引用本文:罗贤俊,林泽洪,刘尉悦. 基于奇偶校验极化码的量子密钥纠错方法[J]. 光通信技术,2024,48(6):104-107.

基于奇偶校验极化码的量子密钥纠错方法

罗贤俊[1],林泽洪[2*],刘尉悦[1]

(1.宁波大学 信息科学与工程学院,浙江 宁波 315211;2.丽水职业技术学院 电子信息学院,浙江 丽水 323000)

摘要:为了提升量子密钥分发(QKD)中密钥纠错的性能,提出了一种基于奇偶校验极化码的量子密钥纠错方法。该方法在密钥纠错过程中引入了奇偶校验极化码,并优化了奇偶校验编码策略,利用密钥极化编码后生成的奇偶校验信息完成密钥纠错。仿真结果表明:与现有的基于极化码的密钥纠错方法相比,该方法可以在相同的量子比特误码率下获得更高的纠错效率;当实际 QKD 实验中的量子比特误码率为 0.010 48 时,其纠错效率达到 1.34,安全成码率可达 1 319 b/s。

关键词:量子光学;奇偶校验;极化码;误码纠错;纠错效率

中图分类号:TN918.1　**文献标志码**:A　**文章编号**:1002-5561(2024)06-0104-04

DOI:10.13921/j.cnki.issn1002-5561.2024.06.019　**开放科学(资源服务)标识码(OSID)**:

Quantum key error correction method based on parity check polar code

LUO Xianjun[1], LIN Zehong[2*], LIU Weiyue[1]

(1. Faculty of Information Science and Engineering, Ningbo University, Ningbo Zhejiang 315211, China;
2. School of Electronics and Information, Lishui Vocational and Technical College, Lishui Zhejiang 323000, China)

Abstract: To enhance the error correction performance of quantum key distribution (QKD), a quantum key error correction method based on parity check polar codes is proposed. This method introduces parity check polar codes into the key error correction process and optimizes the parity check encoding strategy. It uses the parity check information generated by key polar encoding to complete the key error correction. The simulation results show that compared with the existing polar code-based key error correction method, this method can achieve higher error correction efficiency at the same quantum bit error rate, when the actual QKD experiment's quantum bit error rate is 0.010 48, its error correction efficiency reaches 1.34, and the secure coding rate can reach 1 319 b/s.

Key words: quantum optics, parity check, polar code, error correction, error correction efficiency

0 引言

量子密钥分发(QKD)可以为远程用户提供理论上绝对安全的密钥[1-2]。在实际系统中,由于物理噪声、窃听者攻击等因素的影响,制备、传输和检测过程中的量子态可能会产生错误比特[3]。密钥纠错通过经典信道交换密钥的校验信息来纠正这些错误比特[4]。为了保证分发密钥的安全性,经典信道暴露的信息需要被剔除。降低密钥纠错过程暴露的信息量,提高 QKD 的安全成码率是密钥纠错的主要目标。

极化码是一种能够达到香农极限的信道编码方式,其对应的串行抵消(SC)译码算法具有较低的解码复杂度[5-6]。NAKASSIS A 等人[7]将极化码引入密钥纠错,发送方将量子密钥经过极化编码后的冻结比特(frozen bits)通过公共信道传递给接收方,接收方根据接收到的量子密钥信息和冻结比特恢复出与发送方极化编码结果一致的密钥信息,从而完成密钥纠错。然而,SC 译码算法在处理信道容量不为 1 的信息位时容易出现错误[8]。YAN S 等人[9]提出了将串行抵消列表(SCL)译码算法应用于密钥协商的方法。SCL 解码过程中计算每条路径的译码值后验概率,并始终保留后验概率最大的 l 条路径继续译码[10],从而减少了丢失正确路径的可能性,改进了基于极化码的误码协商方

收稿日期:2024-06-12。

基金项目:浙江省自然科学基金项目(LY21F050003、LY23F010003)资助。

作者简介:罗贤俊(2000—),男,硕士研究生,现就读于宁波大学信息科学与工程学院通信工程专业,主要从事量子通信密钥分发技术的研究,并针对密钥分发后处理过程中密钥纠错过程进行优化算法的研究及仿真验证。

