中国科学: 物理学 力学 天文学 2025 年 第 55 卷 第 4 期: 240319
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文 量子密码和量子计算专题

云服务器量子数据秘密共享方案

昌燕[1,2,3], 刘洪林[1,2,3], 苟智坚[1,2,3*], 宋子扬[1,2,3], 赵银山[1,2,3], 段光明[1,2,3], 李鹏亮[1,2,3]

1. 成都信息工程大学网络空间安全学院, 成都 610225
2. 成都信息工程大学, 先进密码技术与系统安全四川省重点实验室, 成都 610225
3. 先进微处理器技术国家工程研究中心(工业控制与安全分中心), 成都 610225
*联系人, E-mail: gzj@cuit.edu.cn

收稿日期: 2024-10-29; 接受日期: 2025-01-17; 网络出版日期: 2025-03-13
国家自然科学基金(编号: 62272068, 62076042)、国家重点研发计划(编号: 2022YFB3103103)和四川省科技项目(2023YFS0419)资助

摘要 数据以量子态的形式存储在云服务器中可以成倍地提高存储效率. 量子数据在云服务器上的存储和共享需要考虑安全问题. 一个聪明的解决方案是将数据以密文的形式存储在云服务器中. 当需要将数据共享给用户时, 云服务器对数据密文进行第二次加密, 并将加密后的密文发送给用户. 用户可以使用自己的私钥解密并获取数据本身. 这个过程可以看作是数据所有者的密文由第三方(云服务器)转换为共享的密文. 本文提出了一种新的云服务器量子数据共享方案. 我们的主要贡献之一是实现了与具有适当权限的用户共享特定数据(满足某些基于属性的条件). 从密钥分析、明文分析、一级密文分析和二级密文分析等方面证明了该方案的安全性.

关键词 量子数据共享, 云服务器, 条件代理重加密, 属性

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

1 引言

1.1 背景

将数据外包给云服务器, 用户可以拥有更好的存储容量和更容易的数据共享, 但是需要考虑外包数据的保密性, 因为所有者不希望未经授权的用户访问数据[1,2]. 例如, 在邮件转发系统[3]中, 发送方使用Alice的公钥对邮件进行加密, 将密文发送给Alice并将其存储在邮件服务器中. 但是, 由于某种原因, Alice可能无法及时处理邮件. 她希望邮件服务器可以将密文转发给她的秘书(Bob), 以帮助她处理邮件. 因此, 如何在不解密的情况下将Alice的密文转换为Bob的密文, 同时不泄露Alice的密钥和对应的明文, 成为一个非常具有挑战性的问题[4].

为了解决密文转发问题, 代理重加密的概念[3]在1998年的欧洲密码学年会上被Blaze等人提出. 代理重加密在传统公钥加密系统的基础上增加了一个代理. 代理可以根据Alice的授权将Alice的密文转换为Bob的密文而无需解密, 代理无法获得对应的明文. Ateniese等人给出了代理重加密的规范化定义, 并提出了第一个代理重加密方案[5], 该方案无法杜绝双向授权, 即代理不仅可以将Alice的密文转换为Bob的密文, 还可以

引用格式: 昌燕, 刘洪林, 苟智坚, 等. 云服务器量子数据秘密共享方案. 中国科学: 物理学 力学 天文学, 2025, 55: 240319
Chang Y, Liu H, Gou Z, et al. Cloud server quantum data secret sharing scheme (in Chinese). Sci Sin-Phys Mech Astron, 2025, 55: 240319, doi: 10.1360/SSPMA-2024-0513

© 2025《中国科学》杂志社

将Bob的密文转换为Alice的密文. Ateniese等人提出的单向授权代理重加密方案[5]中，代理只能单向将Alice的密文转换为Bob的密文, 不能反向将Bob的密文转换为Alice的密文, 与双向授权方案[5]相比, 有更好的安全性和更多的应用场景. 为了简化代理重加密方案中的公钥基础设施，基于身份公钥加密方案的代理重加密方案[6]被提出, 在该方案中如果代理和接收方合谋, 不仅可以获得明文, 还可以获得被授权人的密钥, 因此该方案无法抵抗合谋攻击.

在上述代理重加密方案[4–9]中，代理能够将Alice的所有密文转化成Bob的密文，然而在实际应用中, Alice可能仅仅希望将符合某种条件的而不是所有的密文转发给Bob. 为了使Alice能够灵活控制需要转发的密文，Weng等人提出了条件代理重加密[10]，在该方案中, 只有满足一定条件的密文才能被代理重加密. 为了满足特定应用场景，随后又提出了条件更丰富的代理重加密方案[11–24]，如基于身份的条件代理重加密[16]和基于属性的条件代理重加密[17]. Tang等人提出了一种基于属性的可验证条件代理重加密方案[22]，允许数据在满足特定属性条件时被授权用户解密. Hou等人提出了一种抗量子攻击的多特征属性代理重加密[23]，该方案引入了同态签名技术来实现重加密的可验证性. Liu等人提出了一种基于证书的代理重加密增强方案[24]. 然而，以上代理重加密方案都是在经典公钥加密体系的基础上设计的，其安全性依赖于经典公钥密码体系的安全性, 无法抵御量子计算攻击.

在量子计算[25–31]领域，基于量子力学原理的量子信息，理论上可以突破经典世界的存储、计算和通信的限制，给研究者带来了无限的视野. 量子密码学[32–54]是量子信息的一个重要分支，它为信息安全带来了许多新的解决方案，可以从信息论的角度实现最佳的安全性. 关于数据共享，已经有许多量子密码协议被提出来保证共享数据的机密性，如量子加密协议[32–38]、量子秘密共享协议(QSS)[39–50]和量子同态加密算法(QHE)[51]等. 代理属性重加密在云存储的现实背景下有很多实际的应用需求，但是目前关于云环境下数据共享的量子密码协议是非常缺乏的，因此研究云环境下基于量子技术的代理属性重加密方法是非常有理论价值和实际意义的. 本文提出的方案, 是一个云环境下的量子数据的秘密共享方案，能实现具有特定权限的用户共享特定数据(满足某些基于属性的条件), 具有信息论安全性, 整体安全性高于经典密码, 虽然在量子态的存储上存在困难，但是这个困难几乎是所有量子密码协议和量子算法的共性困难.

1.2　我们的贡献

(1) 提出了一种基于云服务器的量子数据秘密共享方案. 量子数据以密文形式存储在云服务器上. 在所有者授权用户后，云服务器将对密文进行第二次加密并将其提供给用户. 用户可以使用自己的私钥对加密后的密文进行解密, 从而获得共享的量子数据.

