



基于Brown态的多方概率量子同态加密方案

刘明奎, 李祯祯*, 高博, 丁海洋, 李子臣

北京印刷学院, 数字版权保护技术研究中心, 北京 102600

*联系人, E-mail: lizhenzhen1101@163.com

收稿日期: 2024-08-26; 接受日期: 2024-10-24; 网络出版日期: 2025-01-09

国家自然科学基金(编号: 62472040, 61370188, 12161061, 61762068)、内蒙古自治区科技计划项目(编号: SB20210010)、北京市教委科研计划项目(编号: KM202010015009)、北京印刷学院青年卓越项目(编号: Ea202411)、北京市数字教育研究课题(编号: 20240022)、北京市高等教育学会项目(编号: 20240014)和中国版权保护中心版权研究课题(编号: BQ2024017)资助项目

摘要 量子同态加密可以直接对密文进行计算, 这样能够保证隐私数据的安全性. 本文提出了一种新的基于Brown态的多方概率量子同态加密方案, 该方案允许多个客户端同时委托两个服务器进行任意的量子计算. 首先, 引入可信密钥中心, 与客户端利用B92协议合作完成密钥的分发和更新, 以及完成消除T门评价错误的相关操作; 其次, 所提方案利用预共享的非最大纠缠态作为辅助资源来非交互式地解决T门同态评价时发生的错误; 最后, 本方案利用Brown态的属性将单客户端单服务器模式扩展为多客户端多服务器模式, 更加适用于量子分布式网络, 增加了实用性. 另外, 本文在理论上详细证明了该方案具有正确性、全同态性和信息论安全性, 并在本源量子云平台上进行了仿真实验, 进一步验证了所提方案的有效性. 由于该方案可以实现任意量子线路的同态计算, 因此特别适用于量子云网络中的委托计算.

关键词 量子同态加密, 非最大纠缠态, Brown态, 非交互式, 委托计算

PACS: 03.67.-a, 03.67.Dd, 03.67.Hk, 03.67.Lx

1 引言

随着大数据时代的到来和云计算的普及, 数据隐私和安全成为社会各界关注的焦点. 在委托计算的过程中, 最关键的问题是如何确保数据的安全性. 那么, 是否存在一种技术能够解决这一问题, 即在不解密的情况下对加密数据进行计算呢? 早在1978年, Rivest等人^[1]提出了同态加密的概念, 这一技术在当时被称为隐私同态. 他们设想了一种加密系统, 允许在加密数

据上执行特定的计算, 而无需先将数据解密. 然而, 当时并未提出具体的实现方案. 直到2009年, Gentry^[2]提出了第一个基于非标准计算假设的全同态加密(FHE)方案, 实现了在密文上进行任意函数计算, 标志着同态加密研究的重大突破. 此后, 在国际密码学界引起了对全同态加密方案的研究.

经典的同态加密方案的相关问题主要有委托计算^[3]、函数加密^[4]和混淆^[5]. 然而, 大多数经典的同态加密方案都依赖于复杂数学难题. 随着量子计算的发

引用格式: 刘明奎, 李祯祯, 高博, 等. 基于Brown态的多方概率量子同态加密方案. 中国科学: 物理学 力学 天文学, 2025, 55: 240305
Liu M K, Li Z Z, Gao B, et al. Multi-party probabilistic quantum homomorphic encryption scheme based on Brown state (in Chinese). Sci Sin-Phys Mech Astron, 2025, 55: 240305, doi: [10.1360/SSPMA-2024-0355](https://doi.org/10.1360/SSPMA-2024-0355)

展, 传统的密码学面临着严峻的安全挑战. 例如, Shor 算法^[6]利用量子计算的并行性能够在多项式时间内因式分解大整数, 从而威胁到基于数论的经典加密算法(如RSA和ECC)的安全性. 在此背景下, 量子密码学应运而生. 在此同时, 与许多经典的密码方案相比, 量子密码学利用量子力学的特殊性质, 安全性受到海森堡测不准原理和不可克隆定理等物理原理保证, 不需要计算假设, 从而保证了信息理论的安全性. 与上述经典问题类似, 相应的量子密码学方案包括量子私有查询^[7,8]、量子秘密共享(QSS)^[9,10]、盲量子计算^[11,12]和量子同态加密^[8,9,13–24].

到目前为止, 量子同态加密已经得到了广泛的研究. 2012年, Rohde等人^[13]利用玻色子散射模型和量子行走实现了一个受限的量子同态加密方案, 这一研究为量子同态加密的实际应用奠定了基础. 随后在2013年, Liang^[14]定义了量子同态加密(Quantum Homomorphic Encryption, QHE)和量子全同态加密(Quantum Fully Homomorphic Encryption, QFHE)的完整概念, 并构造了首个对称量子同态加密方案, 明确了量子同态加密的理论框架. 2014年, Yu等人^[25]通过对限制量子同态加密实现因素的研究, 发现了一个不可行的结论, 即在非交互的情况下, 具有完美信息理论上安全的QHE方案肯定会导致指数级开销. 同年, Fisher等人^[15]在实验中通过使用单光子和线性光学技术, 成功在密文数据上实现了任意的量子计算, 这一实验进一步验证了量子同态加密的可行性. 2015年, Broadbent和Jeffery^[16](BJ15)在经典全同态加密的基础上, 构造出了仅能完成有限数量非Clifford门评价的QHE方案, 该方案具有计算安全性和非交互性. 2016年, Dulek等人^[17]基于瞬时非局域量子计算和BJ15框架构造了量子小工具来纠正加密量子数据T门评估过程中出现的错误, 同时将BJ15所提的方案扩展为适用于多项式大小非Clifford门的QHE方案. 2017年, Alagic等人^[18]构造了一个带验证的QFHE方案, 该方案提供认证加密, 确保同态运算结果的正确性, 并且可以完成任意多项式时间的量子计算, 而无需客户端和服务端之间的交互. 2018年, Ouyang等人^[19]利用量子编码构造了一个具有信息论安全性的QHE方案, 该方案建立在量子码的结构之上, 允许对包含固定数量的具有熵安全的非Clifford门的电路进行评估. 在此同时, Newman和Shi^[26], Lai和Chung^[27]在Yu等人^[25]研究结果的基础上分别证明了一

个加强的不可行结论: 非交互和信息论安全的量子全同态加密方案是不可能实现的, 因此只能通过降低安全性条件构造出达到计算安全的非交互式量子全同态加密方案. 2019年, Chen等人^[9]基于 (k, n) 门限量子秘密分享方案提出了一个共享量子态的量子同态加密方案, 该方案允许评估器交替地完成对共享加密序列上进行单量子位酉运算的评估, 在整个过程中任意大于固定数量的评估器就可以联合重构初始量子态序列的, 并给出了 $(3, 5)$ 和 $(2, 2)$ 情形来展示评估器的灵活性, 该方案可以根据相关量子秘密共享实验^[10]进行类似的验证. 2020年, Liang^[20]在量子隐形传态的基础上提出了加密门和门隐形传态的概念, 并利用两者进行非交互地解决T门评价的问题, 进而构造出了两个拟紧凑性的量子同态加密方案. 对于隐形传态的改进, Lv等人^[28]进而提出受控高维量子隐形传态并进行实现, 有望进一步增强量子同态加密方案的紧凑性. 2021年, Zhang等人^[21]由于考虑到量子信道中存在噪声, 难以制备最大纠缠态, 然而可以利用纠缠纯化^[29]从低质量纠缠态中提取高质量纠缠态, 因此可以通过客户端与服务端预分享非最大纠缠态来概率性消除T门评价时产生的错误, 在评价过程中, 双方不需要交互, 进而提出了一种概率量子同态加密方案. 之后在2022年, Zhang等人^[22]将自己的概率量子同态加密方案扩展为多客户端单服务器模型. 2023年, Chang等人^[23]提出了一种基于通用量子线路的动态QFHE方案, 该方案需要双方交互来消除T门评价时产生的错误, 同时该方案也可以处理服务器的波动性问题. 同年, Shang等人^[8]利用矩阵分解和线路合成的方法, 提出了一种两轮量子同态加密方案, 并将其应用于密文检索实验. 2024年, Pan等人^[24]基于蝶形网络提出了一种交叉量子同态加密方案, 该方案通过预共享纠缠态和Bell基测量完成对量子明文的加密, 分析还表明该方案还具有较高的效率, 同时还可抵御内外攻击. 然而, 文献^[14,17,19,23]在量子同态加密方案中评价阶段存在客户端与服务器的交互, 这样会占用一定的量子资源, 甚至有可能在交互的过程中造成密钥的泄露问题. 虽然文献^[8,9,13,15,16,18,20–22]中的方案利用各种方法实现了非交互, 但是又没有考虑到方案使用资源的制备问题, 并且方案中客户端为处理T门评价错误需要过多的复杂操作. 对于以上大部分方案, 都是单客户端单服务器的模式, 这种不适用于量子分布式网络, 缺

