2011, 83: 022301
14 Gao F, Qin S J, Huang W, et al. Quantum private query: A new kind of practical quantum cryptographic protocol. Sci China-Phys Mech Astron, 2019, 62: 070301
15 Wei C Y, Cai X Q, Wang T Y, et al. Error tolerance bound in QKD-based quantum private query. IEEE J Sel Areas Commun, 2020, 38: 517–527
16 Shi R, Mu Y, Zhong H, et al. An efficient quantum scheme for private set intersection. Quantum Inf Process, 2016, 15: 363–371
17 Shi R. Quantum private computation of cardinality of set intersection and union. Eur Phys J D, 2018, 72: 221
18 Liu W, Yin H W. A novel quantum protocol for private set intersection. Int J Theor Phys, 2021, 60: 2074–2083
19 Shi R, Mu Y, Zhong H, et al. Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query. Quantum Inf Process, 2017, 16: 8
20 Peng Z, Shi R, Zhong H, et al. A novel quantum scheme for secure two-party distance computation. Quantum Inf Process, 2017, 16: 316
21 Du J-Z, Chen X-B, Wen Q-Y, et al. Secure multiparty quantum summation (in Chinese). Acta Phys Sin, 2007, 56: 6214–6219 [杜建忠, 陈秀波, 温巧燕, 等. 保密多方量子求和. 物理学报, 2007, 56: 6214-6219]
22 Chen X B, Xu G, Yang Y X, et al. An efficient protocol for the secure multi-party quantum summation. Int J Theor Phys, 2010, 49: 2793–2804

23 Zhang C, Sun Z, Huang Y, et al. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. Int J Theor Phys, 2014, 53: 933–941

24 Liu W, Wang Y B, Fan W Q. An novel protocol for the quantum secure multi-party summation based on two-particle bell states. Int J Theor Phys, 2017, 56: 2783–2791

25 Zhang C, Situ H, Huang Q, et al. Multi-party quantum summation without a trusted third party based on single particles. Int J Quantum Inform, 2017, 15: 1750010

26 Yang H Y, Ye T Y. Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf Process, 2018, 17: 129

27 Ye T Y, Hu J L. Quantum secure multiparty summation based on the mutually unbiased bases of d-level quantum systems and its application (in Chinese). Sci Sin-Phys Mech Astron, 2021, 51: 020301 [叶天语, 胡家莉. 基于d级量子系统相互无偏基的量子安全多方求和及其应用. 中国科学: 物理学 力学 天文学, 2021, 51: 020301]

28 Song X, Gou R, Wen A. Secure multiparty quantum computation based on Lagrange unitary operator. Sci Rep, 2020, 10: 7921

29 Zhang C, Long Y, Li Q. Quantum summation using d-level entanglement swapping. Quantum Inf Process, 2021, 20: 137

30 Wu W Q, Ma X X. Multi-party quantum summation without a third party based on d-dimensional Bell states. Quantum Inf Process, 2021, 20: 200

31 Wang Y, Hu P, Xu Q. Quantum secure multi-party summation based on entanglement swapping. Quantum Inf Process, 2021, 20: 319

32 Li Y B, Wen Q Y, Qin S J. Improved secure multiparty computation with a dishonest majority via quantum means. Int J Theor Phys, 2013, 52: 199–205

33 Shi R H, Mu Y, Zhong H, et al. Secure multiparty quantum computation for summation and multiplication. Sci Rep, 2016, 6: 19655

34 Shi R. A generic quantum protocol for one-sided secure two-party classical computations. Quantum Inf Process, 2020, 19: 22

35 Sutradhar K, Om H. Hybrid quantum protocols for secure multiparty summation and multiplication. Sci Rep, 2020, 10: 1–9

36 Clementi M, Pappa A, Eckstein A, et al. Classical multiparty computation using quantum resources. Phys Rev A, 2017, 96: 062317

37 Lu C, Miao F, Hou J, et al. Secure multi-party computation with a quantum manner. J Phys A-Math Theor, 2021, 54: 085301