(2) 提出了一种云服务器上量子数据秘密共享的条件方案. 解密密钥与授权用户的条件相关. 通过对云服务器发送的二次加密密文进行解密，只有符合条件的用户才能获得共享量子数据的明文.

2　一种基于云服务器的量子数据共享方案

2.1　理论基础

一个包含变量θ的2×2酉矩阵描述为

$$U(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}. \tag{1}$$

如果对量子态$|\varphi\rangle=(\cos a|0\rangle+\sin a|1\rangle)$进行$U(\theta)$操作, 该量子态变化为

$$\begin{aligned}U(\theta)|\varphi\rangle &= U(\theta)(\cos a|0\rangle+\sin a|1\rangle)\\ &= \cos(a+\theta)|0\rangle+\sin(a+\theta)|1\rangle.\end{aligned} \tag{2}$$

对任意两个变量θ_a和θ_b, 有如下推导:

$$\begin{aligned}U(\theta_a)U(\theta_b) &= \begin{pmatrix}\cos\theta_a & -\sin\theta_a\\ \sin\theta_a & \cos\theta_a\end{pmatrix}\begin{pmatrix}\cos\theta_b & -\sin\theta_b\\ \sin\theta_b & \cos\theta_b\end{pmatrix}\\ &= \begin{pmatrix}\cos(\theta_a+\theta_b) & -\sin(\theta_a+\theta_b)\\ \sin(\theta_a+\theta_b) & \cos(\theta_a+\theta_b)\end{pmatrix}\\ &= U(\theta_a+\theta_b),\end{aligned} \tag{3}$$

进一步, 我们得到

$$\begin{aligned}&U(\theta_a)U(\theta_b)|\varphi\rangle\\ &= U(\theta_a+\theta_b)(\cos a|0\rangle+\sin a|1\rangle)\\ &= \cos(a+\theta_a+\theta_b)|0\rangle+\sin(a+\theta_a+\theta_b)|1\rangle.\end{aligned} \tag{4}$$

2.2　协议

(1) 方案的目标

Alice将数据编码在量子态序列$\{|\varphi_i\rangle \mid |\varphi_i\rangle = \cos\alpha_i|0\rangle + \sin\alpha_i|1\rangle, i = 1,2,...,N\}$上, $\{|\varphi_i\rangle\}$的密文$\{|\varphi_i{}^*\rangle\}$存储在量子云服务器(称为代理)上. Alice和代理事先共享密钥K_P, Alice和Bob事先共享密钥K_B. 代理通过K_P将$\{|\varphi_i{}^*\rangle\}$重加密为Bob的密文$\{|\varphi_i{}^*\rangle_B\}$, Bob通过$K_B$解密$\{|\varphi_i{}^*\rangle_B\}$可以共享$\{|\varphi_i\rangle\}$.

(2) 初始化

F是一个无限域. Alice定义一个三变量方程$x_1 + x_2 + x_3 = 1$, 其中x_1, x_2, x_3为F中非零元素[46,47]. Alice选择任意元素$\delta \in F, \delta \neq 0$. $\{x_1, x_2, x_3, \delta\}$仅Alice私有.

(3) 加密

Alice在$\{|\varphi_i\rangle\}$的每个量子态上进行$U(\theta_A)$操作, 得到密文序列$\{|\varphi_i{}^*\rangle\} = \{U(\theta_A)|\varphi_i\rangle\}$, 其中$\theta_A = 2\pi - \delta + \delta x_1$. Alice将$\{|\varphi_i{}^*\rangle\}$存储在量子云服务器上.

(4) 密钥产生

Alice生成密钥$K_P = \delta x_2$和$K_B = \delta x_3$, 然后利用量子安全直接通信秘密发送K_P和K_B分别给代理和Bob.

(5) 重加密

代理对$\{|\varphi_i{}^*\rangle\}$的每个量子态进行$U(K_P)$操作, 得到量子态序列

$$\{|\varphi_i{}^*\rangle_B\} = \{U(K_P)|\varphi_i{}^*\rangle\} = \{U(K_P)U(\theta_A)|\varphi_i\rangle\}.$$

代理方随机从集合$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$中选择诱骗粒子, 并将诱骗粒子随机插入量子态序列$\{|\varphi_i{}^*\rangle_B\}$中形成有序序列$\{|\varphi_i{}^{*\prime}\rangle_B\}$, 代理将$\{|\varphi_i{}^{*\prime}\rangle_B\}$发送给Bob. 待Bob收到$\{|\varphi_i{}^{*\prime}\rangle_B\}$后, 代理方告诉Bob $\{|\varphi_i{}^{*\prime}\rangle_B\}$中诱骗粒子的位置和测量基, Bob按照代理方给的位置抽取出诱骗粒子, Bob用代理方告知的测量基按顺序对诱骗粒子进行测量, Bob将测量结果发送给代理方, 代理方比对测量结果. 当误码率低于根据信道噪声设定的阈值时, 判定为没有窃听, 协议可以继续.

(6) 解密

Bob对$\{|\varphi_i{}^*\rangle_B\}$的每个量子态进行$U(K_B)$操作, 得到量子态序列

$$\{U(K_B)|\varphi_i{}^*\rangle_B\} = \{U(K_B)U(K_P)U(\theta_A)|\varphi_i\rangle\} = \{|\varphi_i\rangle\}.$$

(7) 方案的正确性

在Alice加密之后, 初始的单个量子位状态$|\varphi_i\rangle$成为第一级密文$U(\theta_A)|\varphi_i\rangle$. 经过代理重加密后第一级密文$U(\theta_A)|\varphi_i\rangle$变成了第二级密文$U(K_P)U(\theta_A)|\varphi_i\rangle$. 当Bob用私钥$K_B$解密$U(K_P)U(\theta_A)|\varphi_i\rangle$之后, 该量子态变为$U(\theta_A)|\varphi_i\rangle$. 根据$U(\theta_A)$操作的特性, 我们有如下推导:

$$\begin{aligned}
&U(K_B)U(K_P)U(\theta_A)|\varphi_i\rangle \\
&= U(K_B + K_P + \theta_A)|\varphi_i\rangle \\
&= U(\delta x_3 + \delta x_2 + 2\pi - \delta + \delta x_1)|\varphi_i\rangle \\
&= U(2\pi)|\varphi_i\rangle \\
&= |\varphi_i\rangle.
\end{aligned} \tag{5}$$

3　云服务器上量子数据秘密共享的条件方案

3.1　协议

(1) 方案的目标

Alice拥有带有属性的数据. 这些数据的密文存储在量子云服务器上. Alice希望与具有适当权限的用户共享特定的数据. 例如, Alice想与计算机系的老师共享计算机系的数据, 这意味着其他系的老师无法访问计算机系的数据. 如果Bob是计算机系的老师, 他可以访问计算机系的数据. Bob无法访问其他部门的数据. 在该方案中, 数据被编码为带有属性的量子态. 代理(云服务器)通过对带有属性的量子态密文进行重新加密, 帮助Alice和Bob成功完成上述任务.