乏实用性.

通过对以上前人方案的分析, 我们提出了一个新的基于Brown态的多方概率量子同态加密方案, 该方案可以非交互式解决 T 门同态评价时发生错误的问题, 并将其扩展为多客户端多服务器模式. 本文的主要工作如下:

(1) 利用非最大纠缠态来非交互式地完成 T 门评价, 这降低了方案中使用的资源的制备条件, 在不可避免的噪声影响下实现QHE实验更具有现实意义;

(2) 引入可信密钥中心, 负责完成密钥的分发和更新, 以及完成消除 T 门评价错误的相关操作, 减轻了客户端工作量, 降低了对客户端量子能力的要求条件;

(3) 利用Brown态将方案扩展为多服务器模式, 进而扩展为多客户端多服务器模式, 更加适用于量子分布式网络, 增加了实用性;

(4) 通过分析证明了所提方案是正确的、全同态的和信息论安全的, 并在本源量子云平台上进行了仿真, 进一步验证了方案的有效性.

2 基础知识

2.1 量子计算

在这里, 简要描述一下常用的量子门, 具体可见文献[30]. 用于量子计算的量子线路是由Clifford门和非Clifford门组成, 即 $G = \{X, Z, H, S, T, \text{CNOT}\}$. 相应的酉矩阵定义为

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (1)$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix},$$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (2)$$

2.2 Brown态及其属性

Brown态是一个五粒子纠缠态, 其定义如下:

$$|B\rangle_{12345} = \frac{1}{2}(|001\rangle|\Phi^-\rangle + |010\rangle|\Psi^-\rangle + |100\rangle|\Phi^+\rangle + |111\rangle|\Psi^+\rangle)_{12345}. \quad (3)$$

同时, $\{|0\rangle, |1\rangle\}$ 基可以与 $\{|+\rangle, |-\rangle\}$ 通过应用Hadamard门(H 门)进行互相转换, 其转换公式为

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \\ |1\rangle &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle), \end{aligned} \quad (4)$$

通过以上转换公式, 可以将贝尔态转化为

$$\begin{aligned} |\Phi^+\rangle_{45} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{45} = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)_{45}, \\ |\Phi^-\rangle_{45} &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{45} = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)_{45}, \\ |\Psi^+\rangle_{45} &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{45} = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)_{45}, \\ |\Psi^-\rangle_{45} &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{45} = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)_{45}. \end{aligned} \quad (5)$$

假设我们制备一个Brown态, 在其前三个粒子上执行 Z 基单粒子测量, 测量完前三个粒子, 第四个粒子和第五个粒子所形成的贝尔态就可以被确定下来. 然后, 在第四个粒子和第五个粒子执行 X 基单粒子测量, 可以得到测量结果 $\text{measure} = \{MR_4, MR_5\}$. 我们定义 $|+\rangle$ 代表“0”, $|-\rangle$ 代表“1”. 由此可以根据前三个粒子所选择的基, 推出想分享的秘密 $K = MR_4 \oplus MR_5$.

根据上述Brown态及其测量属性, Brown态前三个粒子所选择的基对应的分享秘密如表1所示.

2.3 T 门的评价

用于量子计算的通用量子线路是由Clifford门和非Clifford门组成. Clifford门具有与泡利算子进行交换的特征, 因此在评价阶段不会产生任何错误. 众所周知, T 门是一个非Clifford门, 在评价阶段当它应用于密文态时, 有 $TX^aZ^b|\varphi\rangle = X^aZ^{a\oplus b}S^aT|\varphi\rangle$. 由式子可以观察到, 一个意想不到的 S 门错误出现在同态结果中, 这样会导致服务器评价输出错误的密文态, 因此必须尽力去消除 S 门错误, 来保证同态的正确性. 因此, 利用非最大纠缠态的性质, 经过服务器和客户端的一系列操作, 最终解密得到正确的同态结果. 接下来, 我们将具体阐述一下该方法的主要思路^[21].

假设存在明文量子态 $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, 其中 $|\alpha|^2 + |\beta|^2 = 1$. 首先, 利用一次一密(Quantum One-Time Pad, QOTP)对明文量子态 $|\Psi\rangle$ 进行加密, 可以得到密文

表 1 客户端所选择的前三个粒子的基与其分享秘密对应表

Table 1 The corresponding shared secret for the base of the first three particles selected by the client

前三个粒子	第四、五个粒子所形成的贝尔态	第四个粒子和第五个粒子X基测量结果	分享的秘密K
$ 001\rangle_{123}$	$ \Phi^-\rangle_{45}$	$ +\rangle_4 +\rangle_5$ 或 $ -\rangle_4 -\rangle_5$	0
$ 010\rangle_{123}$	$ \Psi^-\rangle_{45}$	$ +\rangle_4 -\rangle_5$ 或 $ -\rangle_4 +\rangle_5$	1
$ 100\rangle_{123}$	$ \Phi^+\rangle_{45}$	$ +\rangle_4 +\rangle_5$ 或 $ -\rangle_4 -\rangle_5$	0
$ 111\rangle_{123}$	$ \Psi^+\rangle_{45}$	$ +\rangle_4 -\rangle_5$ 或 $ -\rangle_4 +\rangle_5$	1

态 $X^a Z^b |\Psi\rangle$, 其中 $a, b \in \{0, 1\}$, 即

$$|\Psi_0\rangle = \{\alpha|0\rangle + \beta|1\rangle, \alpha|0\rangle - \beta|1\rangle, \alpha|1\rangle + \beta|0\rangle, \alpha|1\rangle - \beta|0\rangle\}.$$

其次, 在 $|\Psi_0\rangle$ 上进行 T 门评价, 可以得到运算后的密文态 $TX^a Z^b |\Psi\rangle$, 即

$$|\Psi\rangle = \{\alpha|0\rangle + e^{i\pi/4}\beta|1\rangle, \alpha|0\rangle - e^{i\pi/4}\beta|1\rangle, e^{i\pi/4}\alpha|1\rangle + \beta|0\rangle, e^{i\pi/4}\alpha|1\rangle - \beta|0\rangle\}.$$

