计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190600020

噪声信道下的盲量子计算

罗文俊　雷　爽
重庆邮电大学计算机科学与技术学院　重庆 400065
(luowj@cqupt.edu.cn)

摘　要　盲量子计算(Blind Quantum Computation,BQC)区别于传统的量子计算(Quantum Metrology),它将客户端的计算任务通过量子信道委托给服务器端完成,解放客户端的计算压力,这就要求在信道的传输过程中,量子尽量精确传输。由于量子信道的噪声问题,理想情况下的无噪传输协议是不可能实现的,需要使用量子纠错码(Quantum Error-Correcting Code,QECC)来纠正由噪声信道引起的量子比特翻转和量子相位翻转错误。在盲量子计算协议的基础上,文中针对噪声比特翻转信道和噪声相位翻转信道分别设计抗噪声的盲量子计算协议,客户端通过不同的方式编码量子比特,利用编码后的量子比特传输量子信息给服务器,服务器利用量子纠错码恢复正确的量子信息与客户端完成盲量子计算。协议分析表明,文中提出的两个盲量子计算协议分别在量子比特翻转和量子相位翻转噪声信道中,通过纠错计算达到了盲量子计算协议对于量子尽量精确传输的要求,并且不改变盲量子计算的正确性和盲特性,不会降低量子计算的无条件安全性。最后展望所提协议可以适用于其他量子纠错码。

关键词:盲量子计算;噪声信道;量子比特翻转;量子相位翻转;量子纠错码
中图法分类号　TP301

Blind Quantum Computation over Noise Channels

LUO Wen-jun and LEI Shuang
College of Computer Science and Technology,Chongqing University of Posts and Telecommunications,Chongqing 400065,China

Abstract　Blind Quantum Computation (BQC),is a kind of protocol that remarkably distinguishes from traditional quantum computation,delegates computing tasks from clients to the servers through the quantum channels which eventually alleviates the computing pressure generated by the clients. Consequently,BQC requires that the quantum is teleported in an accurate manner of transmission via the channels. Due to the problem of noise of quantum channel,a purely noiseless transmission channel under ideal circumstance cannot be realized without quantum error correction codes that are implemented to rectify the flip errors in terms of quantum bit and phase resulted from noise channels. By the basis of BQC protocol,two anti-noise BQC protocols are proposed from the perspectives of noise bit flip channels and noise phase flip channels,respectively. Explicitly,the client encodes the qubits via various ways,then the encoded qubits are used to transmit the quantum information to the server by which the quantum error correction codes are exploited to recover the correct quantum information for the purpose of completion of BQC with the client. A protocol analysis indicates that via correction computation,the requirement of accurate transmission by BQC protocol can be met during the computation of BQC over the quantum bit flip and quantum phase flip noise channels with neither the sacrifice of correctness and blindness of BQC,nor the reduction in unconditional security of quantum computing. Finally,this paper hopes that the new BQC protocols can be applied to other quantum error correction codes as well.

Keywords　Blind quantum computation,Noise channel,Quantum bit flip,Quantum phase flip,Quantum error correcting code

1　引言

量子纠错(Quantum Error Correction,QEC)[1-3]技术是量子计算[4]过程中应对量子噪声的一种必要的方法。与经典计算不同,量子计算的优越性主要体现在量子并行计算上,量子计算利用量子态的相干叠加特性完成高效的复杂运算,可以实现短时间内对现有密码体制的暴力破解。但是量子计算对计算环境的要求极高,由于实际的量子环境中量子态很容易被环境破坏,一旦量子态被破坏,那么量子就会向被破坏的态上偏转,并且这个过程是不可逆的。所以,在有噪信道或者第三方攻击的情况下,量子计算会失去其计算优势。因此,量子纠错在整个量子计算中起到重要的作用。为实现量子纠错,量子纠错编码应运而生。文献[5]对二元非线性等重码的经典纠错码的性能进行研究,证明了 $n\neq 2\omega$ 时 Fu 等提出的改进的王氏猜想成立[6]。本文对量子纠错码进行探究,量子纠错码是在复 Hilbert 空间实现的,相对于经典纠错码,其在对错误信息检错和纠错时存在 3 种难题:1)量子态不可克隆;2)错误是连续的;3)量子信息不可测量。因此为解决上述问题,shor 量子纠错码[7]将单比特量子态编码成一个纠缠态,量子相干性不受影响,错误也能被正常测出。