(2) 初始化

我们定义以下量子叠加态$|I_{ij}\rangle$来表示带有属性的数据, 其中$|a_j\rangle$表示属性, $|d_i\rangle$表示数据:

$$\begin{aligned}
&|I_{ij}\rangle = |d_i\rangle \otimes |a_j\rangle, \ i = 1,2,...,N, j = 1,2,...,M, \\
&|d_i\rangle = \cos\theta_i|0\rangle + \sin\theta_i|1\rangle, \theta_i \in [0, \pi/2].
\end{aligned} \tag{6}$$

Alice拥有一个由量子态序列$\{|I_{ij}\rangle\}$组成的数据序列. 她将$\{|I_{ij}\rangle\}$的密文$\{|I_{ij}{}^{*}\rangle\}$存储在云服务器上. 在代理重新加密数据的密文之后, Alice可以与Bob$_j$共享满足属性条件$|a_j\rangle$的量子态$\{|I_{ij}\rangle\}$.

Alice随机选取一个无限域F, 并且定义j个三变量等式: $f_j: x_1+x_{2j}+x_{2j+1}=1,\ j=1,2,...,M$, 其中$x_1, x_{2j}, x_{2j+1}\ (j=1,2,...,M)\in F$是非零元素, 且彼此不同. $\{x_1, x_{2j}, x_{2j+1}\ (j=1,2,...,M)\}$仅Alice私有[46,47].

(3) 密钥生成

Alice选择任意元素$\delta\in F, \delta\neq 0$, 并定义私钥$K_{Pj}=\delta x_{2j}-a_j$和$K_{Bj}=\delta x_{2j+1}$, 其中$j=1,2,...,M$. 这里, δ仅Alice私有. Alice通过QSDC将K_{Pj}发送给代理, 将K_{Bj}发送给Bob$_j$.

(4) 加密

Alice对$\{|I_{ij}\rangle\}$的每个量子比特执行$U(\theta_A)$操作, 其中$\theta_A=2\pi-\delta+\delta x_1$, 获得密文序列$\{|I_{ij}{}^{*}\rangle\}=\{U(\theta_A)|I_{ij}\rangle\}$, 并将密文序列$\{|I_{ij}{}^{*}\rangle\}$存储在云服务器上.

(5) 重加密

代理对$\{|I_{ij}{}^{*}\rangle\}$的每个量子态进行$U(K_{Pj})$操作, 得到量子态序列

$$\{|I_{ij}{}^{*}\rangle_B\}=\{U(K_{Pj})|I_{ij}{}^{*}\rangle\}=\{U(K_{Pj})U(\theta_A)|I_{ij}\rangle\}.$$

代理方随机从集合$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$中选择诱骗粒子, 并将诱骗粒子随机插入量子态序列$\{|I_{ij}{}^{*}\rangle_B\}$中形成有序序列$\{|I_{ij}{}^{*\prime}\rangle_B\}$, 代理将$\{|I_{ij}{}^{*\prime}\rangle_B\}$发送给Bob$_j$. 待Bob$_j$收到$\{|I_{ij}{}^{*\prime}\rangle_B\}$后, 代理方告诉Bob$_j$ $\{|I_{ij}{}^{*\prime}\rangle_B\}$中诱骗粒子的位置和测量基, Bob$_j$按照代理方给的位置抽取出诱骗粒子, Bob$_j$用代理方告知的测量基按顺序对诱骗粒子进行测量, Bob$_j$将测量结果发送给代理方, 代理方比对测量结果. 当误码率低于根据信道噪声设定的阈值时, 判定为没有窃听, 协议可以继续.

(6) 解密

Bob$_j$对$\{|I_{ij}{}^{*}\rangle_B\}$的每个量子态进行$U(K_{Bj}+a_j)$操作, 得到量子态序列

$$\{U(K_{Bj}+a_j)|I_{ij}{}^{*}\rangle_B\}$$
$$=\{U(K_{Bj}+a_j)U(K_{Pj})U(\theta_A)|I_{ij}\rangle\}=\{|I_{ij}\rangle\}.$$

(7) 完整性验证

存储在云服务器上的数据需要定期审计, 以防止损坏或篡改. 在Bob$_j$接收并解密共享数据后, 他需要验证数据是否被损坏或篡改. Bob$_j$测量属性状态a_j, 并将结果与他拥有的属性进行比较. 如果它们是相同的, 在某种程度上, 数据被认为没有被破坏或篡改.

(8) 方案的正确性

在Alice加密之后, 初始的单个量子位状态$|I_{ij}\rangle$成为第一级密文$U(\theta_A)|I_{ij}\rangle$. 经过代理重加密后第一级密文$U(\theta_A)|I_{ij}\rangle$变成了第二级密文$U(K_{Pj})U(\theta_A)|I_{ij}\rangle$. 当Bob$_j$用私钥$K_{Bj}+a_j$解密$U(K_{Pj})U(\theta_A)|I_{ij}\rangle$之后, 该量子态变为$U(K_{Bj}+a_j)U(K_{Pj})U(\theta_A)|I_{ij}\rangle$. 根据$U(\theta_A)$操作的特性, 我们有如下推导:

$$\begin{aligned}&U(K_{Bj}+a_j)U(K_{Pj})U(\theta_A)|I_{ij}\rangle\\&=U(K_{Bj}+a_j+K_{Pj}+\theta_A)|I_{ij}\rangle\\&=U(\delta x_{2j+1}+a_j+\delta x_{2j}-a_j+2\pi-\delta+\delta x_1)|I_{ij}\rangle\\&=U(2\pi)|I_{ij}\rangle\\&=|I_{ij}\rangle.\end{aligned}\tag{7}$$

3.2　基于条件代理重加密的方案示例

本文提出的云服务器量子数据秘密共享的条件方案流程如图1所示. Alice拥有由量子态$\{|I_{ij}\rangle, i=1,2,3,4, j=1,2\}$组成的数据序列:

$$\begin{aligned}&|I_{11}\rangle=|d_1\rangle\otimes|a_1\rangle,\\&|I_{21}\rangle=|d_2\rangle\otimes|a_1\rangle,\\&|I_{31}\rangle=|d_3\rangle\otimes|a_1\rangle,\\&|I_{42}\rangle=|d_4\rangle\otimes|a_2\rangle.\end{aligned}\tag{8}$$