*** 通信作者**:林泽洪(1989—),男,硕士,主要研究方向为量子通信与应用。

法。尽管在 SCL 译码中正确码字有较高概率出现在生成的列表中,但其并不一定是列表中后验概率最大的码字,这可能导致密钥纠错失败。LEE S 等人[11]在密钥纠错应用中,采用了循环冗余校验(CRC)辅助下的串行抵消列表译码(CA-SCL)方法。他们通过经典信道传输密钥的 CRC 校验信息,并在 SCL 译码结束时,选择那些通过 CRC 校验的路径作为密钥纠错的结果,从而有效地提高了极化码在密钥纠错应用中的性能。然而,CRC 校验仅在译码结束时辅助选择正确的结果,在整个译码过程中并不能检测错误。因此,本文提出一种基于奇偶校验极化码的量子密钥纠错方法,在 QKD 系统中实现更高的安全成码率。

1 基于奇偶校验极化码的量子密钥纠错方法

极化编码可以将一个独立的离散无记忆信道极化为 2 类子信道:一类是噪声子信道(冻结位,其信道容量接近于 0),另一类则是无错误子信道(信息位,其信道容量趋向于 1)。在传统的基于极化码的密钥纠错方法中,通常直接依据子信道的译码错误概率来划分冻结位和信息位[12],并且在经典信道上传输那些位于冻结位的比特信息。本文在密钥纠错过程中,则将原本要发送的噪声子信道的冻结位比特信息替换为冻结位的奇偶校验信息,在译码过程中利用冻结位的奇偶校验信息来及时检测错误的译码路径。基于奇偶校验极化码的量子密钥纠错方法原理框图如图 1 所示。

假设 Alice 和 Bob 分别是通信双方的两端。x、y 分别表示 Alice 和 Bob 在 QKD 过程传输和筛选完成后得到的筛选码。c 是冻结位集合。首先,Alice 将它的筛选码 x 经过极化编码 $u=xG_n$ 得到序列 u,其中 G_n 表示极化码生成矩阵。接着,Alice 计算 u 的 CRC 校验值和 u 在冻结位置生成的奇偶校验值 p,并通过经典信道发送给 Bob。Bob 根据从经典信道接收到的信息和自己的筛选码 y 进行译码,得到 L 条译码结果。然后,选择通过 CRC 校验的译码结果 $\hat{u}$ 作为最终的译码结果,并对 $\hat{u}$ 进行极化编码,从而使 Bob 能够恢复出与 Alice 端筛选码一致的密钥 x,完成密钥纠错。其中,奇偶校验信息是由当前冻结位比特与其前面的一部分比特进行异或运算得到的。在奇偶校验极化码的译码过程中,路径译码结果的奇偶校验需要与接收的值相匹配。当校验位置之前的比特译码出现奇数个错误时,当前冻结位会得到一个错误的结果,从而增加了错误路径与正确译码结果之间的距离。这意味着错误路径有更多的错误位置,因而具有更低的后验概率,降低了错误路径存活的可能性,从而提高了密钥纠错获得正确结果的概率。

1.1 奇偶校验计算

奇偶校验计算是在给定极化编码结果和冻结位置集合的情况下,计算在经典信道中发送的奇偶校验值。奇偶校验的作用是检测路径中已译码部分是否存在奇数个错误。考虑到极化码结构中冻结位和信息位总是连续出现的特点,为了更有效地检测路径是否存在译码错误,被校验的信息位应当分散在不同的校验位中。一种简单易行的方法是采用分组奇偶校验,即将间距为 k 的比特信息归入同一组内,使得每个奇偶校验值仅与同一分组内的比特有关,如式(1)所示。

$$p_i=\bigoplus_{j=0}^{\lfloor i/k \rfloor} u_{i-jk} \tag{1}$$

其中,$\oplus$ 表示异或,i 表示奇偶校验所在位置的索引,j 表示异或项的编号。

分组奇偶校验计算中,每一个分组会包含多个冻结位置。设 i_1、i_2 表示同一分组内的 2 个冻结位置的索引。$i_1<i_2$ 且间距为 k 的倍数。由式(1)可以得

$$p_{i_2}=\bigoplus_{j=0}^{\lfloor i_2/k \rfloor} u_{i_2-jk}=\bigoplus_{j=0}^{(i_2-i_1)/k} u_{i_2-jk}\bigoplus_{j=0}^{\lfloor i_1/k \rfloor} u_{i_1-jk}=\bigoplus_{j=0}^{(i_2-i_1)/k} u_{i_2-jk}\oplus p_{i_1} \tag{2}$$