到稿日期:2019-06-05　返修日期:2019-08-21　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
通信作者:雷爽(ls889933@163.com)

现在的量子纠错码分为两类。一类是对称量子码，上文阐述的经典 shor 量子纠错码就属于这一类。与此同时，CSS 构造码的构造方法解决了构造量子码的难题[8-9]。而后，研究者们提出利用几何特性构造量子纠错码，具有几何特性的量子纠错码的代表为 Quantum Low Density Parity Check(LDPC)码[10-12]，它降低了计算复杂度。另一类量子纠错码是非对称量子码。最初，Steane 讨论了在非对称信道构造量子纠错码的方法[13]，随着研究的深入，越来越多的研究者开始研究非对称量子码。2007 年，Ioffe 等利用量子 CSS 构造原理得到了非对称量子 BCH-LDPC 码[14]。2010 年，Aly 等[15]提出运用经典循环码生成的多项式获得自对偶纠错码，再利用非对称构造定理得到一系列非对称量子纠错码。同年，Wang 等[16]针对非加性对称量子码的特性，扩展得到不对称的非加性量子码。对于某些高效的现代码，找到它的对偶码比较困难。基于这个问题，研究者们提出了算子量子纠错码和基于纠缠辅助的量子纠错码[17-19]。Hsieh 等[20]利用经典的欧式几何与射影几何 LDPC 码来构造低纠缠度的高性能纠缠辅助量子 LDPC 码，仿真结果证实了具有低纠缠消耗率的高性能纠缠辅助量子 LDPC 码优于标准量子 LDPC 码。

本文将纠错码运用到盲量子计算[21-24]中。在盲量子计算过程中，由于 Alice 要通过量子信道向 Bob 发送量子比特，理想状态下的量子无噪信道无法实现，会出现量子比特翻转或者量子相位翻转错误，因此使用量子纠错码，选择辅助量子比特作为纠错码。辅助量子纠错码理论[18,25-27]已经证明，基于辅助构造的量子纠错码可以对抗量子信道引起的噪声问题，只要其满足构造条件就不会出错，能更快地传输信息。

本文首先介绍量子纠错码的研究现状，将其应用于盲量子计算中；接着将量子纠错码重新编码，使其适用于有噪声信道的盲量子计算；然后提出拟定的基于量子纠错码的盲量子计算协议；最后对协议进行分析和展望。

2 理论基础

量子发生的错误分为 3 种，对应 Pauli 矩阵 ***XYZ*** 的线性组合，所以只需纠正这 3 个错误就可以解决所有的量子错误。

2.1 量子纠错码

QEC 基于 3 个核心思想：噪声的数字化、错误操作符的操作和量子纠错码(QECC)的构造。QEC 的成功程度依赖于噪声的物理学。本文在讨论了 3 个核心思想后，根据辅助量子纠错的原理，对噪声信道下的量子比特进行编码并设计新的盲量子计算协议。

2.1.1 噪音数字化

“噪音数字化”指一组量子比特与另一个系统(如环境)之间的相互作用形式，用 $|\varphi\rangle|\varphi_0\rangle_e \rightarrow \sum_i (E_i|\phi\rangle)|\varphi_i\rangle_e$ 表示。其中，每个错误运算符 E_i 是 Pauli 算子作用于量子位的张量积，$|\phi\rangle$ 是初始值量子比特的状态和，$|\varphi_i\rangle_e$ 是环境状态，$|\varphi_i\rangle_e$ 不一定正交或标准化。因此，本文用 Pauli 算子 $\sigma_x,\sigma_y,\sigma_z$ 表示一般噪声或退相干量子比特，表示为 $X\equiv\sigma_x, Z\equiv\sigma_z, Y\equiv -i\sigma_y = XZ$。