Alice要将符合条件$|a_1\rangle$的数据共享给Bob$_1$, 将

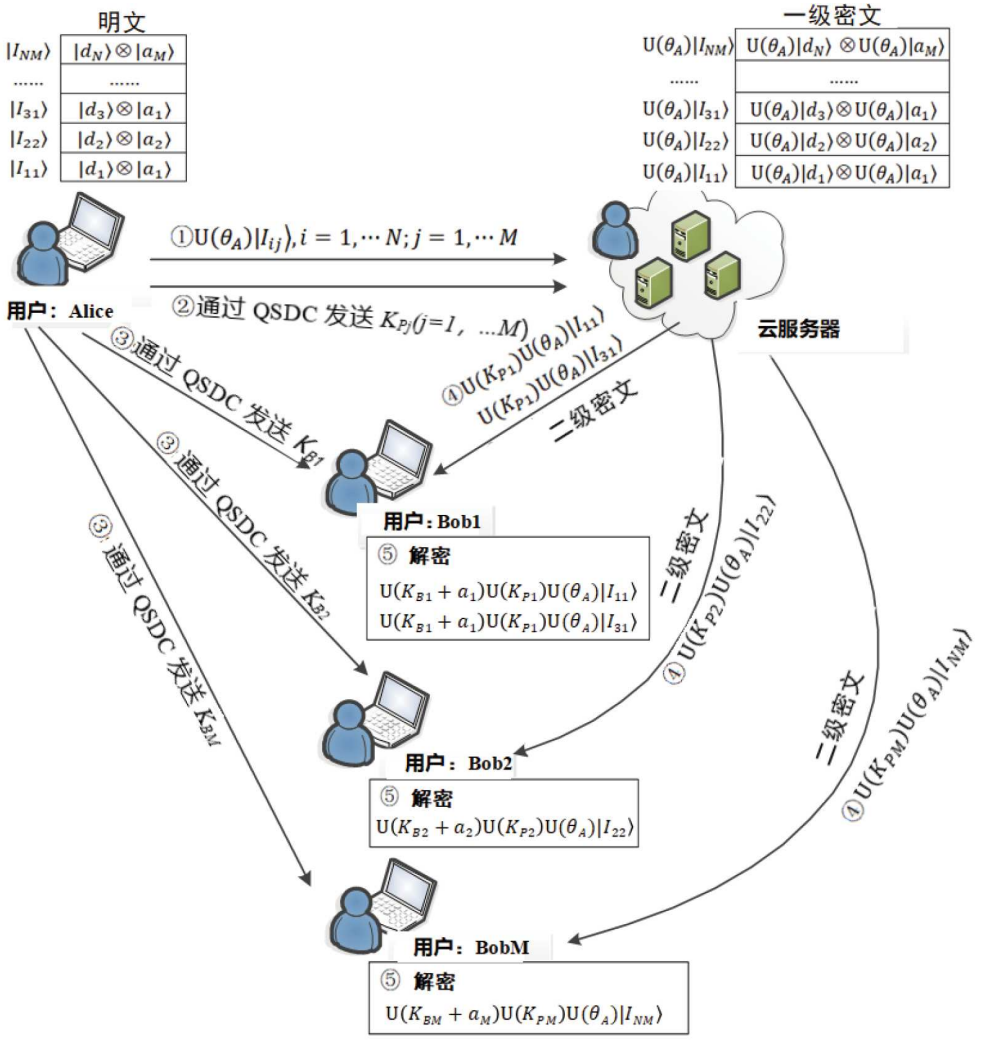


图 1　(网络版彩图)协议结构
Figure 1　(Color online) Protocol structure.

符合条件$|a_2\rangle$的数据共享给Bob$_2$. 也就是说, Alice要将$\left\{|I_{ij}\rangle \mid j=1\right\}=\{|I_{11}\rangle,|I_{21}\rangle,|I_{31}\rangle\}$共享给Bob$_1$, 将$\left\{|I_{ij}\rangle \mid j=2\right\}=\{|I_{42}\rangle\}$共享给Bob$_2$.

Alice随机选择无限域F, 并定义2个三变量等式$f_1: x_1+x_2+x_3=1$, $f_2: x_1+x_4+x_5=1$, 其中$x_1,x_2,x_3,x_4,x_5\in F$非零且互不相等. $\{x_1,x_2,x_3,x_4,x_5\}$仅Alice私有.

Alice随机选择非零元素$\delta\in F$, 并定义私钥$K_{Pj}=\delta x_{2j}-a_j$和$K_{Bj}=\delta x_{2j+1}$, 其中$j=1,2$, 且δ仅Alice私有. Alice发送K_{Pj}给代理, 发送K_{Bj}给Bob.

Alice通过对$\left\{|I_{ij}\rangle\right\}=\{|I_{11}\rangle,|I_{21}\rangle,|I_{31}\rangle,|I_{42}\rangle\}$的每一个态进行$U(\theta_A)$操作得到密文序列$\left\{|I_{ij}^*\rangle\right\}=\left\{U(\theta_A)|I_{ij}\rangle\right\}=\left\{U(\theta_A)\mid I_{11}\rangle, U(\theta_A)\mid I_{21}\rangle, U(\theta_A)\mid I_{31}\rangle, U(\theta_A)|I_{42}\rangle\right\}$, 其中$\theta_A=2\pi-\delta+\delta x_1$. Alice将$\left\{|I_{ij}^*\rangle\right\}$存储在云服务器上.