38 Zhang L W, Song X L, Li C, et al. Quantum secure multiparty multiplication based on Lagrange unitary operator (in Chinese). Sci Sin-Phys Mech Astron, 2022, 52: 260311 [张龙威, 宋秀丽, 李闯, 等. 基于拉格朗日酉算子的量子安全多方求积. 中国科学: 物理学 力学 天文学, 2022, 52: 260311]

39 Wang H Z, Li L, Du R Y, et al. Cryptography and Network Security: Principles and Practice (7th Ed) (in Chinese). Beijing: Publishing House of Electronics Industry, 2017. 33–34 [王后珍, 李莉, 杜瑞颖, 等(译). 密码编码学与网络安全: 原理与实践(第七版). 北京: 电子工业出版社, 2017. 33–34]

40 Wen Q Y, Gao F, Qin S J. Cryptanalysis of quantum cryptographic Protocols (in Chinese). J Cryptol Res, 2014, 1: 200–210 [温巧燕, 高飞, 秦素娟. 量子密码协议安全性分析. 密码学报, 2014, 1: 200–210]

41 Lin S, Guo G D, Xu Y Z, et al. Cryptanalysis of quantum secret sharing with d-level single particles. Phys Rev A, 2016, 93: 062343

42 Liu B, Xiao D, Jia H Y, et al. Collusive attacks to "circle-type" multi-party quantum key agreement protocols. Quantum Inf Process, 2016, 15: 2113–2124

43 Yang Y G, Xia J, Jia X, et al. Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf Process, 2013, 12: 877–885

44 Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85: 5635–5638

45 Lin S, Guo G D, Huang F, et al. Quantum anonymous ranking based on the Chinese remainder theorem. Phys Rev A, 2016, 93: 012318

附录 命题1和2的证明

命题1: 若$E_s = I_2 \otimes X_s$, $P_t^q = CX_t^q(H \otimes I_d)$ $(s,t \in \mathrm{GF}(d), q \in \mathrm{GF}(2))$, 则$E_sP_t^q = P_t^qE_s$.

证明: 首先对$q = 0$的情形进行讨论. 由于

$$E_s = I_2 \otimes X_s = (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes_{i=0}^{d-1} |i \oplus t\rangle\langle i|,$$

$$P_t^0 = CX_t^0(H \otimes I_d) = (|0\rangle\langle 0| \otimes \sum_{i=0}^{d-1} |i\rangle\langle i| + |1\rangle\langle 1|$$

$$\otimes \sum_{i=0}^{d-1} |i \oplus t\rangle\langle i|)\Big[(|+\rangle\langle 0| + |-\rangle\langle 1|) \otimes \sum_{j=0}^{d-1} |j\rangle\langle j|\Big]$$

$$= |0\rangle\langle 0|(|+\rangle\langle 0| + |-\rangle\langle 1|) \otimes \sum_{j=i=0}^{d-1} |j\rangle\langle j| + |1\rangle\langle 1|(|+\rangle\langle 0|$$

$$+ |-\rangle\langle 1|) \otimes \sum_{j=i=0}^{d-1} |j \oplus t\rangle\langle j|$$

$$= \frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0| + |0\rangle\langle 1|) \otimes \sum_{j=0}^{d-1} |j\rangle\langle j| + (|1\rangle\langle 0| - |1\rangle\langle 1|)$$

$$\otimes\sum_{j=0}^{d-1}|j\oplus t\rangle\langle j|\Big], \tag{a1}$$

故可得

$$\begin{aligned}P_t^0E_s=&\frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0|+|0\rangle\langle 1|)(|0\rangle\langle 0|+|1\rangle\langle 1|)\\&\otimes\sum_{i=j=0,i=j\oplus t}^{d-1}|i\rangle\langle i|j\oplus t\rangle\langle j|+(|1\rangle\langle 0|-|1\rangle\langle 1|)(|0\rangle\langle 0|\\&+|1\rangle\langle 1|)\otimes\sum_{i=j=0,i=j\oplus t}^{d-1}|i\oplus t\rangle\langle i|j\oplus t\rangle\langle j|\Big]\\=&\frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0|+|0\rangle\langle 1|)\otimes\sum_{i=0}^{d-1}|i\oplus t\rangle\langle i|+(|1\rangle\langle 0|\\&-|1\rangle\langle 1|)\otimes\sum_{i=0}^{d-1}|i\oplus 2t\rangle\langle i|\Big]=E_sP_t^0.\end{aligned} \tag{a2}$$

同理, 对$q=1$的情形可得相同的结论. 因此, 命题1成立.