2.1.2 错误算子的提取

考虑由 $\{I,X,Y,Z\}$ 组成的集合以及 3 个 Pauli 运算符。Pauli 操作全部表示为与 I 有关的操作：$X^2=Y^2=Z^2=I$，且特征值为 ± 1。集合中的两个操作必须对易($XI=IX$)或反对易 $XZ=-ZX$。Pauli 算子的张量积，即错误算子也需要对易或反对易。如果量子系统中有 n 个量子位，则错误算子的长度也为 n。

2.1.3 量子纠错码的构造条件

令 C 为一个量子码，P 为 C 的投影算子，具有运算元 $\{E_i\}$ 的量子运算用 ε 来表示。则量子码 C 上的纠错运算 ε 存在的充分必要条件为：对某个负数 Hermite 矩阵 $\boldsymbol{\alpha}$ 成立：

$$PE_i^* E_j P = \alpha_{ij} P \tag{1}$$

2.2 盲量子计算

在通用盲量子计算[23]中，(i,j)为量子位索引，其中 i 为列，j 为行，图态 $|G(\theta)\rangle$ 的产生规则如下：

若行 $i \bmod 2=1$，列 $j\equiv 3 \bmod 8$，则对满足条件的(i,j)，$(i+1,j)$，$(i,j+2)$和$(i+1,j+2)$，执行 Controlled-Z 操作。

若行 $i \bmod 2=0$，列 $j\equiv 7 \bmod 8$，则对满足条件的(i,j)，$(i+1,j)$，$(i,j+2)$和$(i+1,j+2)$，执行 Controlled-Z 操作；对于每一行所有(i,j)和$(i+1,j)$，执行 Controlled-Z 操作。

一个 Brickwork 中一个任意角测量的结构如图 1 所示。

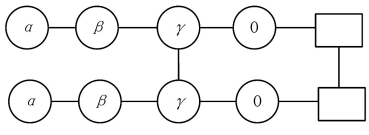

图 1 任意角测量结构图

Fig. 1 Structure of arbitrary angle measuring

假设客户想要完成量子计算，且他已经考虑到对应于图 G 的 n 量子位图态的量子计算，想要执行的量子操作是在基 $|\pm\delta_i\rangle$ 下测量第 i 个量子位，则盲量子计算协议步骤如下：

S1：客户准备 n 个量子比特并发送给服务器。每个量子位的状态是 $|\theta_i\rangle=|0\rangle+e^{i\theta_i}|1\rangle(i=1,2,\cdots,n)$，其中 θ_i 从集合 $S(S=\{0,\frac{\pi}{4},\cdots,\frac{7\pi}{4}\})$中一致地选择。

S2：服务器产生图态 $|G(\theta)\rangle$。

S3：对于 $i=1,2,\cdots,n$，客户随机选择 $r_i\in\{0,1\}$，计算 $\delta_i=(\theta_i+\phi_i'+r_i\pi) \bmod 2\pi$，其中 ϕ_i' 根据前面的测量得到。如果客户端需要服务器测量 $|G(\theta)\rangle$ 的第 i 个量化位，则将 δ_i 发送到服务器。

S4：服务器在 $|\pm\delta_i\rangle$ 基础上对第 $i(i=1,2,\cdots,n)$个量子位进行测量，并通知客户有关测量结果。

3 噪声信道下的盲量子计算协议

在盲量子计算中，由于量子信息传输的过程不可避免地会受到外部环境的影响(外部环境极有可能是噪声状态)，那么在噪声信道下，Bob 收到的量子会被移位或者翻转。在这个情况下，一般有两种应对方式，一种是量子容错，另一种是量子纠错。容错的盲量子计算虽然效率高，但是牺牲了结果的正确性，所以本文利用量子纠错，即加入量子纠错码，使得 Bob 在进行盲量子计算之前，先用纠错码对收到的量子比特进行纠错，再完成计算，以提高结果的正确性。因此，本文利用辅助码对盲量子计算协议进行重新设计，Alice 通过编码量子比特利用编码后的量子比特传输量子信息，在信息比特通过有噪量子信道后，Bob 根据解码的量子比特恢复出正确的量子消息，满足量子纠错条件。

