

基于自对偶量子低密度校验码的量子对话协议

刘芬¹, 贺振兴², 徐鹏翱¹, 马鸿洋²

(1. 青岛理工大学信息与控制工程学院, 山东 青岛 266033;

2. 青岛理工大学理学院, 山东 青岛 266033)

摘要: 在量子信道中, 粒子在传输过程中通常会受到噪声的影响, 提出基于自对偶量子低密度校验码的量子对话协议来抵抗噪声攻击, 使用B构造法和U构造法相结合的方法来构造自对偶量子低密度奇偶校验矩阵。所提量子对话协议能够抵抗常见的外部攻击, 且不存在信息泄露, 提高了编码和译码的效率。从纠错的角度研究所提量子对话协议的安全性, 安全分析表明, 该协议具有足够的安全性, 能够有效抵御常见的恶意攻击。

关键词: 量子低密度码; 量子对话; 自对偶

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020051

Quantum dialogue protocol based on self-dual quantum low density parity check codes

LIU Fen¹, HE Zhenxing², XU Pengao¹, MA Hongyang²

1. School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266033, China

2. School of Sciences, Qingdao University of Technology, Qingdao 266033, China

Abstract: In quantum channels, particles are usually affected by noise during transmission. A quantum dialogue protocol based on self-dual quantum low density parity check codes was proposed to resist noise attacks. A combination of B construction method and U construction method was used to construct a self-dual quantum low density parity check matrix. The proposed quantum dialogue protocol can resist common external attacks, and there was no information leakage, which improved the efficiency of encoding and decoding. The security of quantum dialogue protocol was studied from the perspective of error correction. Security analysis shows that the protocol has sufficient security and can effectively resist common malicious attacks.

Key words: quantum low-density parity code, quantum dialogue, self-dual

收稿日期: 2019-09-18; 修回日期: 2019-10-15

通信作者: 马鸿洋, hongyang_ma@aliyun.com

基金项目: 国家自然科学基金(61772295, 11975132); 山东省高等学校科技计划项目(J18KZ012); 山东省自然科学基金(ZR2019YQ01)

Foundation Items: The National Natural Science Foundation of China(61772295, 11975132), The University Scientific Research Project of Shandong Province, China (J18KZ012), The Natural Science Foundation of Shandong Province, China (ZR2019YQ01)

论文引用格式: 刘芬, 贺振兴, 徐鹏翱, 等. 基于自对偶量子低密度校验码的量子对话协议[J]. 网络与信息安全学报, 2020, 6(4): 148-152.

LIU F, HE Z X, XU P A, et al. Quantum dialogue protocol based on self-dual quantum low density parity check codes[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 148-152.

1 引言

量子密钥分发 (QKD, quantum key distribution) 利用量子物理定律保证了信息传输的安全性, 在理论上已被证明是无条件安全的。QKD 允许两个远程用户通过量子信道和公共经典信道生成共享密钥。第一种无条件安全 QKD 协议由 Bennett 和 Brassard^[1]于 1984 年提出 (简称 BB84 协议)。随后, 两种量子直接通信协议被提出, 即确定性安全量子通信 (DSQC, deterministic secure quantum communication) 协议^[2-4]和量子安全直接通信 (QSDC, quantum secure direct communication) 协议^[5-10]。这两种量子通信协议可以在不创建共享密钥的情况下实现信息的直接传输, 提高了系统的实时性。对于 DSQC 协议, 信息可以直接从发送方传输到接收方, 而不需要预先生成共享密钥, 接收方只能在传输额外的经典信息后提取信息。然而, QSDC 协议可以实现信息的直接传输, 而不需要交换经典信息。近年来, QSDC 在理论研究和实验实施方面取得了巨大进展。然而, DSQC 和 QSDC 协议只是单向通信协议, 两个用户无法实现信息的相互传输。换句话说, 在这两种协议中, 信息只朝一个方向流动。在实际的传输环境中, 两个用户常常需要同时向对方传输信息, 如电话通信。因此, 有必要研究同时进行的双向量子通信。

量子对话 (QD) 是一种双向量子通信。QD 协议允许两个用户同时向对方传输信息。2004 年, Nguyen^[11]首先提出了量子对话协议, 这是量子通信领域发展的一个里程碑。随后, Gao 等^[12]指出 Nguyen 的对话协议存在信息泄露的问题。针对信息泄露问题, 许多 QD 协议^[13-17]被提出。