此时, 需要引入非最大纠缠态, 其形式为 $|\Phi_{12}\rangle = m|00\rangle + n|11\rangle$ ($|m|^2 + |n|^2 = 1$), 该非最大纠缠态的第一个粒子为客户端所持有, 第二个粒子为服务器持有. 再次, 以非最大纠缠态 $|\Phi_{12}\rangle$ 的第二个粒子作为控制位, 以 $|\Psi\rangle$ 作为目标位, 进行CNOT运算, 此时整个系统的状态处于 $(I \otimes \text{CNOT})(|\Phi_{12}\rangle \otimes |\Psi\rangle)$. 最后, 在非最大纠缠态 $|\Phi_{12}\rangle$ 的第一个粒子上依次应用 P^a 门(a 为 X 算子的加密密钥)、 H 门, 此时整个系统的状态处于 $(HP^a \otimes I \otimes I)(I \otimes \text{CNOT})(|\Phi_{12}\rangle \otimes |\Psi\rangle)$. 由于加密密钥 a 的取值不同, 因此进行完以上操作后, 系统的具体状态会出现两种情况, 即 $a = 0$ 和 $a = 1$. 当 $a = 0$ 时,

$$\begin{aligned} & (H \otimes I \otimes I)(I \otimes \text{CNOT})(|\Phi_{12}\rangle \otimes |\Psi\rangle) \\ &= (H \otimes I \otimes \text{CNOT})(|\Phi_{12}\rangle \otimes |\Psi\rangle) \\ &= m(\alpha|0\rangle \pm e^{i\pi/4}\beta|1\rangle)|0\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ &\quad + n(\alpha|1\rangle \pm e^{i\pi/4}\beta|0\rangle)|1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \end{aligned} \quad (6)$$

当 $a = 1$ 时,

$$\begin{aligned} & (HP \otimes I \otimes I)(I \otimes \text{CNOT})(|\Phi_{12}\rangle \otimes |\Psi\rangle) \\ &= (HP \otimes I \otimes \text{CNOT})(|\Phi_{12}\rangle \otimes |\Psi\rangle) \\ &= m(e^{i\pi/4}\alpha|1\rangle \pm \beta|0\rangle)|0\rangle \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ &\quad + n(e^{i\pi/4}\alpha|0\rangle \pm \beta|1\rangle)|1\rangle i \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned} \quad (7)$$

通过对此时系统的第一个粒子和系统的第三个粒子进行测量, 即在此时 $|\Psi\rangle$ 和非最大纠缠态 $|\Phi_{12}\rangle$ 的第一个粒子所在的量子位上执行单粒子 Z 基测量, 测量结果分别表示为 r 和 y , 例如得到测量结果均为 0 , 则系统的第二个粒子将要塌缩为状态 $\frac{1}{\sqrt{2}}(m\alpha|0\rangle \pm e^{i\pi/4}n\beta|1\rangle)$, 更多详细测量结果见文献[21]. 最后, 引入辅助粒子 $|0\rangle$, 同时在辅助粒子 $|0\rangle$ 和非最大纠缠态 $|\Phi_{12}\rangle$ 的第二个粒子上应用酉算子 U , 其定义的矩阵形式为

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & m/n & \sqrt{1-m^2/n^2} \\ 0 & 0 & \sqrt{1-m^2/n^2} & -m/n \end{bmatrix}. \quad (8)$$

以上述测量结果 $\frac{1}{\sqrt{2}}(m\alpha|0\rangle \pm e^{i\pi/4}n\beta|1\rangle)$ 为例,

$$\begin{aligned} & \frac{1}{\sqrt{2}}U(m\alpha|0\rangle \pm e^{i\pi/4}n\beta|1\rangle)|0\rangle \\ &= \frac{1}{\sqrt{2}}\left[m(\alpha|0\rangle \pm e^{i\pi/4}\beta|1\rangle)|0\rangle + e^{i\pi/4}n\beta\sqrt{1-\frac{m^2}{n^2}}|1\rangle|1\rangle\right], \end{aligned}$$

进而对辅助粒子进行测量, 测量结果表示为 t . 根据式子可以观察到, 当辅助粒子处于状态 $|0\rangle$ 时, S 门以 $\frac{m^2}{2}$ 的概率被正确校正, 否则, 校正失败.

通过以上一系列相关操作及测量, 利用非最大纠缠态就可以以 $\frac{m^2}{2}$ 的概率消除 T 门评价造成的错误, 同时根据测量结果 r, y 和加密密钥 $e_k = (a, b)$, 可以得出 $TX^a Z^b |\varphi\rangle = X^{a \oplus r} Z^{a \oplus b \oplus ar \oplus y} T |\varphi\rangle$, 因此 T 门更新后的密钥为 $d_k = (a \oplus r, a \oplus b \oplus ar \oplus y)$.

2.4 量子同态加密

2013年, Liang^[14]正式定义了量子同态加密的完整概念, 并明确了量子同态加密方案的理论框架.

量子同态加密方案包括以下四个阶段: 密钥生成、加密、评价和解密.

(1) 密钥生成: 在此算法中会生成两种密钥, 第一种是加密密钥 e_k , 另一种是评价密钥 ρ_{evk} . 根据密钥更新算法, 使用加密密钥 e_k 可以计算出解密密钥 d_k .

(2) 加密: 我们使用算法Enc作为加密算法, 在量子态 ρ 上执行Enc算法, 输出加密态 $\sigma = \text{Enc}(e_k, \rho)$.

(3) 评价: 我们使用算法Eval作为评价算法, 在加密态 σ 上执行 C_q 计算, 输出评价后的密文态 $\sigma' = \text{Eval}_{\rho_{evk}}(C_q, \sigma)$.

(4) 解密: 我们使用算法Dec作为解密算法, 根据解密密钥 d_k 在加密态 σ' 上执行解密算法, 输出 $\rho' = \text{Dec}(d_k, \sigma')$, 以此获得评价明文态.

3 基于Brown态的多方概率量子同态加密方案

本节提出了一种新的基于Brown态的多方概率量子同态加密方案(BMPQHE), 该方案允许多个客户端同时委托两个服务器进行任意的量子计算, 在同态评价过程中双方不需要进行交互.

在方案中, 客户端需要完成一项巨大的计算任务, 但自身无法胜任, 可以将该任务委托给两个服务器来完成. 如果存在多个客户端, 则可以并行进行任务委托. 方案的参与方分别为客户端、服务器和可信密钥中心. 这里的服务器拥有强大的计算能力, 能够满足用户的需求. 然而, 这些服务器可能并不完全诚实, 存在窃取用户私有数据的风险. 同时引入可信密钥中心Dave, 它是完全诚实的, 与客户端利用B92协议^[31]合

作完成密钥的分发和更新, 以及完成消除 T 门评价错误的相关操作. 假设存在 N 个客户端, 表示为 $Alice_i$, 其中 $i = 1, 2, \dots, N$, 两个用于委托计算的服务器分别为Bob和Charlie. 同时假设客户端想要分享的秘密数据为 n 量子比特.

整体方案由五个阶段组成: 秘密分割阶段、密钥生成阶段、加密阶段、评价阶段和解密阶段. 具体来说, 在秘密分割阶段, 客户端 $Alice_i$ 需要制备Brown态, 并在相应的粒子上执行 Z 基和 X 基测量, 从而完成了秘密分割; 在密钥生成阶段, 多个客户端 $Alice_i$ 和可信密钥中心Dave利用B92协议^[31]完成安全密钥的分发, 从而双方都获得了相同的加密密钥; 在加密阶段, 客户端 $Alice_i$ 使用QOTP技术对秘密数据进行加密并将其分别发给对应的服务器Bob和Charlie, 在此同时, 可信密钥中心Dave需要与每个服务器预共享非最大纠缠态; 在评价阶段, 服务器Bob和Charlie根据量子线路中量子门的顺序在密文态上进行评价并将相应的密文态发送到客户端 $Alice_i$; 在解密阶段, 可信密钥中心Dave根据密钥更新规则进行密钥更新, 生成解密密钥, 并将其发送到客户端 $Alice_i$, 进而客户端根据解密密钥来解密得到同态计算后的明文态. 该方案的具体流程如图1所示.