从解码角度看,在位置 i_1 处进行奇偶校验时,如果被检测比特 $[u_{i\%k}, u_{i\%k+k}, \cdots, u_{i_1-2k}, u_{i_1-k}]$ 存在奇数错误译码,则当前路径译码在 i_1 处会得到一个错误的译码值,从而使得该路径通过奇偶校验。在这种情况下,后续在 i_2 位置进行的校验,无法对 $[u_{i\%k}, u_{i\%k+k}, \cdots, u_{i_1-2k}, u_{i_1-k}]$ 这部分比特值的错误进行有效检测。因此,位置 i_2 的奇偶校验实际检测范围限于当前冻结位与上一个冻结位之间的信息比特。若在编码计算时跳过路径中的冻结比特,则可以扩大奇偶校验的检测范围。

另一方面,如果 $[u_{i\%k}, u_{i\%k+k}, \cdots, u_{i_1-2k}, u_{i_1-k}]$ 出现偶

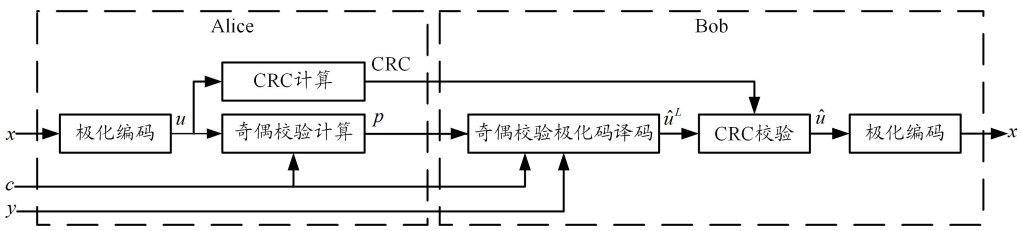

图 1 基于奇偶校验极化码的量子密钥纠错方法原理框图

数个错误译码,则位置 i_1 处的奇偶校验失效。按式(1)的编码方式,在后续位置 i_2 的校验中仍然无法检测这部分错误。因此,在位置 i_2 计算奇偶校验值时,应该只包括[$u_{i\%k}$,$u_{i\%k+k}$,…,u_{i_1-2k},u_{i_1-k}]的一部分,并将可能出现偶数次错误译码的位置再拆分到不同的校验中,以提高奇偶校验对错误路径的检测能力。

综上所述,可以得出优化后的奇偶校验计算方法:将极化码编码的结果分组后,每个奇偶校验值由以下三部分比特值异或而成:

1)当前位置的冻结比特;

2)当前冻结位与上一个冻结位之间的所有信息比特;

3)上一个冻结位之前的部分信息比特。

设置 reg_cur 存储每个分组中奇数位置和偶数位置的奇偶校验信息;reg_last 存储上一次冻结位奇偶校验计算时每个分组中奇数位置和偶数位置的奇偶校验值;reg_state 表示上一次校验计算使用的是奇数位置的校验信息还是偶数位置的校验信息。优化后的奇偶校验计算过程如自算法 1 所示。

算法 1 奇偶校验计算

输入:极化码编码结果 u,冻结位置集合 c,分组距离 k,码长 n

输出:奇偶校验值 p

1) 初始化:reg_cur[0]= reg_cur[1]=…= reg_cur[2k−1]=0

reg_last[0]=reg_last[1]=…=reg_last[2k−1]=0

reg_state[0]=reg_state[1]=…= reg_state[k−1]=0

p[0]=p[1]=… =p[n−1]=−1

for i=0: n−1

2) if $i\in c$

//冻结位置校验信息计算

if reg_state[i%k]==0

p[i]=reg_last[i%k]^reg_cur[i%(2k)]^reg_cur[(i+k)%(2k)]^u[i]