3.1 噪声信道下单量子比特翻转错误纠正

本文协议首先设定盲量子计算中的噪声信道只对单量子比特进行翻转。

本文设计的基于单量子比特翻转错误纠正的盲量子计算协议如下。

S1：Alice 制备 n 个单量子比特，每个量子位的状态是 $|\varphi\rangle=|0\rangle+e^{i\theta_i}|1\rangle(i=1,2,\cdots,n)$，其中 θ_i 从集合 S 中随机选择。在这个情况下，只有 Alice 知道 θ_i 的值。

S2：Alice 编码单量子比特。

$$C(|\varphi\rangle|00\rangle)=|\varphi_E\rangle=|000\rangle+e^{i\theta_i}|111\rangle \tag{2}$$

编码线路如图 2 所示。

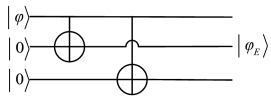

图 2 Alice 编码线路图

Fig. 2 Coded circuit of Alice

S3：Alice 通过量子噪声信道发送 $|\varphi_E\rangle$ 给 Bob。

在量子噪声信道中，由于发生了一位量子比特翻转，此时错误算子的集合为：

$$\varepsilon=\{I_1I_2I_3, X_1I_2I_3, I_1X_2I_3, I_1I_2X_3\}$$

那么，当 p_1, p_2, p_3 分别为错误发生的概率时，E_1, E_2, E_3 分别为其操作元。

$$\begin{cases} E_1=\sqrt{p_1}X_1I_2I_3 \\ E_2=\sqrt{p_2}I_1X_2I_3 \\ E_3=\sqrt{p_3}I_1I_2X_3 \end{cases} \tag{3}$$

此时，Alice 发送的 $|\varphi_E\rangle$ 通过量子噪声信道变为 $|\varphi_E\rangle'$，即：

$$|\varphi_E\rangle\rightarrow|\varphi_E\rangle'=\sum_a E_a|\varphi_E\rangle \tag{4}$$

$$\sum_a E_a|\varphi_E\rangle=(\sqrt{p_1}X_1I_2I_3+\sqrt{p_2}I_1X_2I_3+\sqrt{p_3}I_1I_2X_3)(|000\rangle+e^{i\theta_i}|111\rangle)$$

S4：Bob 收到 Alice 的编码比特 $|\varphi_E\rangle'$ 后，利用 $|00\rangle$ 辅助态纠缠量子编码比特。Bob 利用伴随算子 A：$|a_1a_2a_300\rangle\rightarrow|a_1a_2a_3, a_2\oplus a_3, a_1\oplus a_3|$ 计算 $A(\sum_a E_a|\varphi_E\rangle|00\rangle)$。具体过程如图 3 所示。

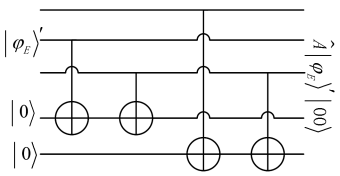

图 3 Bob 编码路线图

Fig. 3 Coded circuit of Bob

S5：Bob 对辅助比特进行测量操作，根据测量结果执行对应门操作从而进行量子纠错，如表 1 所列。测量结果集合为 $\{01,10,11,00\}$。

表 1 量子纠错操作

Table 1 Quantum error correction

测量结果	量子塌缩态	门操作
$\langle 00\rangle$	$\|000\rangle+e^{i\theta_i}\|111\rangle$	$I_1I_2I_3$
$\langle 01\rangle$	$\|100\rangle+e^{i\theta_i}\|011\rangle$	$X_1I_2I_3$
$\langle 10\rangle$	$\|010\rangle+e^{i\theta_i}\|101\rangle$	$I_1X_2I_3$
$\langle 11\rangle$	$\|001\rangle+e^{i\theta_i}\langle 110\rangle$	$I_1I_2X_3$

此时，纠错后的量子比特为 $|\varphi_E\rangle$。

S6：Bob 利用投影算子 $|0\rangle+|1\rangle$，使纠错后的量子比特 $|\varphi_E\rangle$ 塌缩到 $|0\rangle+e^{i\theta_i}|1\rangle$，即 $|\varphi\rangle$ 态。