3.1 秘密分割

在这个阶段, 每个客户端 $Alice_i$ 都制备 n 个Brown态, 在Brown态的前三个粒子上执行 Z 基单粒子测量. 根据2.2节中Brown态的测量属性, 测量完前三个粒子, 第四个粒子和第五个粒子所形成的贝尔态就可以被确定下来, 即知道前三个粒子的测量结果便可以知道第四个粒子和第五个粒子纠缠形成的态. 然后, 第四个粒子和第五个粒子执行 X 基单粒子测量, 从而形成两个粒子集合, 此时粒子集合为 $GH_4^i = \{\rho_i^{GH_{Bob}^k}\}$,

$GH_5^i = \{\rho_i^{GH_{Charlie}^k}\}$, 其中 $k = 1, 2, \dots, n$, 表示秘密数据的第 k 位, 可以获得测量结果集合 $\text{measure}_{GH_4^i} = \{\rho_i^{MR_{Bob}^k}\}$, $\text{measure}_{GH_5^i} = \{\rho_i^{MR_{Charlie}^k}\}$. 根据Brown态前三个粒子的测量结果, 就可以很容易地推出第 i 个客户端 $Alice_i$ ($i = 1, 2, \dots, N$)想要分享的秘密为

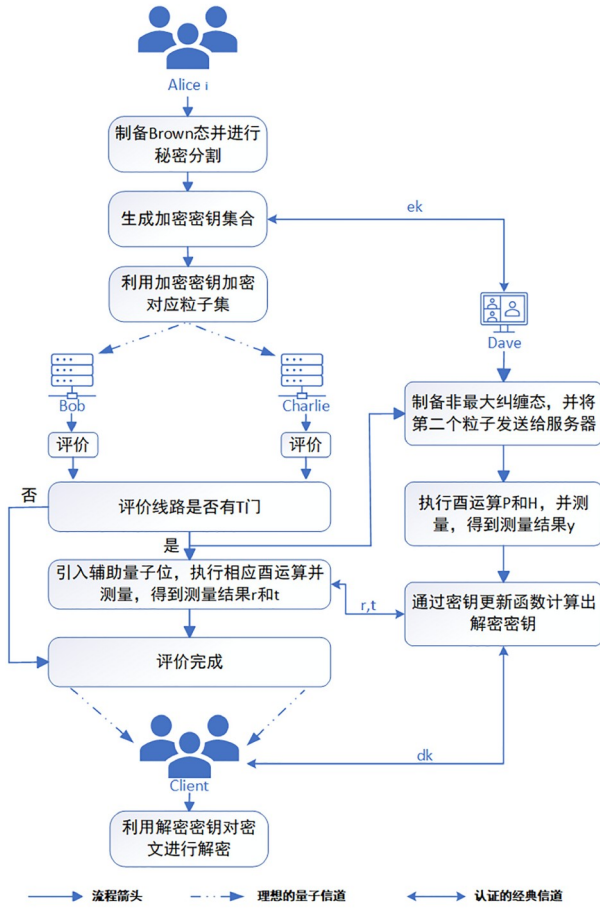


图 1 (网络版彩图)量子同态加密方案流程图

Figure 1 (Color online) The flow chart of quantum homomorphic encryption scheme.

$$K_i = \rho_i^{MR_{Alice}} \oplus \rho_i^{MR_{Bob}}, \quad (9)$$

对于每个 k , 即每位秘密数据, 我们有对应的公式如下:

$$K_i(k) = \rho_i^{MR_{Bob}^k} \oplus \rho_i^{MR_{Charlie}^k}, \quad (10)$$

对于每个 i , 即每个客户端, 过程仍然相同.

3.2 密钥生成

在这个阶段, 每个客户端都需要和可信密钥中心利用B92协议^[31]合作完成安全密钥的分发, 从而双方都获得了相同的加密密钥. 首先, 客户端 $Alice_i$ ($i = 1, 2, \dots, N$) 与可信密钥中心Dave约定好用于密钥生成的态集合 $\{|0\rangle, |+\rangle\}$, 并规定: $|0\rangle$ 编码为二进制经典比特“0”, $|+\rangle$ 编码为二进制经典比特“1”, 即

$$\begin{aligned} |0\rangle &\xrightarrow{\text{编码}} 0, \\ |+\rangle &\xrightarrow{\text{编码}} 1. \end{aligned} \quad (11)$$

客户端 $Alice_i$ ($i = 1, 2, \dots, N$) 随机产生一个量子比特串, 并将其通过量子信道按照一定的时间间隔 Δt 依次传输给可信密钥中心Dave, 其中时间间隔同步可以由多用户量子接入网络(QAN)^[32]技术来实现. 待可信密钥中心Dave接收完所有的量子比特后, 对其进行投影测量, 在测量过程中随机选择测量基. 可信密钥中心Dave通过经典信道告诉客户端 $Alice_i$ ($i = 1, 2, \dots, N$) 哪些操作获得了确定的测量结果, 但是不公布在测量过程中所选择的测量基, 即选取投影算子 $|0\rangle\langle 0|$ 还是 $|+\rangle\langle +|$ 是秘密的. 然后, 根据双方通信的结果, 客户端 $Alice_i$ ($i = 1, 2, \dots, N$) 与可信密钥中心Dave只需要保留得到确定测量结果对应的量子态, 并根据编码规则对保留的量子态进行编码, 作为筛选密钥, 其余量子态丢弃. 客户端 $Alice_i$ ($i = 1, 2, \dots, N$) 与可信密钥中心Dave从原始量子比特串中随机选择部分量子比特进行公开来完成窃听检测, 根据出错率来判断是否有窃听者的存在, 如果出错率在量子信道噪声阈值内, 则对筛选密钥作进一步的加强保密处理, 否则, 说明信道存在窃听者Eve, 需要终止协议, 进而重新发起协议, 重复上述操作.

最终, 双方都获得了相同且安全的加密密钥, 其形式为 $e_{k_i} = (a_i, b_i)$, 其中 $a_i, b_i \in \{0, 1\}^{2n}$. 由于秘密数据进行了分割, 形成了两个粒子集合, 因此在密钥生成阶段, 每个客户端都需要执行两次上述协议, 用于生成两对加密密钥, 即 $e_{k_i}^{Bob}$ 和 $e_{k_i}^{Charlie}$. 对于多个客户端来说, 每个客户端可以依次与可信密钥中心Dave完成密钥的协商, 操作过程相同.

3.3 加密

在这个阶段, 需要完成两项任务: 第一, 客户端对秘密数据进行加密; 第二, 可信密钥中心与服务器预共享非最大纠缠态. 将依次执行下面两步操作:

(1) 加密: 客户端 $Alice_i$ ($i = 1, 2, \dots, N$) 使用上一阶段生成的加密密钥 $e_{k_i}^{Bob} = (a_i, b_i)$, $e_{k_i}^{Charlie} = (a_i, b_i)$ 和量子一次一密技术分别对分割后粒子集合 GH_4^i 和 GH_5^i ,

即 $\rho_i^{GH_{\text{Bob}}^k}$ 和 $\rho_i^{GH_{\text{Charlie}}^k}$ 进行加密. 此后, 客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$ 就得到了两个加密的粒子集 $\rho_i^{GH_{\text{Bob}}^k}$ 和 $\rho_i^{GH_{\text{Charlie}}^k}$, 并将其和同态评价的量子线路 C_q 分别发送给服务器 Bob 和 Charlie .

(2) 预共享: 假设量子通用线路由量子门集和 $G = \{X, Z, H, S, T, \text{CNOT}\}$ 中的门组成, 其中 T 为非 Clifford 门, 在同态评价阶段会产生相位门错误, 因此必须要消除错误. 在这里, 与之前不同的是, 客户端不再制备预共享的非最大纠缠态, 而是可信密钥中心 Dave 需要制备非最大纠缠态, 其形式为 $|\Phi_{12}\rangle = x|00\rangle + y|11\rangle (|x|^2 + |y|^2 = 1)$, 并将其第二个粒子发送到服务器, 此时已经完成了预共享, 即可信密钥中心持有非最大纠缠态 $|\Phi_{12}\rangle$ 的第一个粒子, 服务器持有非最大纠缠态 $|\Phi_{12}\rangle$ 的第二个粒子.