3) else

p[i]=reg_last[i%(k)+k]^reg_cur[i%(2k)]^reg_cur[(i+k)%(2k)]^u[i]

4) end if

//校验信息继承

reg_last[i%k]=reg_cur[i%(2k)];

reg_last[i%k+k]=reg_cur[(i+k)%(2k)]

reg_state[i%k]=1−reg_state[i%k]

5) else

//分组奇偶校验信息更新

reg_cur[i%(2k)]=reg_cur[i%(2k)]^u[i]

6) end if

7) end for

1.2 奇偶校验极化码译码

奇偶校验极化码译码器在 SCL 译码器的基础上,修改了冻结位的译码方式。奇偶校验极化码译码器与 SCL 译码器在信息位置的解码方式是相同的。在冻结位置译码时,首先根据奇偶校验计算策略来计算冻结位之前的译码结果的奇偶校验值,然后将这个奇偶校验值与接收到的值进行比对。如果相同,冻结比特判决为 0;否则,冻结比特判决为 1。

2 仿真和验证

2.1 模拟仿真

密钥纠错主要评价指标有纠错效率 f 和纠错失败概率(FER)。纠错效率 f 定义为

$$f=\frac{m}{nH_2(E_\mu)} \tag{3}$$

其中,m 表示协商泄露信息量,n 表示码长,E_μ 表示量子比特误码率,$H_2(E_\mu)$表示二进制信息熵,$nH_2(E_\mu)$表示香农理论下完成纠错需要泄露信息量的理论值。仿真参数设置如表 1 所示。

表 1 仿真参数

参数	取值
CRC 校验长度 d/个	32
奇偶校验编码分组个数 k/个	9
列表大小 L/个	16

不同码率 R 条件下的 FER 表现如图 2 所示。在各种码率设置下,Pc-Polar 方法的 FER 均低于传统的 Polar 方法 Pc-Polar 方法(基于奇偶校验极化码的量子密钥纠错方法,本文方法)的 FER 均低于传统的 Polar 方法(基于极化码的密钥纠错方法[11])。当 FER 分别为 0.1 和 0.01 时,2 种方法的码率差值分别为 0.009 8 和 0.012 7。在密钥纠错过程中,使用更高的码率进行纠错意味着泄露的密钥信息更少。仿真结果显示,Pc-Polar 方法能够有效地减少信息泄露,并且在低 FER 条件下其效果尤为显著。本文选择 FER 最接近 0.01 的点计算纠错效率,得到 2 种方法在不同量子比特误码率的纠错效率,如表 2 所示。可以看出,当 E_μ 相同时,奇偶校验极化码在在 2 种码长(2^{10} 和 2^{16})下的纠错效率均优于极化码。在较短码长(2^{10})下,Pc-Polar 方法和 Polar 方法的纠错效率差距较大;而在较长码长

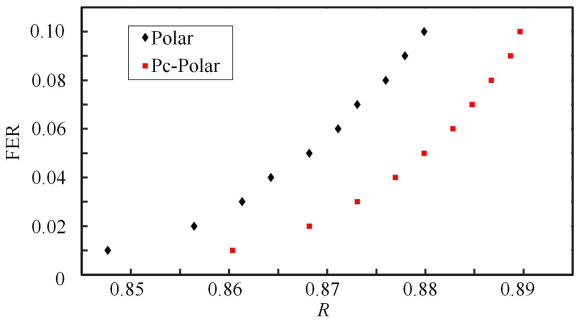

图 2 不同码率 R 下的 FER

表 2 不同量子比特误码率下的纠错效率

E_μ	纠错效率			
	$f_{\text{Polar},2^{10}}$	$f_{\text{Pc-Polar},2^{10}}$	$f_{\text{Polar},2^{16}}$	$f_{\text{Pc-Polar},2^{16}}$
0.005	2.171	1.956	1.428	1.394
0.01	1.886	1.728	1.341	1.312
0.015	1.738	1.651	1.297	1.276
0.02	1.622	1.539	1.265	1.245
0.025	1.563	1.505	1.244	1.221
0.03	1.507	1.457	1.225	1.209
0.035	1.472	1.428	1.21	1.196
0.04	1.451	1.402	1.197	1.187
0.045	1.42	1.383	1.187	1.176
0.05	1.394	1.35	1.177	1.169°

