华南师范大学学报(自然科学版)
Journal of South China Normal University(Natural Science Edition)
2019,51(2):1-6
doi:10.6054/j.jscnun.2019015

基于极化码的单步量子密钥分发后处理

李　锦[1],蒋　琳[2],林旭城[1],方俊彬[1*]
(1. 暨南大学光电工程系//广东省可见光通信工程技术研究中心//广州市可见光通信工程技术重点实验室,广州 510632;
2. 哈尔滨工业大学(深圳)计算机科学与技术学院,深圳 518005)

摘要: 量子密钥分发结合"一次一密"的加密方案可以从理论上保证通信的无条件安全性. 然而,量子密钥分发后处理过程中的误码纠错和密性放大这2个步骤引入了较高的处理延时,影响了最终安全密钥生成速率以及量子密钥分发系统的实用性. 文中提出一种基于极化码的单步高效量子密钥后处理算法,根据Wyner窃听信道模型分析合法通信双方以及窃听者的信道容量,设计出可同时满足可靠性和安全性的极化码码字结构,并将其应用于量子密钥分发后处理,从而实现在一次编译码步骤中同时完成误码纠错和密性放大,将这2个处理步骤合二为一,降低了系统复杂度和处理延时. 实验结果表明,在量子比特误码率 $[0,0.08]$ 范围内,提出的算法可同时满足纠后误码率 $\leqslant 10^{-7}$ 的可靠性条件以及窃听信息量 $\leqslant 10^{-14}$ bit 的安全性条件. 当码长为 2^{20} bit 时,译码吞吐率可达3 Mb/s,采用并行算法的译码吞吐率可达86 Mb/s.

关键词: 量子密钥分发; 后处理; 极化码; 误码纠错; 密性放大
中图分类号: TN918　　**文献标志码:** A　　**文章编号:** 1000-5463(2019)02-0001-06

Polar Codes-Based One-Step Post-Processing of Quantum Key Distribution

LI Jin[1], JIANG Lin[2], LIN Xucheng[1], FANG Junbin[1*]
(1. Department of Optoelectronic Engineering, Jinan University//Guangdong Provincial Engineering Technology Research Center on Visible Light Communication//Guangzhou Municipal Key Laboratory of Engineering Technology on Visible Light Communication, Guangzhou 510632, China; 2. School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518005, China)

Abstract: Quantum key distribution guarantees the unconditional security of communication by combining with the one-time pad encryption scheme. However, the error correction and privacy amplification of quantum key distribution post-processing may result in high processing delay, influencing the final secret key generation rate and the practicality of quantum key distribution system. Therefore, a one-step post-processing algorithm based on polar codes for quantum key distribution was proposed. By analyzing the channel capacity of the two legal communicators and the eavesdropper respectively under the Wyner's wiretap channel model, a codeword structure of polar codes is designed, which can satisfy the reliability and security of quantum key distribution post-processing, so that the error correction and privacy amplification can be completed synchronously in every encoding and decoding step. Combining the two processing steps into one, it reduces the system complexity and the processing delay. Experimental results show that the proposed algorithm can satisfy the reliability condition of a bit error rate less than 10^{-7} after error correction and the security condition of the information eavesdropping less than 10^{-14} bit in the quantum bit error rate $[0,0.08]$, and the decoding throughput can achieve 3 Mb/s and 86 Mb/s with parallel decoding under the code length 2^{20} bit.

Keywords: quantum key distribution; post-processing; polar codes; error correction; privacy amplification

收稿日期: 2019-01-27　　《华南师范大学学报(自然科学版)》网址: http://journal.scnu.edu.cn/n
基金项目: 国家自然科学基金项目(61771222);广东省科技计划项目(2016A010101017);广州市科技计划项目(201707010253,201803020023);深圳基础研究项目(JCYJ20170815145900474)

* 通信作者:方俊彬,教授,Email: junbinfang@foxmail.com.