3.4 评价

在这个阶段, 服务器会根据客户端的量子线路对密文态进行同态评价, 并将相应的密文态发送到客户端. 首先, 服务器 Bob 和 Charlie 不仅会接收到非最大纠缠态 $|\Phi_{12}\rangle$ 的第二个粒子, 还会接收到客户端发来的评价线路 C_q 和密文粒子集, 此时服务器 Bob 接收到的密文粒子集形式为 $\rho_1^{GH_{\text{Bob}}^k} \otimes \rho_2^{GH_{\text{Bob}}^k} \otimes \dots \otimes \rho_i^{GH_{\text{Bob}}^k} \otimes \dots \rho_N^{GH_{\text{Bob}}^k}$, 服务器 Charlie 接收到的密文粒子集形式为 $\rho_1^{GH_{\text{Charlie}}^k} \otimes \rho_2^{GH_{\text{Charlie}}^k} \otimes \dots \otimes \rho_i^{GH_{\text{Charlie}}^k} \otimes \dots \rho_N^{GH_{\text{Charlie}}^k}$. 之后, 服务器 Bob 和 Charlie 会根据客户端的量子线路 C_q 对密文态进行同态评价. 假设量子线路 C_q 包括 p 个量子门, 依次为 $\text{Gate}[1], \text{Gate}[2], \dots, \text{Gate}[p]$, 其中存在 q 个 T 门. 对于每一个 $g \in \{1, 2, \dots, p\}$, 有两种情况发生:

当 $\text{Gate}[g] \notin T$, 那么服务器 Bob 和 Charlie 会直接将根据量子线路 C_q 在密文上依次应用量子门, 得到分别评价之后的密文粒子集 $\rho_i^{GH_{\text{Bob}}^k}$ 和 $\rho_i^{GH_{\text{Charlie}}^k}$;

当 $\text{Gate}[g] \in T$, 那么就需要利用预共享的非最大纠缠态来解决 T 门评价产生的错误. 这里对 2.3 节进行优化, 与之前不同的是, 这里需要服务器和可信密钥中心完成各自的操作任务: 第一为服务器进行相关操作, 首先, 服务器 Bob 和 Charlie 将 T 门应用于密文粒子

集, 得到分别经过 T 门评价之后的密文粒子集 $\rho_{iT}^{GH_{\text{Bob}}^k}$ 和 $\rho_{iT}^{GH_{\text{Charlie}}^k}$; 其次, 以非最大纠缠态 $|\Phi_{12}\rangle$ 的第二个粒子作为控制位, 以经过 T 门评价之后的密文粒子集作为目标位, 应用 CNOT 门, 测量此时的量子位密文粒子集, 测量结果记为 r_i ; 最后, 引入辅助粒子 $|0\rangle$, 同时在辅助粒子 $|0\rangle$ 和非最大纠缠态 $|\Phi_{12}\rangle$ 的第二个粒子上应用酉算子 U , 进而对辅助粒子进行测量, 测量结果记为 t_i . 第二为可信密钥中心进行相关操作, 可信密钥中心 Dave 将在非最大纠缠态 $|\Phi_{12}\rangle$ 的第一个粒子上依次应用 P^{a_i} 门 (a_i 为 X 算子的加密密钥)、 H 门, 并进行测量, 测量结果记为 y_i . 完成上述操作后, 此时的非最大纠缠态 $|\Phi_{12}\rangle$ 的第一个粒子就是经过 T 门评价校正之后的密文粒子集 $\rho_i^{GH_{\text{Bob}}^k}$ 和 $\rho_i^{GH_{\text{Charlie}}^k}$.

评价完所有量子线路 C_q 后, 将密文粒子集 $\rho_i^{GH_{\text{Bob}}^k}$ 和 $\rho_i^{GH_{\text{Charlie}}^k}$ 以及相应的测量结果 t_i 发送到相应的客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$, 同时将测量结果 r_i 发送给可信密钥中心 Dave .

3.5 解密

在解密阶段, 关键的任务就是可信密钥中心完成密钥更新和客户端完成解密. 将依次执行下面两步操作:

(1) 密钥更新: 可信密钥中心 Dave 将要根据密钥更新函数、量子线路 C_q 以及加密密钥 $e_{k_i} = (a_i, b_i)$ 计算出解密密钥, 其形式为 $d_{k_i} = (a'_i, b'_i)$, 其中 $a'_i, b'_i \in \{0, 1\}^{2n}$, 并将其发送给相应的客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$. 由于秘密数据进行了分割, 形成了两个粒子集合, 从而在密钥更新时, 可信密钥中心更新的解密密钥的数量对应于加密密钥的数量, 因此每个客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$ 都会接收到两对解密密钥, 即 $d_{k_i}^{\text{Bob}}$ 和 $d_{k_i}^{\text{Charlie}}$. 其中, 密钥更新函数为

- (i) 如果 $\text{Gate}[g] = X$ 或 $\text{Gate}[g] = Z$, $e_{k_i} = (a_i, b_i) \rightarrow d_{k_i} = (a'_i, b'_i) = (a_i, b_i)$;
- (ii) 如果 $\text{Gate}[g] = H$, $e_{k_i} = (a_i, b_i) \rightarrow d_{k_i} = (a'_i, b'_i) = (b_i, a_i)$;

- (iii) 如果 $\text{Gate}[g] = S$, $e_{k_i} = (a_i, b_i) \rightarrow d_{k_i} = (a'_i, b'_i) = (a_i, a_i \oplus b_i)$;
- (iv) 如果 $\text{Gate}[g] = \text{CNOT}$, $e_{k_i} = (a_i, b_i, c_i, d_i) \rightarrow d_{k_i} = (a'_i, b'_i, c'_i, d'_i) = (a_i, b_i \oplus d_i, a_i \oplus c_i, d_i)$;
- (v) 如果 $\text{Gate}[g] = T$, $e_{k_i} = (a_i, b_i) \rightarrow d_{k_i} = (a'_i, b'_i) = (a_i \oplus r_i, a_i \oplus b_i \oplus a_i r_i \oplus y_i)$.

在特殊情况下, 即在完成 T 门评价后, 可信密钥中心会接收到服务器发来的测量结果 r_i , 再加上自己所持有的测量结果 y_i 和加密密钥 $e_{k_i} = (a_i, b_i)$, 根据 2.3 节中的 T 门更新密钥函数, 便可以很容易算出解密密钥 $d_{k_i} = (a_i \oplus r_i, a_i \oplus b_i \oplus a_i r_i \oplus y_i)$.

(2) 解密: 经过上述阶段后, 客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$ 会接收到由服务器 Bob 和 Charlie 发来的经过同态评价之后的密文粒子集 $\rho_i^{GH^k_{\text{Bob}}}$, $\rho_i^{GH^k_{\text{Charlie}}}$ 和测量结果 t_i 以及由可信密钥中心 Dave 发来的解密密钥 $d_{k_i} = (a'_i, b'_i)$. 在此同时, 客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$ 可以根据测量 t_i 来判断 T 门的错误是否被正确校正, 在利用非最大纠缠态来校正错误的过程中, 成功的概率为 $\frac{x^2}{2}$. 之后, 客户端 $\text{Alice}_i (i = 1, 2, \dots, N)$ 利用 QOTP 和解密密钥 $d_{k_i} = (a'_i, b'_i)$ 对密文粒子集 $\rho_i^{GH^k_{\text{Bob}}}$ 和 $\rho_i^{GH^k_{\text{Charlie}}}$ 进行解密, 就可以得到同态评价之后的明文粒子集.