S7：Bob 利用 $|\varphi\rangle$ 态量子比特排列图 G，从通用盲量子计算步骤 S3 开始，与 Alice 进行经典盲量子比特计算。

量子码的译码即纠正量子在信道中发生移位、翻转等错误。在本文协议中，纠错的过程如下：

Alice 将 k-qubit 量子态 $|\varphi\rangle_k$ 编码为 n-qubit 序列 $S=|\varphi_1\varphi_2\cdots\varphi_n\rangle$，编码操作如下：

$$|\varphi_n\rangle=U_E|\phi\rangle_c^A|\varphi_k\rangle|0\rangle_{n-c-k} \tag{5}$$

Bob 对经由量子噪声信道输出的 Alice 发送信息的量子态序列 $|\varphi_n'\rangle$ 进行错误伴随式测量，接着进行迭代译码，对错误的恢复操作为：

$$\begin{aligned} |\varphi_k'\rangle&=D_{\hat{E}}^{\wedge}|\varphi_n'\rangle|\phi\rangle_c^B \\ &=D_{\hat{E}}^{\wedge}E|\varphi_n\rangle|\phi\rangle_c^B \\ &=D_{\hat{E}}^{\wedge}EU_E|\phi\rangle_c^A|\varphi_k\rangle|0\rangle_{n-c-k}|\phi\rangle_c^B \\ &=D_{\hat{E}}^{\wedge}EU_E|\varphi_k\rangle \end{aligned} \tag{6}$$

根据错误伴随式 S 对辅助量子纠错码进行译码，得到最可能的信道错误算子 $\hat{E}$，当 $\hat{E}=E$ 时，可通过算符 $D_{\hat{E}}^{\wedge}$ 的操作恢复出正确的量子态序列。

3.2 噪声信道下单量子比特相位翻转错误纠正

在噪声信道中有可能发生相位翻转错误，相位翻转噪声下，Alice 发送的量子比特可能变为：

$$|\varphi_E\rangle=|000\rangle+e^{i\theta_i}|111\rangle\rightarrow|\varphi_E\rangle'=|000\rangle-e^{i\theta_i}|111\rangle \tag{7}$$

这时，Alice 用比特翻转编码协议无法满足对错误的修正了。因此，本文对量子相位翻转的盲量子协议设计如下：

S1：同基于单量子比特翻转错误纠正的盲量子计算协议的 S1。

S2：Alice 利用哈达玛门（Hadamard）编码单量子比特。

$$C(|\varphi\rangle|00\rangle)=|\varphi_E\rangle=|+++\rangle+e^{i\theta_i}|---\rangle \tag{8}$$

编码线路如图 4 所示。

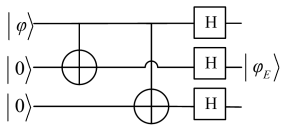

图 4 Alice 编码线路图

Fig. 4 Alice coded circuit

S3：Alice 通过量子噪声信道发送 $|\varphi_E\rangle$ 给 Bob。

在量子噪声信道中，由于发生了一位量子相位翻转，但这时量子比特已经被编码成 $|\varphi_E\rangle$，因此相位翻转错误作用在 $|\varphi_E\rangle$ 上的错误算子集合等效为：

$$\varepsilon=\{I_1I_2I_3, X_1I_2I_3, I_1X_2I_3, I_1I_2X_3\}$$

Bob 收到的 $|\varphi_E\rangle'$ 有如下 4 种情况：

$$\begin{aligned} |\varphi_E\rangle_0'&=|+++)+e^{i\theta_i}|---) \\ |\varphi_E)_1'&=|-++)+e^{i\theta_i}|+--) \\ |\varphi_E)_2'&=|+-+)+e^{i\theta_i}|-+-) \\ |\varphi_E\rangle_3'&=|++-)+e^{i\theta_i}|--+) \end{aligned} \tag{9}$$

可以看出，协议通过哈达玛门转化，已经将相位翻转变为比特翻转，即：

$$|\varphi_E\rangle\rightarrow|\varphi_E\rangle'=\sum_a E_a|\varphi_E\rangle \tag{10}$$