代理对$\left\{|I_{ij}^*\rangle\right\}$的每个态进行$U(K_{Pj})$操作, 得到Bob的密文序列:

$$\begin{aligned}\left\{\left|I_{ij}{}^{*}\right\rangle_B\right\} &= \left\{U(K_{Pj})\left|I_{ij}{}^{*}\right\rangle\right\}\\ &= \left\{U(K_{P1})U(\theta_A)|I_{11}\rangle, U(K_{P1})U(\theta_A)|I_{21}\rangle,\right.\\ &\quad \left. U(K_{P1})U(\theta_A)|I_{31}\rangle, U(K_{P2})U(\theta_A)|I_{42}\rangle\right\}.\end{aligned}$$

代理发送$\left\{\left|I_{ij}{}^{*}\right\rangle_B\right\}$给Bob. Bob对$\left\{\left|I_{ij}{}^{*}\right\rangle_B\right\}$的每个态进行$U(K_{Bj}+a_j)$操作, 得到$\left\{U(K_{Bj}+a_j)\left|I_{ij}{}^{*}\right\rangle_B\right\}$:

$$\begin{aligned}&\left\{U(K_{Bj}+a_j)\left|I_{ij}{}^{*}\right\rangle_B\right\}\\ &= \left\{U(K_{Bj}+a_j)U(K_{Pj})U(\theta_A)\left|I_{ij}\right\rangle\right\}\\ &= \left\{U(K_{B1}+a_1)U(K_{P1})U(\theta_A)|I_{11}\rangle,\right.\\ &\quad U(K_{B1}+a_1)U(K_{P1})U(\theta_A)|I_{21}\rangle,\\ &\quad U(K_{B1}+a_1)U(K_{P1})U(\theta_A)|I_{31}\rangle,\\ &\quad \left.U(K_{B2}+a_2)U(K_{P2})U(\theta_A)|I_{42}\rangle\right\}\\ &= \left\{U(K_{B1}+a_1+K_{P1}+\theta_A)|I_{11}\rangle,\right.\\ &\quad U(K_{B1}+a_1+K_{P1}+\theta_A)|I_{21}\rangle,\\ &\quad U(K_{B1}+a_1+K_{P1}+\theta_A)|I_{31}\rangle,\\ &\quad \left.U(K_{B2}+a_2+K_{P2}+\theta_A)|I_{42}\rangle\right\}\\ &= \left\{U(\delta x_3+a_1+\delta x_2-a_1+2\,\pi-\delta+\delta x_1)|I_{11}\rangle,\right.\\ &\quad U(\delta x_3+a_1+\delta x_2-a_1+2\,\pi-\delta+\delta x_1)|I_{21}\rangle,\\ &\quad U(\delta x_3+a_1+\delta x_2-a_1+2\,\pi-\delta+\delta x_1)|I_{31}\rangle,\\ &\quad \left.U(\delta x_5+a_2+\delta x_4-a_2+2\,\pi-\delta+\delta x_1)|I_{42}\rangle\right\}\\ &= \left\{|I_{11}\rangle, |I_{21}\rangle, |I_{31}\rangle, |I_{42}\rangle\right\}. \end{aligned} \tag{9}$$

4　模拟实验

实验使用Python库的pyqpanda来实现模拟电路. 由于在经典硬件上模拟量子电路时, 内存需求会随着量子电路的量子比特数和电路深度的增长而指数级增长, 因此, 本文设计如图2所示的6量子位电路, 实现表1中三条数据记录的基于学院属性的秘密共享, 验证基于云服务器的量子数据秘密共享方案的可行性. q_0, q_2, q_4 三个量子位分别编码序号为1, 2, 3的三条数据记录的数据部分, q_1, q_3, q_5三个量子位分别编码序号为1, 2, 3的三条数据记录的属性部分(学院信息). 编码层电路采用角度编码和基态编码策略将数据和属性信息分别编码到量子态上, 加密层电路完成Alice对数据的初始加密(加密密钥为θ_A, 加密操作为Ry门), 代理重加密层电路完成代理对数据的重加密(重加密密钥为K_{Pj}, 加密操作为控制Ry门), 解密层电路完成Bob对密文数据的解密(重加密密钥为K_{Bj}, 加密操作为Ry门).

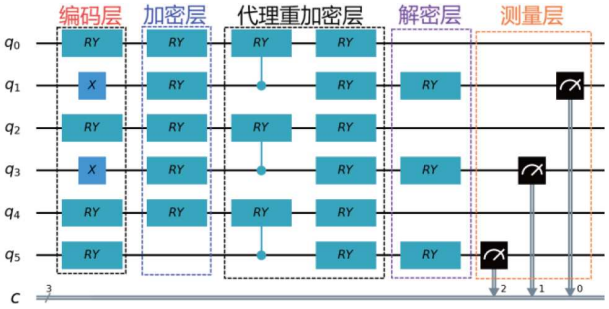


图 2　(网络版彩图) 6量子位电路图
Figure 2　(Color online) Six qubit circuit chart.

表 1　人员信息表
Table 1　Personnel information form

序号	姓名	性别	学院
1	张三	男	网络安全学院
2	李四	女	网络安全学院
3	王五	女	计算机学院

本实验要验证: 如果Bob是计算机学院的老师, 即Bob拥有计算机学院属性, 那么他可以正确解密序号为3的数据记录, 无法正确解密序号为1和2的数据记录; 如果Bob是网络安全学院的老师, 即Bob拥有网络安全学院属性, 那么他可以正确解密序号为1和2的数据记录, 无法正确解密序号为3的数据记录.

定义经典数据0代表属性值计算机学院, 1代表属性值网络安全学院. $\{x_1, x_2, x_3, x_4, x_5, \delta\}$的取值为$\{-0.8, 0.2, 1.6, -0.2, 2, 3.14\}$. 图3和4分别展示了对$q_5, q_3, q_1$三个量子位进行100次测量后的测量结果分布. 下面分两种情况分析图3和4的实验结果.

情况1: Bob是计算机学院老师. Bob对q_5, q_3, q_1三个量子位分别进行测量的测量结果分布如图3所示. 000, 001, 010, 011表示多次测量q_5量子位的结果都是0, 而q_3, q_1量子位的结果是0和1的不确定组合. 出现这种情况的原因是由于Bob正确解密了序号为3的数据记录, 所以得到了准确的数据属性, 但是无法正确解密序号为1和2的数据记录, 所以测量结果不确定.

情况2: Bob是网络安全学院的老师. Bob

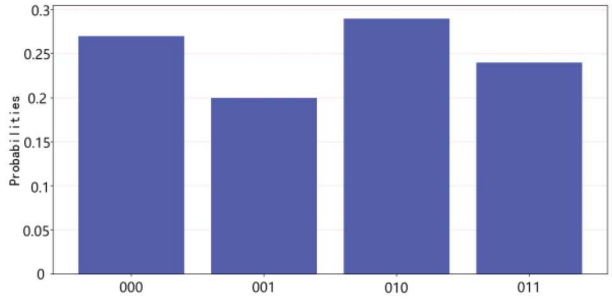


图 3　(网络版彩图) Bob是计算机学院老师时的测量结果分布图

Figure 3　(Color online) The distribution chart of measurement results when Bob is a teacher in the School of Computer.