量子密钥分发(Quantum Key Distribution,QKD)结合“一次一密”的加密方式可以从理论上保证通信系统的无条件安全性[1-3],是近年来兴起的保障信息安全的有效解决方案之一. 实际QKD系统中通常采用光子作为量子比特的信息载体[4-5]易受到器件缺陷等影响引入比特误码及泄露信息,因此需要通过后处理中的误码纠错和密性放大2个步骤分别纠正量子信道传输所引入的比特误码并剔除泄露信息量,但这2个步骤增加的系统处理开销和引入的较高的处理延时成为高速QKD系统的瓶颈[6-7],限制了量子密钥分发的进一步实用化. 最先用于QKD后处理误码纠错的BBBSS算法[8]以及基于其改进的级联奇偶校验二分法Cascade算法[9],由于频繁的信息交互导致处理延时较高、纠错速度较低. 随后提出的基于汉明码的Winnow算法[10]只需传输一次校验信息即可纠正密钥段,但是在量子比特误码率安全阈值范围内的纠错效率较低;而ELKOUSS提出将LDPC码用于QKD后处理[11]以获得更好的纠错性能,但是由于LDPC码的校验矩阵依赖于具体误码率,且采用迭代译码导致译码复杂度较高;2014年,JOUGUET研究组首次将码率可达香农极限的极化码应用于QKD后处理的误码纠错,实验结果表明其具有较高的编码效率和纠错速度[12]. 另外,在密性放大步骤中普遍采用通用类哈希函数[13]进行信息压缩以保证密钥安全性,但由于运算次数较多从而导致延时较高.

为了解决QKD后处理延时和系统复杂度较高的问题,本文提出一种基于极化码的单步量子密钥分发后处理算法,通过设计可同时满足可靠性和安全性的极化码码字结构用于QKD后处理,将误码纠错和密性放大2个延时最高的环节合二为一,以达到减少QKD后处理延时和系统复杂度,提升最终密钥生成速率的目的,可突破高速QKD系统的瓶颈,提升QKD系统的实用性.

1 基本原理

1.1 Wyner窃听信道模型

保密通信的目的是使得合法通信双方在被窃听的情况下依然可以实现安全可靠的信息传输. 图1为Wyner窃听信道模型[14]. 发送方Alice将长度为k的原始信息U进行编码生成码长为n的码字X,并通过主信道W发送给合法接收方Bob. 与此同时,窃听方Eve通过窃听信道W^*窃听信息,传输过后Bob和Eve分别获取到信息Y和Z,并分别译码得到对原始信息U的译码估计$\hat{U}'$和$\hat{U}''$.

在Wyner窃听信道模型中,当窃听信道W^*关于主信道W退化时(即窃听信道容量$C(W^*)$小于主信道容量$C(W)$),随着码长趋近于无限长,可设计安全编码方案满足信息的可靠性和安全性,并用安全容量$C_{\text{sec}}=C(W)-C(W^*)$表征此安全编码方案的理论最大编码码率,即:对于任意$\varepsilon>0$,当编码码率$R\geqslant C_{\text{sec}}-\varepsilon$时,存在一种编码方案可以渐进地满足信息的可靠性和安全性[15].

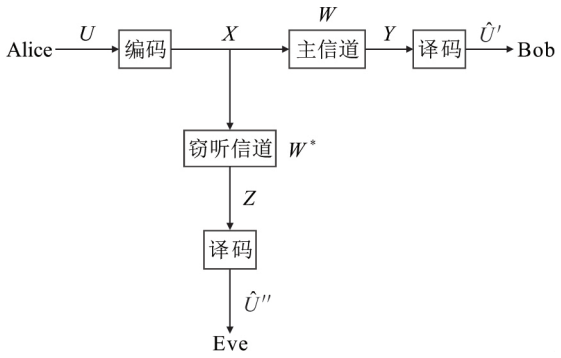

图1 窃听信道模型

Figure 1 The wiretap channel model

可靠性用接收方Bob译码后的比特误码率衡量,即:

$$\lim_{n\to\infty} Pr\{\hat{U}'\neq U\}=0. \tag{1}$$

安全性用窃听端获取到窃听信息和原始信息间的互信息量衡量,即:

$$\lim_{n\to\infty} I(\hat{U}'';U)=0. \tag{2}$$

结合互信息量与条件熵之间的转换关系式:

$$I(U;\hat{U}'')=H(U)-H(U|\hat{U}'')=1-H(U|\hat{U}''), \tag{3}$$

式(2)可进一步写成:

$$\lim_{n\to\infty} Pr(\hat{U}''\neq U)=0.5. \tag{4}$$

因此,设计一个满足可靠性和安全性的编码方案,应该同时保证Bob与Eve的译码误码率分别趋近于0和0.5.