4 分析

本节主要分析了所提方案的正确性、全同态性和安全性. 其中, 正确性是最关键的部分, 全同态性能够表明该方案适用于通用量子线路, 安全性能够保证秘密信息和密钥不会被泄露.

4.1 正确性分析

定理1 如果可信密钥中心、客户端和服务端在秘密分割、密钥生成、加密、评价、解密阶段能够诚实地执行, 客户端可以得到正确的结果.

证明 在所提方案中, 对于客户端输入明文 ω , 加密密钥 $e_k = (a, b)$, 量子线路为 C_q , 同态评价应该满足

$$\text{VerDec}\left(\text{Eval}_{\rho_{\text{evk}}}^{C_q}(\text{Enc}(\text{Split}(\omega)))\right) = \Phi_{C_q}(\omega), \quad (12)$$

其中, $\text{VerDec}\left(\text{Eval}_{\rho_{\text{evk}}}^{C_q}(\text{Enc}(\text{Split}(\omega)))\right)$ 表示明文数据在执行完秘密分割、密钥生成、加密、评价、解密阶段后的结果, $\Phi_{C_q}(\omega)$ 表示量子线路 C_q 直接作用在明文数据上的结果. 如果可信密钥中心、客户端和服务端在秘密分割、密钥生成、加密、评价、解密阶段能够诚实地执行, 则两者的结果应该是相等的.

具体地说, 首先, 客户端进行制备相关量子态并进行测量; 其次, 客户端与可信密钥中心利用 B92 协议^[31] 合作完成密钥分发来生成安全的密钥; 然后, 客户端使用 QOTP 对分割后的秘密数据进行加密, 同时可信密钥中心与服务器预共享非最大纠缠态; 再次, 在评价阶段, 服务器根据量子线路中量子门的顺序在密文态上进行评价并发送给客户端, 评价过程中, 如果量子门为 Clifford 门, 因具有与泡利组进行交换的特征, 因此不会产生任何错误, 进而很容易更新密钥完成同态评价, 如果量子门为 T 门, 就可以利用非最大纠缠态来消除错误, 这样就可以完全保证同态评价的正确性, 即客户端可以获得正确的评价之后的密文; 最后, 客户端使用可信密钥更新出的解密密钥来得到同态计算后的明文. 因此, 如果可信密钥中心、客户端和服务端能够诚实地执行所提方案, 即按照上述操作执行, 这样在密文上做完计算解密后的结果就会等于直接在明文上计算的结果, 便证明了方案的正确性.

4.2 全同态分析

定理2 所提方案是全同态的, 可以实现对任何量子线路的量子同态加密, 即适用于通用量子线路.

证明 众所周知, 任意量子线路都是由 Clifford 门和 T 门组成, 即 $G = \{X, Z, H, S, T, \text{CNOT}\}$. 不失一般性, 假设在方案中所使用的量子线路为 $C_q = \Omega_1 \otimes T_2 \otimes \Omega_3 \otimes \dots \otimes \Omega_n$, 作用于 n 量子比特 $|\omega\rangle = |\omega_1\rangle \otimes |\omega_2\rangle \otimes |\omega_3\rangle \otimes \dots \otimes |\omega_n\rangle$ 加密后的密文态, 即在第一个量子位 $|\omega_1\rangle$ 上应用 Ω_1 , 在第二个量子位 $|\omega_2\rangle$ 上应用 T 门, 依次应用到相应的量子位. 同时假设加密密钥为 $e_k = (a, b)$, 其中 $a, b \in \{0, 1\}^{2n}$, 解密密钥 $d_k = (a', b')$, 其中 $a', b' \in \{0, 1\}^{2n}$. 在整个过程中, 以下等式成立:

$$\begin{aligned}
 & C_q X^a Z^b |\omega\rangle \\
 &= (\Omega_1 \otimes T_2 \otimes \Omega_3 \otimes \cdots \otimes \Omega_n) \\
 & \quad (X^{a_1} Z^{b_1} |\omega_1\rangle \otimes X^{a_2} Z^{b_2} |\omega_2\rangle \\
 & \quad \otimes X^{a_3} Z^{b_3} |\omega_3\rangle \otimes \cdots \otimes X^{a_n} Z^{b_n} |\omega_n\rangle) \\
 &= \Omega_1 X^{a_1} Z^{b_1} |\omega_1\rangle \otimes T_2 X^{a_2} Z^{b_2} |\omega_2\rangle \\
 & \quad \otimes \Omega_3 X^{a_3} Z^{b_3} |\omega_3\rangle \otimes \cdots \otimes \Omega_n X^{a_n} Z^{b_n} |\omega_n\rangle \\
 &= X^{a_1} Z^{b_1} \Omega_1 |\omega_1\rangle \otimes X^{a_2} Z^{b_2} T_2 |\omega_2\rangle \\
 & \quad \otimes X^{a_3} Z^{b_3} \Omega_3 |\omega_3\rangle \otimes \cdots \otimes X^{a_n} Z^{b_n} \Omega_n |\omega_n\rangle \\
 &= X^a Z^b C_q |\omega\rangle. \tag{13}
 \end{aligned}$$

在解密阶段, 只要将解密密钥和QOTP应用于式(13)结果, 客户端最终可以得到解密结果, 这与直接将量子线路应用于明文量子态的结果相同, 在理论上证明了方案的正确性. 在此同时, 由于所提方案中 C_q 可以是任意的量子线路, 即通用量子线路, 包括Clifford门和 T 门, 因此证明了该方案能够实现对任意量子线路的量子同态加密, 即具有全同态性.

4.3 安全性分析

定理3 所提方案是信息论安全性的, 能够保证关于明文数据和密钥的任何信息不会被泄露.

证明 在所提方案中, 加密和解密都是使用的一次一密技术^[33,34], QOTP只依赖于物理机制, 而不依赖于经典的数学复杂难题. 假设明文是 n 量子比特 $|\omega\rangle = |\omega_1\rangle \otimes |\omega_2\rangle \otimes |\omega_3\rangle \otimes \cdots \otimes |\omega_n\rangle$, 密文是 n 量子比特 $|\omega'\rangle = |\omega_1'\rangle \otimes |\omega_2'\rangle \otimes |\omega_3'\rangle \otimes \cdots \otimes |\omega_n'\rangle$, QOTP的加密算子是 $X^a Z^b$, 加密密钥 $a, b \in \{0, 1\}^{2n}$ 是随机生成的, 并且只使用一次. 以下等式成立:

$$\begin{aligned}
 & |\omega'\rangle \langle \omega'| \\
 &= |\omega_1'\rangle \langle \omega_1'| \otimes |\omega_2'\rangle \langle \omega_2'| \otimes |\omega_3'\rangle \langle \omega_3'| \\
 & \quad \otimes \cdots \otimes |\omega_n'\rangle \langle \omega_n'| \\
 &= X^{a_1} Z^{b_1} |\omega_1\rangle \langle \omega_1| (X^{a_1} Z^{b_1})^\dagger \otimes X^{a_2} Z^{b_2} |\omega_2\rangle \\
 & \quad \cdot \langle \omega_2| (X^{a_2} Z^{b_2})^\dagger \otimes X^{a_3} Z^{b_3} |\omega_3\rangle \langle \omega_3| (X^{a_3} Z^{b_3})^\dagger \\
 & \quad \otimes \cdots \otimes X^{a_n} Z^{b_n} |\omega_n\rangle \langle \omega_n| (X^{a_n} Z^{b_n})^\dagger \\
 &= \frac{1}{2^{2n}} \sum_{a, b \in \{0, 1\}^{2n}} X^a Z^b |\omega\rangle \langle \omega| (X^a Z^b)^\dagger \\
 &= \frac{I_{2^n}}{2^n}, \tag{14}
 \end{aligned}$$

由式(14)可知, 客户端对明文量子态 $|\omega\rangle$ 进行QOTP加密后, 得到的密文量子态 $|\omega'\rangle$ 是处于完全混合态的, 因此服务器和外部窃听者无法获取关于明文量子态 $|\omega\rangle$ 和密钥 $e_k = (a, b)$ 的任何信息.