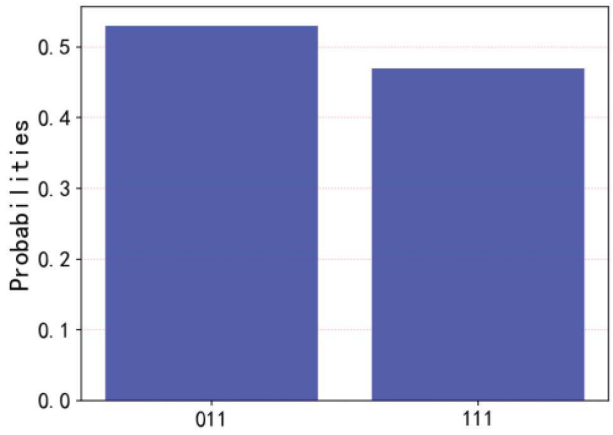


图 4　(网络版彩图) Bob是网络安全学院老师时的测量结果分布图

Figure 4　(Color online) The distribution chart of measurement results when Bob is a teacher in the School of Cyber Security.

对q_5,q_3,q_1三个量子位分别进行测量的测量结果分布如图4所示. 111, 011表示多次测量q_1和q_3量子位的结果都是11, 而q_5量子位的结果不确定, 可能为0, 可能为1. 出现这种情况的原因是由于Bob正确解密了序号为1和2的数据记录, 所以得到了准确的数据属性, 但是无法正确解密序号为3的数据记录, 所以测量结果是不确定.

当$\{x_1,x_2,x_3,x_4,x_5,\delta\}$取其他值时, q_5,q_3,q_1的测量结果分布也呈现出相同的规律, 即当Bob是计算机学院老师时, 多次测量q_5量子位的结果都是0, 而q_3,q_1量子位的结果是0和1的不确定组合; 当Bob是网络安全学院的老师时, 多次测量q_3,q_1量子位的结果都是11, 而q_5量子位的结果可能是0, 可能是1.

5　安全分析

提出的基于条件代理重加密的量子数据共享方案, 实现了与具有相应权限的用户的特定数据共享, 特别是满足基于属性条件的数据共享. 例如, 存储在云服务器上的计算机部门的数据可以与计算机部门的教师共享. 然而, 其他部门的教师无法访问计算机部门的数据. 因此, 我们从私钥的安全性、明文的安全性、一级密文的安全性、二级密文的安全性等方面对方案的安全性进行了分析.

5.1　私钥的安全性

在密钥生成阶段, 密钥$\theta_A=2\pi-\delta+\delta x_1$, $K_{Pj}=\delta x_{2j}-a_j$和$K_{Bj}=\delta x_{2j+1}$由Alice定义, 用于生成这些密钥的元素$\{\delta,x_1,x_{2j},x_{2j+1}\}$由Alice选择, 并且只有Alice知道. 在密钥传输阶段, K_{Pj}和K_{Bj}通过量子安全直接通信的方式分别发送给代理和Bob$_j$, 保证了密钥传输过程中的安全性.

除了Alice之外, 每个参与者都无法根据他或她所知道的信息推导出其他人的密钥. 例如, 代理不能导出Bob$_j$的密钥, 因为他不知道δ和x_{2j+1}. 代理不能导出Alice的密钥, 因为他不知道也不能导出δ和x_1. 因此, 代理无法得知存储在云上的数据, 因为, 一旦他对云上的数据进行测量, 很大概率会选错测量基, 从而导致测量结果错误, 同时造成原始量子态状态的改变, 从而在审计的过程中被发现. 同样的道理, 除代理方之外的其他数据窃取者, 也无法获取存储在云上的数据. 数据在传送过程中和在云上存储的安全性保障都是基于量子不可克隆和测不准原理, 因此本文算法具有信息论安全性, 整体安全性高于经典密码.

5.2　明文的安全性

明文序列由Alice用密钥$\theta_A=2\pi-\delta+\delta x_1$进行加密, 然后存储在云服务器上. Alice存储在云服务器上的密文称为一级密文. 一级密文有两种解密方法: 一种是, Alice可以用她的密钥$\theta_A=2\pi-\delta+\delta x_1$进行$U(-\theta_A)$运算来解密一级密文; 另一种是, 首先代理用自己的密钥$K_{Pj}=\delta x_{2j}-a_j$执行$U(K_{Pj})$操作, 然后Bob$_j$用自己的密钥K_{Bj}和自己拥有的属性a_j执行$U(K_{Bj}+a_j)$操作. 也就是

说, Alice单独, 或者Bob$_j$与代理合作, 可以胜任这件事. 要获得明文数据, 需要单独知道θ_A, 或者同时知道K_{Pj}, K_{Bj}和a_j.

此外, 只有具有属性a_j的用户才能访问满足基于属性的条件a_j的数据序列$\left\{\left|I_{ij}\right\rangle\right\}$, 因为只有他/她可以构造解密密钥($K_{Bj}+a_j$). 例如, Bob$_k$拥有属性$a_k$, 他可以访问数据序列$\left\{\left|I_{ij}\right\rangle \,\middle|\, j=k\right\}$, 但是他不能访问数据序列$\left\{\left|I_{ij}\right\rangle \,\middle|\, j\neq k\right\}$.

存储在云上的数据需要定期审计, 以防止被损坏或篡改. 在Bob$_j$接收并解密共享数据后, 他需要验证数据是否被损坏或篡改. Bob$_j$测量属性状态$\left|a_j\right\rangle$并将结果与他拥有的属性进行比较. 如果它们是相同的, 在某种程度上, 明文数据被认为没有被破坏或篡改. 因此, 任何非法操作都会导致密文量子态序列发生变化, 这些变化将在一致性检测(完整性验证)阶段被发现.

5.3　一级密文的安全性

利用量子非克隆定理和测不准原理, 保证了存储在云服务器上的一级密文量子态序列的安全性. 任何非法操作(包括克隆、测量、损坏和篡改)都会导致密文量子态序列发生变化, 这些变化将在一致性检测(完整性验证)阶段被发现.

5.4　二级密文的安全性

在第二级密文量子态序列传输到Bob$_j$之前, 在序列中插入诱饵粒子, 发现非法操作, 确保第二级密文序列安全传输到Bob$_j$. 因此, 在这个过程中, 如果攻击者拦截了一些粒子, 用伪造的粒子重新发送加密序列, 就可以利用诱饵粒子检测攻击者.

5.5　讨论

条件代理重加密依赖于属性匹配, 下面针对属性冲突和高维数据情况下可能带来的安全性问题进行讨论.