1.2 离散QKD系统的安全容量

在量子密钥分发系统中,发送端Alice和接收端Bob是在完成量子密钥比特传输和对基(调制基与测量基的对比)以后获得筛后密钥$K_{A,\text{sifted}}$和$K_{B,\text{sifted}}$的. 由于实际系统存在器件缺陷[16]、信道噪声等因素以及可能存在被窃听的操作,一般来说$K_{A,\text{sifted}}\neq K_{B,\text{sifted}}$,即存在误码比特,记为量子比特误

码率 p. 对于离散变量 QKD 系统/BB84 密钥分发协议来说,传输量子密钥比特的信道可看作二进制对称信道(Binary symmetric channel,BSC) ,Alice 和 Bob 之间的平均互信息量 $I_{AB}=1-h_2(p)$,其中 $h_2(\cdot)$ 为二进制熵函数[11] . 从系统最大安全性考虑,认为筛后密钥中的所有误码比特均由窃听者 Eve 的窃听操作引起,即 Eve 所获得的窃听信息量为 $I_{AE}=h_2(p)$. 使用 Wyner 窃听信道模型描述 QKD 系统,则 Alice 与 Bob 之间的主信道容量为 $C(W)=I_{AB}=1-h_2(p)$,而 Alice 与 Eve 之间的窃听信道容量为 $C(W^*)=I_{AE}=h_2(p)$,系统的安全容量为 $C_{sec}=C(W)-C(W^*)=1-2h_2(p)$,等于离散变量 QKD 系统的安全成钥率 k_{th}[16] .

由于离散变量 QKD 系统的安全成钥率上限 $k_{th}=1-2h_2(p)\geqslant 0$,则量子比特误码率 p 的取值范围为 [0,0.11] . 因此在此范围内有 $C(W^*)<C(W)$,即窃听信道是关于主信道退化的,有 $C_{sec}\geqslant 0$,满足 Wyner 窃听信道模型中关于退化的假设,因此可针对 QKD 设计纠错编码方案达到安全容量.

1.3　极化码

极化码是目前唯一被理论证明对于任何二进制离散无记忆信道,其编码码率可达到香农信道容量极限,并且编译码复杂度相对 LDPC 码等较低的新型编码[17] . 通过对 N 个信道容量为 C_N 的独立同分布信道进行递归信道极化操作,所得到的 N 个虚拟比特子信道的信道容量呈现两极化: $N\times C_N$ 个信道容量趋近于 1 的“优化信道”和 $N\times(1-C_N)$ 个信道容量趋近于 0 的“劣化信道”. 然后,通过将信息比特编码在“优化信道”上发送而将休眠比特编码在“劣化信道”上发送即可实现信息比特的“无差错传输”,由此构成编码码率可达香农信道容量极限的极化码纠错编码.

不同的信道采用不同的方法计算评估虚拟比特子信道的信道质量,进而完成极化码码字构造. 对于 BSC 信道而言,采用虚拟比特信道的译码误码率 $P_{e,m}(W_N^{(i)})$ 来衡量虚拟比特信道的质量,并用渐进法计算得到 $P_{e,m}(W_N^{(i)})$ 上界用以构造极化码[18] .

2　基于极化码的单步量子密钥分发后处理算法

误码纠错和密性放大是后处理中的 2 个关键步骤. 误码纠错的目的是通过 Alice 与 Bob 的信息交互纠正双方筛后密钥中的差异比特,从而获得主信道的信道容量 $C(W)$; 而密性放大的目的是压缩 Alice与 Bob 之间的共享信息,从而剔除被窃听者所获取的窃听信道容量 $C(W^*)$.

针对后处理这 2 个关键步骤的主要功能,本文提出一种可同时实现误码纠错和密性放大的高效后处理编译码算法. 具体算法如下:

(1) 在 Alice 与 Bob 传输完量子密钥比特并经过对基获得筛后密钥之后,Alice 与 Bob 通过误码估算得到量子比特误码率 p,若 p 超出安全阈值,中止本次密钥分配,否则进入下一步骤.

(2) 令编码分组长度为 N,Alice 以 p 作为主信道的信道质量指标,采用极化码构造算法[18] 计算主信道所对应的 N 个虚拟比特子信道的译码误码率 $P_{e,m}(W_N^{(i)})\{i\in N\}$ 上界.

(3) Alice 将主信道的虚拟比特子信道按译码误码率 $P_{e,m}(W_N^{(i)})$ 上界从小到大排序. 根据可靠性要求条件:

$$\sum_i P_{e,m}(W_N^{(i)})\leqslant \mathrm{FER}=N\cdot\beta, \tag{5}$$

其中,FER 为纠错后的目标误帧率,β 为纠错后的目标误码率. 选择满足式(5) 的比特子信道组成优化子信道集 $G_N(W,\beta)$,其余比特子信道组成劣化信道集 $B_N(W,\beta)$.