命题2: 若$\widehat{E}_s=I_2\otimes\widehat{X}_s$, $\widehat{P}_t^q=\widehat{CX}_t^q(H\otimes I_d)$, 则$\widehat{E}_s\widehat{P}_t^q=\widehat{P}_t^q\widehat{E}_s$.

证明: 首先对$q=0$的情形进行讨论. 由于

$$\begin{aligned}\widehat{E}_s=&I_2\otimes\widehat{X}_s=(|0\rangle\langle 0|+|1\rangle\langle 1|)\\&\otimes\left(\sum_{i=0}^{d-2}|i\widehat{\oplus}t\rangle\langle i|+|d-1\rangle\langle d-1|\right),\\\widehat{P}_t^0=&\widehat{CX}_t^0(H\otimes I_d)\end{aligned} \tag{a3}$$

$$\begin{aligned}=&\frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0|+|0\rangle\langle 1|)\otimes\sum_{i=0}^{d-1}|i\rangle\langle i|+(|1\rangle\langle 0|-|1\rangle\langle 1|)\\&\otimes\left(\sum_{i=0}^{d-2}|i\widehat{\oplus}t\rangle\langle i|+|d-1\rangle\langle d-1|\right)\Big],\end{aligned}$$

故可得

$$\begin{aligned}\widehat{E}_s\widehat{P}_t^0=&\frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0|+|1\rangle\langle 1|)(|0\rangle\langle 0|+|0\rangle\langle 1|)\\&\otimes\left(\sum_{i=0}^{d-2}|i\widehat{\oplus}t\rangle\langle i|+|d-1\rangle\langle d-1|\right)\sum_{i=0}^{d-1}|j\rangle\langle j|\\&+(|0\rangle\langle 0|+|1\rangle\langle 1|)(|1\rangle\langle 0|-|1\rangle\langle 1|)\\&\otimes\left(\sum_{i=0}^{d-2}|i\widehat{\oplus}t\rangle\langle i|+|d-1\rangle\langle d-1|\right)\\&\times\left(\sum_{j=0}^{d-2}|j\widehat{\oplus}t\rangle\langle j|+|d-1\rangle\langle d-1|\right)\Big]\\=&\frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0|+|0\rangle\langle 1|)\\&\otimes\left(\sum_{i=0}^{d-2}|i\widehat{\oplus}t\rangle\langle i|+|d-1\rangle\langle d-1|\right)+(|1\rangle\langle 0|-|1\rangle\langle 1|)\\&\otimes\Big(\sum_{i=0}^{d-2}|i\widehat{\oplus}2t\rangle\langle i|+|d-1\rangle\langle d-1|\Big]=\widehat{P}_t^0\widehat{E}_s.\end{aligned} \tag{a4}$$

同理, 对$q=1$的情形可得相同的结论. 因此, 命题2成立.

An efficient secure multiparty quantum computation protocol

LIN Song[1*], WANG Ning[1,2] & LIU Xiao-Fen[1]

[1]*College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350100, China;;*
[2]*School of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, China*

Secure multiparty computing is an important class of cryptographic primitives and is widely used in electronic voting, data mining, blockchain, cloud computing and other fields. In this paper, we propose an efficient secure multiparty quantum computation protocol based on quantum entanglement and the Euler theorem. In this protocol, all participants can safely compute multivariate polynomial functions with the help of a semitrusted third party. A performance analysis shows that the protocol is correct and can resist some common external and internal attacks. Additionally, the proposed protocol not only improves particle detection efficiency but also effectively reduces the communication complexity.

quantum cryptography, secure multiparty quantum computation, Euler theorem, polynomial function

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud

doi: 10.1360/SSPMA-2023-0030