大多数 QD 协议是在理想的环境下提出的, 即假设量子信道中没有噪声。在传输过程中, 光子的偏振受到通道噪声的影响。由于量子信道中的噪声是不可避免的, 因此如何使量子密码协议在噪声信道下正常工作显得尤为重要。近年来, 针对所有问题, 许多量子对话协议^[18-23]陆续被提出。本文采用量子纠错码提出了基于自对偶量子低密度奇偶校验纠错的量子对话协议。本协议可以提供更高的通

信保真度, 在一定程度上提高了信息传输的安全性。安全分析表明, 所提方法是可行的, 并且可以抵抗常见的外部攻击而不存在信息泄露。

2 本文协议

本文所提协议依赖于自对偶量子低密度校验码, 量子信息的传输过程依赖于量子信道, 而误码率的计算依赖于经典信道。

2.1 构建自对偶量子低密度奇偶校验码

1) 通话方 Bob 随机生成循环稀疏序列 L 。 L 满足: 序列长为 M 、只包含 (0,1) 且行重为 k , 序列中每两个 1 所在的位置做模 M 减操作, 其结果属于 $(0, M-1)$, 除零之外, 每个数字至多出现一次。由循环得到一个 $M \times M$ 的循环矩阵 R_0 , R_0 每一行的行重均为 k , 循环稀疏序列 L 的不同行重下对应 H_0 的 $2N$ 、 $2K$ 取值如表 1 所示。综上, 可推出 R_0 中任意两行有且只有一列同时为 1。

表 1 循环稀疏序列 L 的不同行重下
对应 H_0 的 $2N$ 、 $2k$ 取值

Table 1 Values of $2N$ and $2k$ corresponding to H_0 under different row weights of the cyclic sparse sequence L

L 的行重 k	L 的长度 N	H_0 的行重 $2k$	H_0 的行长 $2N$
3	7	6	14
4	13	8	26
5	21	10	42
6	31	12	62
7	43	14	86
8	57	16	114
9	73	18	146
10	91	20	182

2) 将 R_0 转置得到 R_0^T , 将这两个矩阵按照式 $H_0 = (R_0, R_0^T)$ 合并, 则得到一个 $M \times 2M$ 矩阵, 其行重为 $2k$, 在 R_0 中出现的每一对 1 将在 R_0^T 出现。删除 H_0 中的一些行, 使 H_0 可作用于编码长度, 最终得到一个 $M_0 \times 2M$ 的矩阵 H , 即为构建自对偶 $(j, 2k)(2M, M_0)$ 量子低密度奇偶校验矩阵, 每一列列重为 j (即一列有 j 个 1)。 M 与 k 满足

$$M = k(k-1) + 1 \quad (1)$$

3) 通话方 Alice 随机生成循环稀疏序列 T 。

T 满足：序列长为 N 、只包含 $(0,1)$ 且行重为 k ，序列中每两个 1 所在的位置做模 N 减操作，其结果属于 $(0, N-1)$ ，除零之外，每个数字至多出现一次。由 T 循环得到一个 $N \times N$ 的循环矩阵 $\mathbf{S}$ ， $\mathbf{S}$ 每一行的行重均为 k 。综上，可推出 $\mathbf{S}$ 中任意两行有且只有一列同时为 1。

4) 将 $\mathbf{S}$ 转置得到 $\mathbf{S}^T$ ，将这两个矩阵按照式 $\mathbf{F} = (\mathbf{S}, \mathbf{S}^T)$ 合并，得到一个行重为 $2k$ 的 $N \times 2N$ 的矩阵。由不同的量子对话，规定循环系数序列的行重，删除其中的一些行，使 $\mathbf{F}$ 可作用于编码长度，最终得到一个 $M_0 \times 2N$ 的矩阵 $\mathbf{C}$ ，即构建自对偶 $(j, 2k)(2N, M_0)$ 量子低密度奇偶校验矩阵，每一列列重为 j （即一列有 j 个 1）。 N 与 k 满足

$$N = k(k-1) + 1 \quad (2)$$

校验矩阵每一行可以生成两个生成元。若校验矩阵的第一行为 (11010001000101) ，则可生成对应生成元。

$$M_1 = \mathbf{X}\mathbf{X}\mathbf{I}\mathbf{X}\mathbf{I}\mathbf{I}\mathbf{X}\mathbf{I}\mathbf{I}\mathbf{X}\mathbf{I}\mathbf{X}$$

$$M_2 = \mathbf{Z}\mathbf{Z}\mathbf{I}\mathbf{Z}\mathbf{I}\mathbf{I}\mathbf{Z}\mathbf{I}\mathbf{Z}$$