将主信道对应的虚拟比特子信道划分为 2 类:

$$\begin{cases} G_N(W,\beta)=\{i\in[N],\sum_i P_{e,m}(W_N^{(i)})\leqslant(N\cdot\beta)\} \\ B_N(W,\beta)=\{N\backslash G_N(W,\beta)\}. \end{cases} \tag{6}$$

文献[12] 基于式(6) 所示的码字结构将极化码应用于后处理中的误码纠错,本文进一步设计编译码算法同时实现误码纠错和密性放大的功能.

(4) Alice 以 I_{AE} 作为窃听信道的信道质量指标,采用极化码构造算法计算窃听信道所对应的 N 个虚拟比特子信道的译码误码率 $P_{e,w}(W_N^{*(i)})\{i\in N\}$ 上界,并利用式(7) 换算为 N 个虚拟比特子信道的信道容量:

$$C_w(W_N^{*(i)})=1-h_2(P_{e,w}(W_N^{*(i)})). \tag{7}$$

(5) Alice 将窃听信道的虚拟比特子信道的信道容量 $C_w(W_N^{*(i)})$ 从小到大排序. 根据密性放大的目标安全性要求 δ_N 的选取满足式(8) 中比特子信道组成针对 Eve 的 δ_{N-poor} 劣化子信道集 $P_N(W^*,\delta_N)$,其余比特子信道组成针对 Eve 的非 δ_{N-poor} 劣化子信道集 not-

$P_N(W^*,\delta_N)$. 安全性要求条件为:

$$P_N(W^*,\delta_N)=\{i\in[N]\ \sum_i C_w(W_N^{*(i)})\leqslant\delta_N\}. \quad (8)$$

如果 Alice 将筛后密钥比特安置在 $\delta_{N-\text{poor}}$ 劣化子信道集 $P_N(W^*,\delta_N)$ 并将非 $\delta_{N-\text{poor}}$ 劣化子信道集 not$-P_N(W^*,\delta_N)$ 的比特预置为随机比特,采用系统极化码编码后并在公开信道上发送校验比特,因为编码结构针对 Eve 已经获得的信息量进行了劣化设计,则 Eve 的译码结果误码率为 0.5,窃听信息量压缩为 0.

(6) 如图 2 所示,经过以上步骤,N 个虚拟比特子信道分为 4 类: 对 Bob 的优化信道 $G_N(W,\beta)$、对 Bob 的劣化信道 $B_N(W,\beta)$,对 Eve 的劣化信道 $P_N(W^*,\delta_N)$、对 Eve 的非劣化信道 not$-P_N(W^*,\delta_N)$. 因为窃听信道关于主信道退化,所以对 Bob 劣化的信道也必然对 Eve 劣化,即 $P_N(W^*,\delta_N)$ 包含 $B_N(W,\beta)$; 从另一个角度看,总是存在一部分信道对 Bob 优化而对 Eve 劣化,即 $P_N(W^*,\delta_N)$ 与 $G_N(W,\beta)$ 存在交集,这部分比特子信道能够同时满足可靠性要求和安全性要求.

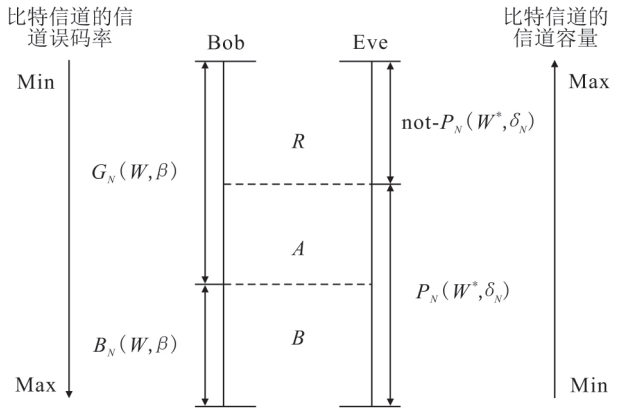

图 2 极化码的虚拟比特子信道构造

Figure 2 The virtual bit subchannel construction of polar codes

(7) Alice 根据上述所得的 4 类比特子信道集合,将非 $\delta_{N-\text{poor}}$ 劣化子信道集 not$-P_N(W^*,\delta_N)$ 的比特安排为随机比特,记为 R; 将筛后密钥比特安排在 $P_N(W^*,\delta_N)\cap G_N(W,\beta)$ 子信道集上,记为 A; 将 $B_N(W,\beta)$ 子信道集安排为休眠比特 0,记为 B. 关系式如下:

$$\begin{cases}R=[N]\setminus P_N(W^*,\delta_N)=\text{not}-P_N(W^*,\delta_N);\\ A=P_N(W^*,\delta_N)\cap G_N(W,\beta);\\ B=P_N(W^*,\delta_N)\setminus G_N(W,\beta)=B_N(W,\beta).\end{cases} \quad (9)$$

(8) Alice 将比特串 R、A、B 串联组成 N 比特长的原始码字,并用系统极化码编码算法[19]生成码字 CW_{enc},Alice 仅将码字中的校验比特部分 $\text{CW}_{\text{enc}}^{\text{check}}$ 经公开信道发送给 Bob 用于译码纠错(图 3).