属性冲突一般发生在不同云内的用户相互跨云访问对方数据, 而每个云的访问控制策略不同时. 解决这个问题的常见方法是通过属性映射, 统一各云的访问控制策略. 为解决属性冲突, 可以通过增加经典的属性映射模块, 先统一各云的访问控制策略, 再实施本文方案, 实现量子和经典混合的云数据条件属性共享方案, 方案的整体安全性不受影响.

本文方案同样适用于云上存储的数据是高维数据, 但是查询条件是固定某属性的情况. 在这种情况下, 只需要将高维数据编码为量子叠加态. 这里以包含{“姓名”, “性别”, “院系”}等三个属性的数据集S为例来描述高维数据的条件属性量子共享方案. 假设S = {{“张三”, “男”, “计算机学院”}, {“李四”, “女”, “网络安全学院”}, {“王五”, “男”, “计算机学院”}}, 只按“院系”属性进行授权访问, 那么每条数据记录编码为一个叠加态. 设分别用$d_1=\{d_{11},d_{12},d_{13}\}$, $d_2=\{d_{21},d_{22},d_{23}\}$, $d_3=\{d_{31},d_{32},d_{33}\}$表示$S$中的三条记录, 其中$d_{ik}$ $(i,k=1,2,3)$表示第i条记录的第k个属性. 那么构成数据序列的量子态$\left|I_{ij}\right\rangle=\left|d_i\right\rangle\left|a_j\right\rangle$中的$\left|d_i\right\rangle$可以表示为叠加态$\left|d_i\right\rangle=\frac{1}{\sqrt{p}}\sum_{k=1}^{p}\left|k\right\rangle\left(\cos\theta_{ik}\left|0\right\rangle+\sin\theta_{ik}\left|1\right\rangle\right)$, 其中$\sin\theta_{ik}=d_{ik}$. 数据序列$\left\{\left|I_{ij}\right\rangle\right\}$经Alice加密后的密文序列$\left\{\left|I_{ij}{}^{*}\right\rangle\right\}$存储在云服务器上. 当Alice对存储在云上的数据进行定期审计时, 为降低测量复杂叠加态$\left|d_i\right\rangle=\frac{1}{\sqrt{p}}\sum_{k=1}^{p}\left|k\right\rangle\left(\cos\theta_{ik}\left|0\right\rangle+\sin\theta_{ik}\left|1\right\rangle\right)$的难度, Alice可以只测量表示条件属性的粒子$\left|a_j\right\rangle$, 通过$\left|a_j\right\rangle$的测量结果判断数据是否被窃取或损坏, 方案的整体安全性不受影响.

6　结论

综上所述, 我们提出了一种基于代理重加密和条件代理重加密的云服务器量子数据共享方案. 在该方案中, 代理对量子态数据的密文进行重新加密后, 可以将特定的数据(满足一定的基于属性的条件)与具有相应权限的用户共享. 虽然本文算法没有用到量子纠缠特性, 但是用到了量子不可克隆和测不准原理, 因此本文算法具有信息论安全性, 整体安全性高于经典密码. 存储在代理云上的量子态形式的数据, 需要定期审计, 虽然经典数据是编码在了量子态的角度上, 加解密操作也是通过角度旋转来实现, 但是如果代理云在不知道解密密钥的情况下对量子态进行测量就会有很大的概率导致测量结果错误, 同时造成原始量子

态状态的改变, 从而在审计的过程中被发现. 量子态存储是本文实现的难点, 同时也是绝大部分量子密码协议及量子算法的共性困难. 降低密码协议或算法在量子态存储方面的实现难度, 是我们后续研究的重点. 另外, 利用量子的方式生成代理重加密和解密的密钥也是该领域的一个很好的研究方向, 利用量子纠缠态的纠缠特性努力提升量子态的共享信息承载量和共享灵活性是该方向研究需要解决的主要问题.

参考文献

1 Zhang Y, Xu C, Lin X, et al. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. IEEE Trans Cloud Comput, 2021, 9: 923–937

2 Gao X, Yu J, Shen W T, et al. Achieving low-entropy secure cloud data auditing with file and authenticator deduplication. Inf Sci, 2021, 546: 177–191

3 Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In: Advances in Cryptology—EUROCRYPT'98. Berlin, Heidelberg: Springer, 1998. 127–144

4 Ge C P. Research on Several Problems of Proxy Re-encryption (in Chinese). Dissertation for Doctoral Degree. Nanjing: Nanjing University of Aeronautics and Astronautics, 2016 [葛春鹏. 代理重加密若干问题研究. 博士学位论文. 南京: 南京航空航天大学, 2016]

5 Ateniese G, Fu K, Green M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans Inf Syst Secur, 2006, 9: 1–30

6 Green M, Ateniese G. Identity-based proxy re-encryption. In: Applied Cryptography and Network Security. Berlin, Heidelberg: Springer, 2007. 288–306

7 Boneh D, Franklin M. Identity-based encryption from the weil pairing. In: Advances in Cryptology—CRYPTO 2001. Berlin, Heidelberg: Springer, 2001. 231–229

8 Chu C, Tzeng W. Identity-based proxy re-encryption without random oracles. In: Information Security. Berlin, Heidelberg: Springer, 2007. 189–202

9 Waters B. Efficient identity-based encryption without random oracles. In: Advances in Cryptology—EUROCRYPT 2005. Berlin, Heidelberg: Springer, 2005. 189–202

10 Weng J, Deng R H, Chu C, et al. Conditional proxy re-encryption secure against chosen-ciphertext attack. In: Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2009. 322–332

11 Weng J, Yang Y J, Tang Q, et al. Efficient conditional proxy re-encryption with chosen-ciphertext security. In: Information Security. Berlin, Heidelberg: Springer, 2009. 151–166

12 Tang Q. Type-based proxy re-encryption and its construction. In: Progress in Cryptology—INDOCRYPT 2008. Berlin, Heidelberg: Springer, 2008. 130–144

13 Chu C K, Weng J, Chow S S M, et al. Conditional proxy broadcast re-encryption. In: Information Security and Privacy. Berlin, Heidelberg: Springer, 2009. 327–342

14 Shao J, Cao Z, Liang X, et al. Proxy re-encryption with keyword search. Inf Sci, 2010, 180: 2576–2587

15 Fang L, Susilo W, Ge C, et al. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. Theor Comput Sci, 2012, 462: 39–58

16 Liang K T, Liu Z, Tan X, et al. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: Information Security and Cryptology—ICISC 2012. Berlin, Heidelberg: Springer, 2012. 189–202

17 Liang X H, Cao Z F, Lin H, et al. Attribute-based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. New York: ACM, 2009. 276–286