其中， $\mathbf{X}$ 、 $\mathbf{Z}$ 、 $\mathbf{I}$ 为 Pauli 算子，分别对应比特翻转、相位翻转以及没有发生翻转的情况。

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2.2 数据传输阶段

1) 假设 Alice 有 $2N$ 位组成的秘密信息。其消息可描述为 $\{x_1, x_2, \dots, x_{2N}\}$ ，其中 $x_i \in \{0, 1\}$ ；Bob 有 $2M$ 位组成的秘密消息，其消息为 $\{y_1, y_2, \dots, y_{2M}\}$ ，其中 $y_i \in \{0, 1\}$ 。为了安全地交换他们的消息，进行秘密对话，在不失一般性的情况下，可以设置 $N = M$ 。

2) Bob 使用所得的 $2M_0$ 个生成元编码待发送的量子比特序列 $\{y_1, y_2, \dots, y_{2M}\}$ 中的每一个 y_i ，对于自对偶 $(j, 2k)(2M, M_0)$ 量子低密度奇偶校验码，可一次性编码 $4M - 2k$ 个量子比特。

$$\begin{aligned} |y_1, \dots, y_i, \dots, y_{4M-2k}\rangle &= \left[\prod_{i=1}^{2M_0} (I + M_i) \right] \cdot \\ \overline{Y}_1^{y_1} \dots \overline{Y}_i^{y_i} \dots \overline{Y}_{4M-2k}^{y_{4M-2k}} |0 \dots 0\rangle &= \\ \overline{Y}_1^{y_1} \dots \overline{Y}_i^{y_i} \dots \overline{Y}_{4M-2k}^{y_{4M-2k}} \cdot \left(\sum_{M_0 \in W} M_i |0 \dots 0\rangle \right) \end{aligned} \quad (3)$$

其中， $|y_1, \dots, y_i, \dots, y_{4M-2k}\rangle$ 为 $4M - 2k$ 个量子比特状态序列， y_i 取 0 或 1，表示成任何 0,1 顺序的发送序列； $\mathbf{I}$ 为单位矩阵； M_i 为校验矩阵 $\mathbf{H}$ 的生成元空间 W 中的第 i 个生成元； $\overline{Y}_i^{y_i}$ 是校验矩阵 $\mathbf{H}$ 中第 i 行 $\overline{Y}_i$ 被序列中对应位置的 y_i 作用产生的由 0 和 1 组成的序列。Bob 将使用上式编译完成的量子比特序列 $\{y'_1, y'_2, \dots, y'_{2M}\}$ ，通过量子信道发送给待对话的通话方 Alice。

3) Bob 从 $\{y_1, y_2, \dots, y_{2M}\}$ 中随机选取长度为 $\frac{m}{2}$ 的子集 Q ，并记录集合 Q 中元素在原序列中所位置。将集合 Q 以及相关位置信息打包，通过经典网络信道传输给 Alice。

4) Alice 收到数据包后，将 Q 中元素与 $\{y'_1, y'_2, \dots, y'_{2M}\}$ 中对应位置的数据比较，可计算其误码率 $P = \frac{e}{m}$ ，其中 e 为误码数。为了保证量

子信道传输中发生的误码在自对偶量子低密度奇偶校验码的检错及纠错范围内，当 $P < t$ 时进入下一步；否则启动量子比特数据的重传操作。

5) Alice 使用从校验矩阵 $\mathbf{C}$ 中可得到 $2M_0$ 个生成元编码待发送的量子比特序列 $\{x_1, x_2, \dots, x_{2N}\}$ 中的每一个 x_i ，对于自对偶 $(j, 2k)(2N, M_0)$ 量子低密度奇偶校验码，可一次性编码 $4N - 2k$ 个量子比特。

$$\begin{aligned} |x_1, \dots, x_i, \dots, x_{4N-2k}\rangle &= \left[\prod_{i=1}^{2M_0} (I + M_i) \right] \cdot \\ \overline{X}_1^{x_1} \dots \overline{X}_i^{x_i} \dots \overline{X}_{4N-2k}^{x_{4N-2k}} |0 \dots 0\rangle &= \\ \overline{X}_1^{x_1} \dots \overline{X}_i^{x_i} \dots \overline{X}_{4N-2k}^{x_{4N-2k}} \cdot \left(\sum_{M_0 \in W} M_i |0 \dots 0\rangle \right) \end{aligned} \quad (4)$$