S4:Bob 收到 Alice 的编码比特$|\varphi_E\rangle'$后,利用$|++\rangle$辅助态纠缠量子编码比特,如图 5 所示。

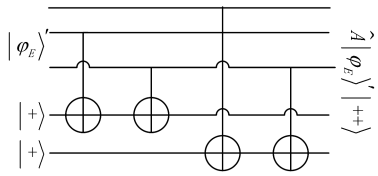

图 5 Bob 编码线路图

Fig. 5 Bob coded circuit

Bob 利用伴随算子$A:|a_1a_2a_3++\rangle\rightarrow|a_1a_2a_3,a_2\oplus a_3,a_1\oplus a_3\rangle$计算$A(\sum_a E_a|\varphi_E\rangle|++\rangle)$。

S5:Bob 对辅助比特进行测量操作,根据测量结果执行对应门操作从而进行量子纠错,如表 2 所列。测量结果集合为$\{++,+-,-+,--\}$。

表 2 量子纠错操作

Table 2 Quantum error correction

测量结果	量子塌缩态	门操作
$\|++\rangle$	$\|+++\rangle+e^{i\theta_i}\|---\rangle$	$I_1I_2I_3$
$\|+-\rangle$	$\|-++\rangle+e^{i\theta_i}\|+--\rangle$	$X_1I_2I_3$
$\|-+\rangle$	$\|+-+\rangle+e^{i\theta_i}\|-+-\rangle$	$I_1X_2I_3$
$\|--\rangle$	$\|++-\rangle+e^{i\theta_i}\|--+\rangle$	$I_1I_2X_3$

S6:Bob 利用哈达玛门对纠错后的量子$|\varphi_E\rangle$还原量子态。因为哈达玛门的平方等于 1,再次利用哈达门编码量子比特可以不改变量子态,如图 6 所示。

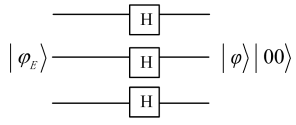

图 6 Bob 编码线路图

Fig. 6 Bob coded circuit

S7,S8:与基于单量子比特翻转错误纠正的盲量子计算协议步骤 S6,S7 相同。

4 协议分析

4.1 可行性证明

4.1.1 单量子比特翻转错误纠正的盲量子计算协议

本节对基于单量子比特翻转错误纠正的盲量子计算协议的纠错能力进行可行性证明和盲特性证明。

由于 Alice 控制θ_i的值,控制了计算的盲特性,Bob 不知道θ_i,不能得到最终的计算结果。下面从协议整体流程分析θ_i所在位置的变化情况以及其拥有者,如表 3 所列。

表 3 量子态变化情况

Table 3 Quantum state transformation

步骤	量子态	量子态拥有者	θ_i 控制者
1	$\|\varphi\rangle$	Alice	Alice
2	$\|\varphi_E\rangle$	Alice	Alice
3	$\|\varphi_E\rangle'$	Bob	Alice
4	$\|\varphi_E\rangle'\|00\rangle$	Bob	Alice
5	$\|\varphi_E\rangle$	Bob	Alice
6	$\|\varphi\rangle$	Bob	Alice

由表 3 可以看出,在整个协议中,θ_i值由 Alice 保存,Alice 通过控制θ_i达到控制计算的目的,保证了协议的可行性和盲特性。

4.1.2 单量子比特相位翻转错误纠正的盲量子计算协议

本节对基于单量子比特相位翻转错误纠正的盲量子计算协议的纠错能力进行可行性证明和盲特性证明。

Alice 在这个协议中依然通过控制θ_i的值来控制计算流程。由于经过的噪声信道不同,与比特翻转协议不同的是,纠正相位翻转运用了哈达玛门,使其可以等同于比特翻转,等效证明过程如下:

$$\begin{aligned}|000\rangle&\xrightarrow{H}\frac{1}{2\sqrt{2}}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\\&=|+++\rangle\\&=\frac{1}{2\sqrt{2}}(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+\\&\quad|101\rangle+|110\rangle+|111\rangle)\end{aligned}\tag{11}$$

$$\begin{aligned}|111\rangle&\xrightarrow{H}\frac{1}{2\sqrt{2}}(|0\rangle-|1\rangle)\otimes(|0\rangle-|1\rangle)\otimes(|0\rangle-|1\rangle)\\&=|---\rangle\\&=\frac{1}{2\sqrt{2}}(|000\rangle-|001\rangle-|010\rangle+|011\rangle-|100\rangle+\\&\quad|101\rangle+|110\rangle-|111\rangle)\end{aligned}\tag{12}$$