(2^{16})下,这种差距有所缩小,但 Pc-Polar 方法仍然更具优势。因此,使用 Pc-Polar 方法可以在QKD 系统中使纠错效率更接近 1。

2.2 实验验证

将本文方法应用到实际的 QKD 系统中进行实验验证。系统参数如下:基矢比对因子为 0.5,实验发射信号频率为 625 MHz,信号态平均光子数与诱骗态平均光子数分别为 0.8 和 0.1,信号态、诱骗态和真空态的比例为 2:1:1。实验中获取的原始密钥采用码长为 2^{16} 的 Pc-Polar 方法和 Polar 方法进行密钥纠错,结果如表 3 所示。其中,S 表示安全成码率。可以看出,在相同的实验条件下,由于基于奇偶校验极化码的 Pc-Polar 方法纠错效率比 Polar 方法高,其安全成码率也高于 Polar 方法。

表 3 实验结果

参数	值
链路衰减/dB	46.72
探测器的暗计数/(c/s)	756
E_μ	0.010 48
$f_{\text{Pc-Polar}}$	1.24
f_{Polar}	1.386
$S_{\text{Pc-Polar}}$/(b/s)	1 319
S_{Polar}/(b/s)	1 289

3 结束语

本文提出一种基于奇偶校验极化码的量子密钥纠错方法,通过将密钥纠错过程中要发送的冻结位比特信息替换为冻结位的奇偶校验信息,优化了极化码在密钥纠错中的应用。结果表明,与现有的基于极化码的密钥纠错方法相比,该方法在完成密钥纠错时所需暴露的信息量更少,使其纠错效率更加接近香农极限。这能够有效地提升基于极化码的密钥纠错方法在QKD 系统中的安全成码率。

参考文献:

[1] LO H K, MA X, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94: 230504-1–230504-5.

[2] RENNER R. Security of quantum key distribution[J]. International Journal of Quantum Information, 2008, 6(1): 1–127.

[3] LI J, PAN Z, ZHENG J, et al. The security analysis of quantum SAGR04 protocol in collective-rotation noise channel[J]. Chinese Journal of Electronics, 2015, 24 (4): 689–693.

[4] JESUS M, DAVID E, VICENTE M. Key reconciliation for high performance quantum key distribution[J]. Scientific reports, 2013, 3 (1): 1576-1–1576-6

[5] ARIKAN E. Channel polarization: a method for constructing capacity-achieving codes [C]//IEEE. Proceedings of International Symposium on Information Theory. Toronto: IEEE, 2008: 1173–1177.

[6] ARIKAN E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels[J]. IEEE Transactions on Information Theory, 2009, 55(7): 3051–3073.

[7] NAKASSIS A, MINK A. Polar codes in a QKD environment[J]. National Institute of Standards and Technology, 2014, 9123(1): 912305-1–912305-11.

[8] JOUGUET P, KUNZ-JACQUES S. High performance error correction quantum key distribution using polar codes[J]. Quantum Information & Computation, 2014, 14 (3/4): 329–338.

[9] YAN S, WANG J, FANG J, et al. An improved polar codes-based key reconciliation for practical quantum key distribution[J]. Chinese Journal of Electronics, 2018, 27 (2): 250–255.

[10] TAL I, VARDY A. List decoding of polar codes[J]. IEEE Transactions on Information Theory, 2015, 61(5): 2213–2226.

[11] LEE S, PARK J, HEO J. Improved reconciliation with polar codes in quantum key distribution [J]. Quantum Information & Computation, 2018, 18(9): 795–813.

[12] TAL I, VARDY A. How to construct polar codes[J]. IEEE Transactions on Information Theory, 2013, 59 (10): 6562–6582.