其中， $|x_1, \dots, x_i, \dots, x_{4N-2k}\rangle$ 为 $4N - 2k$ 个量子比特状态序列， x_i 取 0 或 1，表示成任何 0,1 顺序的发送序列； $\mathbf{I}$ 为单位矩阵； M_i 为校验矩阵 $\mathbf{C}$ 的生成

元空间 W 中的第 i 个生成元; $\overline{X_i^{x_i}}$ 是校验矩阵 C 中第 i 行 $\overline{X_i}$ 被序列中对应位置的 x_i 作用产生的由 0 和 1 组成的序列。Alice 将使用上式编译完成的量子比特序列 $\{x'_1, x'_2, \dots, x'_{2N}\}$, 通过量子信道发送给待对话的通话方 Bob。

6) Alice 从 $\{x_1, x_2, \dots, x_{2N}\}$ 中随机选取长度为 $\frac{n}{2}$ 的子集 G , 并记录集合 G 中元素在原序列中的位置。将集合 G 以及相关位置信息打包, 通过经典网络信道传输给 Bob。

7) Bob 收到数据包后, 将 G 中元素与 $\{x'_1, x'_2, \dots, x'_{2N}\}$ 中对应位置的数据比较, 可计算其误码率 $P = \frac{e}{\frac{n}{2}}$, 其中 e 为误码数。为了保证量子

信道传输中发生的误码在自对偶量子低密度奇偶校验码的检错及纠错范围内, 当 $P < t$ 时进入下一步; 否则启动量子比特数据的重传操作。

8) 量子对话完成。

3 安全性分析

对于使用校验矩阵 H 的生成元编码而成的 $\{y'_1, y'_2, \dots, y'_{2M}\}$ 来说, 若传输过程中没有发生错误, 则其中任意的元素 y'_i 有

$$y'_i H^T = 0 \quad (5)$$

若在传输过程中发生了量子态翻转错误, 则 y'_i 变为 $y'_i + e_i$, 此时有

$$(y'_i + e_i) H^T = y'_i H^T + e_i H^T = e_i H^T \quad (6)$$

由式(6)可以得出结论, 对于不同的翻转错误 e_i , 可以得到其不同的伴随式。在误码检错时, 对应不同的误码伴随式, 可以方便地检测出误码种类, 纠正这些误码。对应误码检测结果, 对于不同的翻转错误进行相应的纠错门操作, 最终实现量子比特的正确传输。

对于使用校验矩阵 C 的生成元编码而成的 $\{x'_1, x'_2, \dots, x'_{2N}\}$ 来说, 若传输过程中没有发生错误, 则其中任意的元素 x'_i 有

$$x'_i C^T = 0 \quad (7)$$

若在传输过程中发生了量子态翻转错误,

则 x'_i 变为 $x'_i + e_i$, 此时有

$$(x'_i + e_i) C^T = x'_i C^T + e_i C^T = e_i C^T \quad (8)$$

由式(8)可以得出结论, 对于不同的翻转错误 e_i , 可以得到其不同的伴随式。在误码检错时, 对应不同的误码伴随式, 可以方便地检测出误码种类, 纠正这些误码。对应误码检测结果, 对于不同的翻转错误进行相应的纠错门操作, 最终实现量子比特的正确传输。

4 结束语

本文提出基于自对偶量子低密度校验码的量子对话协议, 用自对偶量子低密度校验码对通信双方的信息进行编码, 并相互传输, 以实现量子比特的正确传输。安全分析表明, 该协议具有足够的安全性, 能够有效抵御常见的恶意攻击。本文从纠错的角度研究所提量子对话协议的安全性。

参考文献:

- [1] BENNETT C H. Quantum cryptography : public key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. 1984: 175-179.
- [2] CAI Q Y, LI B W. Deterministic secure communication without using entanglement[J]. Chinese Physics Letters, 2004, 21(4): 601-603.
- [3] LI X H, DENG F G, LI C Y, et al. Quantum secure direct communication without maximally entangled states[J]. Journal of the Korean Physical Society, 2006, (49): 1354-1359.
- [4] BOSTRÖM K, FELBINGER T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902.
- [5] LONG G L, LIU X S. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. Physical Review A, 2002, 65(3): 032302.
- [6] DENG F G, LONG G L. Secure direct communication with a quantum one-time pad[J]. Physical Review A, 2004, 69(5): 052319.
- [7] GUERRA A G D A H, RIOS F F S, RAMOS R V. Quantum secure direct communication of digital and analog signals using continuum coherent states[J]. Quantum Information Processing, 2016, 15(11): 4747-4758.
- [8] WANG C, DENG F G, LI Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding[J]. Physical Review A, 2005, 71(4): 044305.
- [9] ZHU F, ZHANG W, SHENG Y B, et al. Experimental long-distance quantum secure direct communication[J]. Science Bulletin, 2017, 62(22): 1519-1524.

- [10] WU F Z, YANG G J, WANG H B, et al. High-capacity quantum secure direct communication with two-photon six-qubit hyperentangled states[J]. Science China(Physics, Mechanics & Astronomy), 2017, 60(12): 24-30.
- [11] NGUYEN B A. Quantum dialogue[J]. Physics Letters A, 2004, 328(1): 6-10.
- [12] GAO F, GUO F Z, WEN Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication[J]. Science in China, 2008(5): 111-118.
- [13] SUN Y, WEN Q Y, GAO F, et al. Improving the security of secure quantum telephone against an attack with fake particles and local operations[J]. Optics Communications, 2009, 282(11): 2278-2280.
- [14] WANG H, ZHANG Y Q, LIU X F, et al. Efficient quantum dialogue using entangled states and entanglement swapping without information leakage[J]. Quantum Information Processing, 2016, 15(6): 2593-2603.
- [15] GAO G. Two quantum dialogue protocols without information leakage[J]. Optics Communications, 2010, 283(10): 2288-2293.
- [16] YE T Y. Quantum dialogue without information leakage using a single quantum entangled state[J]. International Journal of Theoretical Physics, 2014, 53(11): 3719-3727.
- [17] ZHENG C, LONG G F. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs[J]. Science China Physics Mechanics & Astronomy, 2014, 57(7): 1238-1243.
- [18] QI J M, XU G, CHEN X B, et al. Two authenticated quantum dialogue protocols based on three-particle entangled states[J]. Quantum Information Processing, 2018, 17(9): 247.
- [19] ZHANG L, DONG S, ZHANG K J, et al. A controller-independent quantum dialogue protocol with four-particle states[J]. International Journal of Theoretical Physics, 2019, 58(6): 1927-1936.
- [20] LIU Z H, CHEN H W. Security loopholes in the controlled quantum dialogue robust against conspiring users protocol[J]. Quantum Information Processing, 2019, 18(7): 228.
- [21] ZHANG M H, CAO Z W, PENG J Y, et al. Fault tolerant quantum dialogue protocol over a collective noise channel[J]. The European Physical Journal D, 2019, 73(3): 57.
- [22] YANG Y, GAO S, ZHOU Y, et al. New secure quantum dialogue protocols over collective noisy channels[J]. International Journal of Theoretical Physics, 2019, 58(9): 2810-2822.

- [23] 齐佳敏. 基于纠缠态和身份认证的量子对话协议的设计与研究[D]. 北京: 北京邮电大学, 2019.

QI J M. Design and research of quantum dialogue protocol based on entangled state and identity authentication[D]. Beijing: Beijing University of Posts and Telecommunications, 2019.

[作者简介]



刘芬(1996-), 女, 山东潍坊人, 青岛理工大学硕士生, 主要研究方向为量子通信。



贺振兴(1995-), 男, 山东淄博人, 青岛理工大学硕士生, 主要研究方向为应用数学。



徐鹏翱(1995-), 男, 山东菏泽人, 青岛理工大学硕士生, 主要研究方向为量子通信。



马鸿洋(1976-), 男, 山东即墨人, 博士, 青岛理工大学教授, 主要研究方向为网络空间安全、量子信息、量子保密通信。