即:

$$\begin{aligned}|000\rangle+|111\rangle&\xrightarrow{H}\frac{1}{2\sqrt{2}}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes(|0\rangle+\\&\quad|1\rangle)+\frac{1}{2\sqrt{2}}(|0\rangle-|1\rangle)\otimes(|0\rangle-|1\rangle)\otimes(|0\rangle-|1\rangle)\\&=|+++\rangle+|---\rangle\end{aligned}\tag{13}$$

这个过程不改变其协议的可行性和盲特性。

4.2 安全性分析

窃听者 Eve 的目的是获得发送者 Alice 发送的信息,需要通过窃听或者纠缠的方法推测出 Alice 的角度值θ_i。

Eve 通过窃听得到 Alice 传送的某一个粒子,对其进行测量来推测θ_i的值。Eve 利用截取/重发攻击方案,当 Alice 发送量子比特$|\varphi_E\rangle=|000\rangle+e^{i\theta_i}|111\rangle$给 Bob 时,Eve 在量子噪声信道截获量子,随机产生基序列对截获的量子进行测量,希望以此获得比特序列。然后,Eve 随机选取基,发送制备的量子。Bob 将收到 Eve 发送的量子得到错误的运算结果。本文对 Eve 进行分析,当 Eve 窃听到$|0\rangle+e^{i\theta_i}|1\rangle$时,由于$\theta_i$是 Alice 的随机值,Eve 得到$|0\rangle+e^{i\theta_i}|1\rangle$也推测不出$\theta_i$;当 Eve 窃听到$|0\rangle$量子时,不会得到任何收获。接下来对 Bob 得到的结果进行分析。当 Bob 得到的值是$|\varphi_E\rangle$经过噪声信道传过来的$|\varphi_E\rangle'$时,Bob 能成功恢复出 Alice 的量子比特$|\varphi\rangle$,然后对量子比特进行纠缠图态操作。Alice 通过选取和 Bob 相同的基作为测试位,得到正确的计算结果。当 Bob 得到的值是 Eve 重发过来的量子比特时,Alice 计算的误码率必然大于 0,可以确定 Eve 窃听。因此,本文协议可以抵抗 Eve 截取/重发攻击。

纠错码的作用是判定 Bob 收到的量子态是否受到噪声环境的影响,发生 XYZ 错误。如果错误发生,则按照译码操作恢复量子信息。纠错码参数的选择关系到编码粒子传回给

Bob过程中的安全性，即第二次窃听检测问题。在无噪声的理想信道条件下，检测码单纯用以判定Bob是否正确接收Alice发送的信息。

基于单量子比特相位翻转错误纠正的盲量子计算协议的安全性与基于单量子比特翻转错误纠正的盲量子计算协议相同。

结束语 本文提出了在噪声信道下，基于辅助比特纠错的盲量子计算协议，利用量子纠错码纠正信道引起的比特翻转、相位移位等错误，论证了协议计算过程中的正确性，并对协议的可行性和安全性进行分析。分析表明，该协议可以抵御第三方量子攻击，是盲量子计算协议的一个扩展，使其盲量子计算可以适用于噪声信道环境；协议中的纠错步骤可以替换为最新的纠错算法，具有适应延展性，对量子计算机的发展提供了一种新的可能性。

参 考 文 献

[1] GOTTESMAN D. Class of quantum error-correcting codes saturating the quantum Hamming bound [J]. Physical Review A, 1996,54(3):1862-1868.

[2] CHIAVERINI J, LEIBFRIED D, SCHAETZ T, et al. Realization of quantum error correction [J]. Nature, 2004, 432(7017): 602-605.

[3] CÁRCOLES AD, MAGESAN E, SRINIVASAN S J, et al. Demonstration of a quantum error detection code using a square lattice of four superconducting qubits [J]. Nature Communications, 2015, 6: 6979.

[4] TÓTH G, APELLANIZI. Quantum metrology from a quantum information science perspective [J]. Journal of Physics A Mathematical & Theoretical, 2014, 47(42): 15-22.

[5] LUO W J. Error Correction Performance of Binary Nonlinear Equal Weight Codes [J]. Chinese Science Bulletin, 2000, 45(13): 1441-1446.