18 Liang K T, Fang L M, Wong D S, et al. A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security. In: Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems. Xi'an: IEEE, 2013. 552–559

19 Liang K T, Au M H, Susilo W, et al. An adaptively CCA-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. In: Information Security Practice and Experience. Berlin, Heidelberg: Springer, 2014. 448–461

20 Fang L, Susilo W, Ge C, et al. Interactive conditional proxy re-encryption with fine grain policy. J Syst Softw, 2011, 84: 2293–2302

21 Ge C, Susilo W, Wang J, et al. A key-policy attribute-based proxy re-encryption without random oracles: Table 1. Comput J, 2016, 59: 970–982

22 Tang Y, Jin M, Meng H, et al. Attribute-based verifiable conditional proxy re-encryption scheme. Entropy, 2023, 25: 822

23 Hou J, Peng C, Tan W, et al. Quantum-resistant multi-feature attribute-based proxy re-encryption scheme for cloud services. Comput Model Eng Sci, 2024, 138: 917–938

24 Liu S, Qin H, Taniar D, et al. A certificate-based proxy re-encryption plus scheme for secure medical data sharing. Internet Things, 2023, 23: 100836

25 Zeng Y, Dong Z, Wang H, et al. A general quantum minimum searching algorithm with high success rate and its implementation. Sci China-Phys Mech Astron, 2023, 66: 240315

26 Huang H L, Xu X Y, Guo C, et al. Near-term quantum computing techniques: Variational quantum algorithms, error mitigation, circuit compilation, benchmarking and classical simulation. Sci China-Phys Mech Astron, 2023, 66: 250302, arXiv: 2211.08737

27 Hou X, Zhou G, Li Q, et al. A duplication-free quantum neural network for universal approximation. Sci China-Phys Mech Astron, 2023, 66: 270362, arXiv: 2211.11228

28 Li Z H, Yu G F, Wang Y X, et al. Experimental demonstration of deterministic quantum search algorithms on a programmable silicon photonic chip. Sci China-Phys Mech Astron, 2023, 66: 290311

29 Song Y, Wu Y, Wu S, et al. A quantum federated learning framework for classical clients. Sci China-Phys Mech Astron, 2024, 67: 250311, arXiv: 2312.11672

30 Zheng Q, Yu M, Zhu P, et al. Solving the subset sum problem by the quantum Ising model with variational quantum optimization based on conditional values at risk. Sci China-Phys Mech Astron, 2024, 67: 280311

31 Li L, Li J, Song Y, et al. An efficient quantum proactive incremental learning algorithm. Sci China-Phys Mech Astron, 2025, 68: 210313

32 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302, arXiv: quant-ph/0012056

33 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317, arXiv: quant-ph/0308173

34 Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305

35 Yu K F, Yang C W, Liao C H, et al. Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf Process, 2014, 13: 1457–1465

36 Zou X, Qiu D, Li L, et al. Semiquantum-key distribution using less than four quantum states. Phys Rev A, 2009, 79: 052312

37 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

38 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, arXiv: 2308.14385

39 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834, arXiv: quant-ph/9806063

40 Gottesman D. Theory of quantum secret sharing. Phys Rev A, 2000, 61: 042311, arXiv: quant-ph/9910067

41 Xiao L, Lu Long G, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307, arXiv: quant-ph/0405179

42 Wang J, Zhang S, Zhang Q, et al. Semiquantum secret sharing using two-particle entangled state. Int J Quantum Inform, 2012, 10: 1250050

43 Yang C W, Hwang T. Efficient key construction on semi-quantum secret sharing protocols. Int J Quantum Inform, 2013, 11: 1350052

44 Xie C, Li L, Qiu D. A novel semi-quantum secret sharing scheme of specific bits. Int J Theor Phys, 2015, 54: 3819–3824

45 Gao X, Zhang S, Chang Y. Cryptanalysis and improvement of the semi-quantum secret sharing protocol. Int J Theor Phys, 2017, 56: 2512–2520

46 Mashhadi S. General secret sharing based on quantum Fourier transform. Quantum Inf Process, 2019, 18: 114

47 Liu W, Gao P, Liu Z, et al. A quantum-based database query scheme for privacy preservation in cloud environment. Secur Commun Netws, 2019, 2019: 1–14

48 Liu W, Xu Y, Zhang M, et al. A novel quantum visual secret sharing scheme. IEEE Access, 2019, 7: 114374–114384

49 Cao H, Ma W P. Threshold quantum state sharing scheme based on linear equations and unitary operation. IEEE Photon J, 2017, 9: 1–7

50 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, arXiv: 2303.14622

51 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

52 Chang Y, Zhang S B, Yan L L, et al. A quantum secure sharing protocol for Cloud data based on proxy re-encryption. Sci Rep, 2020, 10: 9074

53 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

54 Yan P S, Zhou L, Zhong W, et al. Advances in quantum entanglement purification. Sci China-Phys Mech Astron, 2023, 66: 250301, arXiv: 2304.12679

Cloud server quantum data secret sharing scheme

CHANG Yan[1,2,3], LIU Honglin[1,2,3], GOU Zhijian[1,2,3*], SONG Ziyang[1,2,3], ZHAO Yinshan[1,2,3], DUAN Guangming[1,2,3] & LI Pengliang[1,2,3]

[1] *School of Cybersecurity, Chengdu University of Information Technology, Chengdu 610225, China*
[2] *Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu University of Information Technology, Chengdu 610225, China*
[3] *SUGON Industrial Control and Security Center, Chengdu 610225, China*
**Corresponding author (email: gzj@cuit.edu.cn)*

Storing data in the form of quantum states on cloud servers can significantly enhance storage efficiency. The storage and sharing of quantum data on cloud servers necessitate consideration of security issues. An ingenious solution is to store data in the form of ciphertext on cloud servers. When data needs to be shared with users, the cloud server performs a second encryption on the data ciphertext and sends the doubly encrypted ciphertext to the users. Users can decrypt and obtain the data itself using their private keys. This process can be regarded as the transformation of the data owner's ciphertext into a shared ciphertext by a third party (the cloud server). This study proposes a new quantum data sharing scheme for cloud servers. One of our main contributions is the realization of sharing specific data with users who have appropriate permissions (satisfying certain attribute-based conditions). The security of the scheme is demonstrated through key analysis, plaintext analysis, first-level ciphertext analysis, and second-level ciphertext analysis.

quantum data sharing, cloud servers, conditional proxy re-encryption, attributes

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

doi: 10.1360/SSPMA-2024-0513