具体来说, 在秘密分割阶段, 明文数据一直处于客户端持有, 没有任何传输的过程, 因此不会受到任何攻击. 在密钥生成阶段, 密钥分发的过程中可以通过误码率来判断是否存在窃听者, 同时可采用虚拟互无偏基^[35]进行分析密钥速率、传输距离和安全性, 并且B92协议被证明可以抵御窃听攻击^[36]. 在加密阶段, 客户端使用QOTP技术对明文进行加密, 会得到处于完全混合态的密文, 从其中得不到任何有用的信息. 在评价阶段, 服务器接收到的仍然是处于完全混合态的密文, 由于服务器或者窃听者没有关于密钥的任何信息, 因此他们不能正确解密. 在解密阶段, 完全诚实的可信密钥中心会通过认证的经典信道将解密密钥发送给客户端用于解密. 在所提方案的整个过程, 都会受到QOTP的保护.

5 仿真分析

在本节中, 使用提出的量子同态加密方案, 在本源量子云平台上实现四量子位量子同态加密的仿真实验.

仿真实验中所使用的量子线路包含7个量子比特 $q[0], q[1], q[2], q[3], q[4], q[10]$ 和 $q[16]$, 其中前四个量子比特为数据位, 后三个量子比特为校正 T 门评价错误时的辅助量子位, 初始状态都为 $|0\rangle$. 泡利算子 X 可以使状态 $|0\rangle$ 转化为状态 $|1\rangle$, 因此可以使用泡利算子 X 来设置不同的明文态. 仿真实验中设置初始明文态为 $|\omega\rangle = |1010\rangle$, 同态评价所使用的量子线路为 $C_q = (ZS/ZP)_1 \otimes \text{CNOT}_{12} \otimes (XH)_3 \otimes T_4$, 作用于四量子比特 $|\omega\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle$ 加密后的密文态, 其中 CNOT_{12} 表示第一量子位为控制位, 第二量子位为目标位. 同时假设随机选取的加密密钥为 $e_k = \{(0, 0), (0, 1), (1, 1), (1, 0)\}$, 根据密钥更新规则, 可以计算出解密密钥 $d_k = \{(0, 1), (0, 1), (1, 1), (1 \oplus r, 1 \oplus r \oplus y)\}$, 具体更新过程如表2所示.

表 2 仿真实验的密钥更新过程

Table 2 The key update process for the simulation experiment

量子比特	e_k	S_1/P_1	Z_1	CNOT_{12}	H_3	X_3	T_4	d_k
$q[0]$	(0, 0)	(0, 0)	(0, 0)	(0, 1)	—	—	—	(0, 1)
$q[1]$	(0, 1)	—	—	(0, 1)	—	—	—	(0, 1)
$q[2]$	(1, 1)	—	—	—	(1, 1)	(1, 1)	—	(1, 1)
$q[3]$	(1, 0)	—	—	—	—	—	$(1 \oplus r, 1 \oplus r \oplus y)$	$(1 \oplus r, 1 \oplus r \oplus y)$

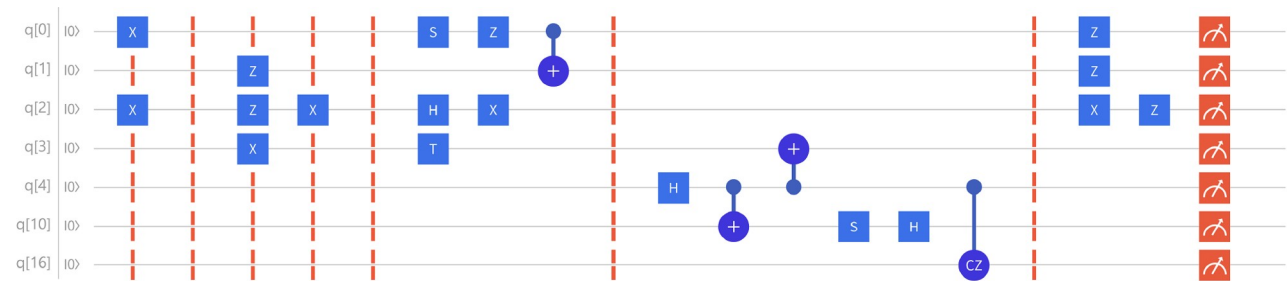


图 2 (网络版彩图)量子线路图
Figure 2 (Color online) The diagram of the quantum circuit.

当评价的量子线路中包含 T 门时, 需要预共享非最大纠缠态 $|\Phi_{12}\rangle$ 并引入辅助量子位. 因实验平台功能有限, 不能成功制备非最大纠缠态, 但可以通过 H 门和 CNOT 门制备最大纠缠态, 此时取 $|\Phi_{12}\rangle = x|00\rangle + y|11\rangle$ ($|x|^2 + |y|^2 = 1$) 的特殊情形, 即最大纠缠态 $|\Phi_{12}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, 来代替非最大纠缠态 $|\Phi_{12}\rangle$. 两种状态在仿真实验中作用相同, 原理相同, 不影响仿真实验的效果和正确性. 整个量子同态加密方案的仿真线路如图 2 所示, 其中明文量子态设置、加密、同态评价、 T 门校正、解密和测量分别用长虚线隔开.

仿真线路的运行效果如图 3 所示, 其中横轴代表量子态, 纵轴代表测量结果的概率. 由于第五量子位(因第四量子位的评价结果会出现在第五量子位)的解密密钥取决于测量结果 r 和 y , 因此在仿真过程中无法直接在线路中解密. 由图可知, 第一、二、三量子位的运行结果为分别以 50% 的概率处于态 $|111\rangle$ 和 $|110\rangle$, 第四、五、六、七量子位的运行结果为分别以 25% 的概率

率处于态 $|1000\rangle$, $|0100\rangle$, $|1010\rangle$ 和 $|0110\rangle$, 通过计算可得第五量子位(即数据第四量子位)的解密结果为态 $|0\rangle$. 综上所述, 经过同态评价后的四量子比特明文数据位为以 50% 的概率处于态 $|1110\rangle$, 以另外 50% 的概率处于

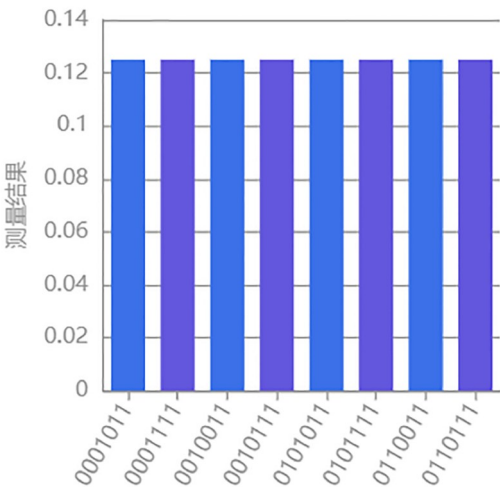


图 3 (网络版彩图)量子线路的运行结果
Figure 3 (Color online) The result of the quantum circuit.

态 $|1100\rangle$, 这与评价线路 C_q 直接作用在明文量子态 $|\omega\rangle$ 的结果相同.

6 结论

在论文中, 我们基于Brown态提出了一个全同态和信息论安全的多方概率量子同态加密方案, 并在本源量子云平台上实现了四量子位量子同态加密的仿真实验. 该方案通过利用预共享的非最大纠缠态作为辅助资源来非交互式地解决 T 门同态评价时发生的错误,

进而利用Brown态的属性将单客户端单服务器模式扩展为多客户端多服务器模式, 此外, 方案还引入了可信密钥中心, 与客户端利用B92协议^[31]合作完成密钥的分发和更新, 以及完成消除 T 门评价错误的相关操作. 在整个过程中, QOTP保证了秘密数据不会被泄露.