[6] FU F W, XIA S T. Error detection performance of binary nonlinear equal weight codes [J]. Science Bulletin, 1997, 42(4): 343-347.

[7] SHOR P W. Scheme for reducing decoherence in quantum computer memory [J]. Physical Review A, 1995, 52(4): R2493-R2496.

[8] CALDERBANK A R, SHORPW. Good quantum error-correcting codes exist [J]. Physical Review A, 1996, 54(2): 1098-1105.

[9] ZHAO S M. Construction of a quantum CSS code based on sparse sequence [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2011, 31(2): 1-5.

[10] FUJIWARA Y, CLARK D, VANDENDRIESSCHE P, et al. Entanglement-assisted quantum low-density parity-check codes [J]. Physical Review A, 2010, 82(4): 272-277.

[11] DJORDJEVIC, IVAN B. Quantum LDPC Codes from Balanced Incomplete Block Designs [J]. IEEE Communications Letters, 2008, 12(5): 389-391.

[12] WANG X Y, ZHANG Y C, YU S, et al. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code[J]. Scientific reports, 2018, 8(1): 1-7.

[13] STEANE, ANDREW M. Error Correcting Codes in Quantum Theory [J]. Physical Review Letters, 1996, 77(5): 793-797.

[14] IOFFE L, MEZARD M. Asymmetric quantum error correcting codes [J]. Phys. Rev. A, 2007, 75(3): 723-727.

[15] ALY S A, ASHIKHMIN A. Nonbinary quantum cyclic and subsystem codes over asymmetrically-decohered quantum channels [C]// 2010 IEEE Information Theory Workshop on Information Theory. Cairo: IEEE, 2010: 1-5.

[16] WANG L, FENG K, LING S, et al. Asymmetric Quantum Codes: Characterization and Constructions [J]. IEEE Transactions on Information Theory, 2010, 56(6): 2938-2945.

[17] DAVID K, LAFLAMME R. Unified and generalized approach to quantum error correction [J]. Physical Review Letters, 2005, 94(18): 180501. 1-180501. 4.

[18] BRUN T, IGOR D, AND MIN-HSIU H. Correcting quantum errors with entanglement [J]. Science, 2006, 314(5798): 436-439.

[19] LUO L, ZHI M A, WEI Z, et al. Non-binary entanglement-assisted quantum stabilizer codes[J]. Science China (Information Sciences), 2017, 60(4): 210-223.

[20] HSIEH M H, YEN W T, HSU L Y. High Performance Entanglement-Assisted Quantum LDPC Codes Need Little Entanglement [J]. IEEE Transactions on Information Theory, 2011, 57(3): 1761-1769.

[21] NAYAK C, SIMON S H, STERN A, et al. Non-Abelian Anyons and Topological Quantum Computation [J]. Review of Modern Physics, 2008, 80(3): 1083-1159.

[22] KASHEFI E, WALLDEN P. Garbled Quantum Computation [J]. Cryptography, 2017, 1(1): 6-36.

[23] LOSS D, DIVINCENZO D P. Quantum Computation with Quantum Dots [J]. Phys. Rev. A, 1997, 57(1): 120-126.

[24] BRIEGEL H J, BROWNE D E, DüR W, et al. Measurement-based quantum computation[J]. Nature Physics, 2009, 5: 19-26.

[25] LAI C Y, BRUN T. Entanglement Increases the Error-Correcting Ability of Quantum Error-Correcting Codes [J]. Physical Review A, 2010, 88(1): 2343-2347.

[26] BRUN T A, DEVETAK I, HSIEH M H. Catalytic Quantum Error Correction [J]. IEEE Transactions on Information Theory, 2006, 60(6): 3073-3089.

[27] TANG J, LIU J W, CAO Y Q. Cognitive spectrum allocation on demand based on quantum coding and mimic physical optimization[J]. Computer Engineering, 2015, 41(12): 135-139.

LUO Wen-jun, born in 1966, professor, Ph.D, is a member of China Computer Federation. His main research interests include cyberspace security and cryptography.

LEI Shuang, born in 1995, postgraduate. Her main research interests include cryptography, quantum computing and quantum security.