在此同时, 我们希望所构造的方案可以更加适用于量子分布式网络, 加快大规模量子信息安全高效传输的建设. 在以后的工作中, 可以尝试进一步利用更多量子属性来优化过程, 提升量子同态加密方案的效率.

参考文献

- 1 Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms. *Found Secure Comput*, 1978, 4: 169–180
- 2 Gentry C. A Fully Homomorphic Encryption Scheme. Manhattan: Stanford University, 2009
- 3 Goldwasser S, Kalai Y T, Rothblum G N. Delegating computation: Interactive proofs for muggles. *J ACM*, 2015, 62: 1–64
- 4 Goldwasser S, Kalai Y, Popa R A, et al. Reusable garbled circuits and succinct functional encryption. In: *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*. Palo Alto, 2013. 555–564
- 5 Garg S, Gentry C, Halevi S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits. *SIAM J Comput*, 2016, 45: 882–929
- 6 Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Santa Fe: IEEE, 1994. 124–134
- 7 Giovannetti V, Lloyd S, Maccone L. Quantum private queries. *Phys Rev Lett*, 2008, 100: 230502
- 8 Shang T, Wang S, Jiang Y, et al. Two-round quantum homomorphic encryption scheme based on matrix decomposition. *Quantum Inf Process*, 2023, 22: 422
- 9 Chen X B, Sun Y R, Xu G, et al. Quantum homomorphic encryption scheme with flexible number of evaluator based on (k, n) -threshold quantum state sharing. *Inf Sci*, 2019, 501: 172–181
- 10 Shen A, Cao X Y, Wang Y, et al. Experimental quantum secret sharing based on phase encoding of coherent states. *Sci China-Phys Mech Astron*, 2023, 66: 260311
- 11 Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation. In: *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*. Atlanta: IEEE, 2009. 517–526
- 12 Morimae T, Fujii K. Blind topological measurement-based quantum computation. *Nat Commun*, 2012, 3: 1036
- 13 Rohde P P, Fitzsimons J F, Gilchrist A. Quantum walks with encrypted data. *Phys Rev Lett*, 2012, 109: 150501
- 14 Liang M. Symmetric quantum fully homomorphic encryption with perfect security. *Quantum Inf Process*, 2013, 12: 3675–3687
- 15 Fisher K A G, Broadbent A, Shalm L K, et al. Quantum computing on encrypted data. *Nat Commun*, 2014, 5: 3074
- 16 Broadbent A, Jeffery S. Quantum homomorphic encryption for circuits of low T -gate complexity. In: *Proceedings of the Annual Cryptology Conference*. Berlin, Heidelberg: Springer, 2015. 609–629
- 17 Dulek Y, Schaffner C, Speelman F. Quantum homomorphic encryption for polynomial-sized circuits. In: *Proceedings of the Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference*. Santa Barbara: Springer, 2016. 3–32
- 18 Alagic G, Dulek Y, Schaffner C, et al. Quantum fully homomorphic encryption with verification. In: *Proceedings of the Advances in Cryptology-ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security*. Hong Kong: Springer International Publishing, 2017. 438–467
- 19 Ouyang Y, Tan S H, Fitzsimons J F. Quantum homomorphic encryption from quantum codes. *Phys Rev A*, 2018, 98: 042334
- 20 Liang M. Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security. *Quantum Inf Process*,

- 2020, 19: 28
- 21 Zhang J W, Chen X B, Xu G, et al. Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme. *Chin Phys B*, 2021, 30: 070309
- 22 Zhang J W, Chen X B, Xu G, et al. A secure multiparty quantum homomorphic encryption scheme. *Comput Mater Continua*, 2022, 73: 2835–2848
- 23 Chang W, Li Z Z, You F C, et al. Dynamic quantum fully homomorphic encryption scheme based on universal quantum circuit. *J Inf Secur Appl*, 2023, 75: 103510
- 24 Pan X, Lei Y T, Li X, et al. Cross quantum homomorphic encryption based on the butterfly network. *Phys Rev A*, 2024, 109: 062606
- 25 Yu L, Pérez-Delgado C A, Fitzsimons J F. Limitations on information-theoretically-secure quantum homomorphic encryption. *Phys Rev A*, 2014, 90: 050303
- 26 Newman M, Shi Y. Limitations on transversal computation through quantum homomorphic encryption. arXiv: [1704.07798](https://arxiv.org/abs/1704.07798)
- 27 Lai C Y, Chung K M. On statistically-secure quantum homomorphic encryption. arXiv: [1705.00139](https://arxiv.org/abs/1705.00139)
- 28 Lv M Y, Hu X M, Gong N F, et al. Demonstration of controlled high-dimensional quantum teleportation. *Sci China-Phys Mech Astron*, 2024, 67: 230311
- 29 Yan P S, Zhou L, Zhong W, et al. Advances in quantum entanglement purification. *Sci China-Phys Mech Astron*, 2023, 66: 250301
- 30 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2001
- 31 Bennett C H. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett*, 1992, 68: 3121–3124
- 32 Huang C, Chen Y, Luo T, et al. A cost-efficient quantum access network with qubit-based synchronization. *Sci China-Phys Mech Astron*, 2024, 67: 240312
- 33 Boykin P O, Roychowdhury V. Optimal encryption of quantum bits. *Phys Rev A*, 2003, 67: 042317
- 34 Ambainis A, Mosca M, Tapp A, et al. Private quantum channels. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science. Redondo Beach: IEEE, 2000. 547–553
- 35 Li H W, Hao C P, Chen Z J, et al. Security of quantum key distribution with virtual mutually unbiased bases. *Sci China-Phys Mech Astron*, 2024, 67: 270313
- 36 Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices. In: Proceedings of the International Symposium on Information Theory. Chicago: IEEE, 2004. 136

Multi-party probabilistic quantum homomorphic encryption scheme based on Brown state

LIU MingKui, LI ZhenZhen^{*}, GAO Bo, DING HaiYang & LI ZiChen

Digital Rights Management Research Center, Beijing Institute of Graphic Communication, Beijing 102600, China

**Corresponding author (email: lizhenzhen1101@163.com)*

Quantum homomorphic encryption allows computations to be performed directly on encrypted data, ensuring the security of private information. A novel multi-party probabilistic quantum homomorphic encryption scheme based on the Brown state is proposed in this study, which permits multiple clients to simultaneously delegate arbitrary quantum computations to two servers. Firstly, the trusted key center is introduced to collaborate with clients using the B92 protocol for key distribution and updating, as well as to perform operations that eliminate T -gate evaluation errors. Secondly, the proposed scheme employs pre-shared non-maximally entangled states as auxiliary resources to non-interactively address errors occurring during the homomorphic evaluation of T -gate. Lastly, the scheme leverages the properties of Brown state to extend the single-client single-server model to the multi-client multi-server model, making it more suitable for quantum distributed networks and enhancing its practicality. Moreover, this study theoretically proves the correctness, fully homomorphic nature, and information-theoretically security of the scheme. Simulations conducted on the Origin Quantum Cloud platform further validate the scheme's effectiveness. As the proposed scheme can realize homomorphic computation of any quantum circuit, it is particularly well-suited for delegated computation in quantum cloud networks.

quantum homomorphic encryption, non-maximally entangled state, Brown state, non-interactive, delegated computation

PACS: 03.67.-a, 03.67.Dd, 03.67.Hk, 03.67.Lx

doi: [10.1360/SSPMA-2024-0355](https://doi.org/10.1360/SSPMA-2024-0355)