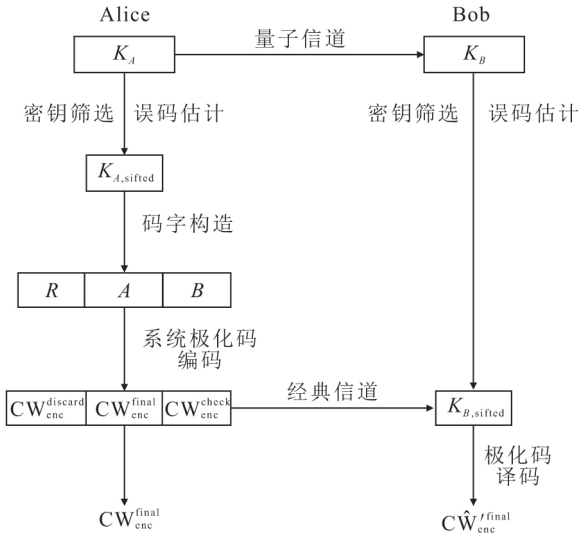

图 3 基于极化码的单步量子密钥后处理算法

Figure 3 The one-step post-processing algorithm based on polar codes for quantum key distribution

(9) Bob 在接收到 $\text{CW}_{\text{enc}}^{\text{check}}$ 后与自己持有的对应密钥比特 $K_{B,\text{sifted}}$ 组合并经系统极化码译码算法恢复得到 $\hat{\text{CW}}_{\text{enc}}^{\prime\text{final}}$. 因为根据式(5),式(9)所示的码字结构选择了对 Bob 优化的子信道传输密钥比特,故 $\hat{\text{CW}}_{\text{enc}}^{\prime\text{final}}$ 与 $\text{CW}_{\text{enc}}^{\text{final}}$ 之间的误码率低于所设定的纠后误码率,满足可靠性要求,所设计的编译码算法实现了误码纠错功能.

(10) Eve 在公开信道上也接收到 $\text{CW}_{\text{enc}}^{\text{check}}$,与在量子信道上窃听得到的对应密钥比特 $K_{E,\text{sifted}}$ 组合,同样经过系统极化码译码算法恢复得到 $\hat{\text{CW}}_{\text{enc}}^{\prime\prime\text{final}}$. 因为根据式(8),式(9)所示的码字结构选择了对 Eve 有 $\delta_{N-\text{poor}}$ 劣化的子信道传输密钥比特,故 $\hat{\text{CW}}_{\text{enc}}^{\prime\prime\text{final}}$ 与 $\text{CW}_{\text{enc}}^{\text{final}}$ 之间的误码率趋近于 0.5,Eve 的窃听信息量被压缩至 0,所设计的编译码算法实现了密性放大功能. 经上述算法,最终得到安全可靠的密钥对 $\{\text{CW}_{\text{enc}}^{\text{final}},\hat{\text{CW}}_{\text{enc}}^{\prime\text{final}}\}$.

3 算法验证分析

采用一系列的仿真实验以验证本文算法的性能,实验参数如下:(1) 分组码码长: $N=2^{20}$ bit; (2) 可靠性条件[12]: 纠错后误码率 $\beta\leqslant10^{-7}$; (3) 安全性条件[20]: 窃听信息量 $\delta_N\leqslant10^{-14}$ bit; 所设分组码长 2^{20} bit 以减缓极化码有限长效应,同时保证经本文

算法提取的最终密钥的误码率 $\leqslant 10^{-7}$，并且窃听端获取到的密钥信息 $\leqslant 10^{-14}$ bit，能够满足实际 QKD 系统的需求.

在量子比特误码率的理论阈值范围 [0,0.11] 内以步长 0.01 递增进行仿真测试. 本文算法所能达到的实际安全编码码率 R_c 和实际安全编码率可达安全容量的比率 $R_c:C_{sec}$ 如表 1 所示.

表 1　不同量子比特误码率下的安全编码码率

Table 1　The secret coding rate at different quantum bit error rates

量子比特误码率 p	安全容量 C_{sec}	安全编码码率 R_c	$R_c:C_{sec}$ / %
0.01	0.838 4	0.762 6	90.96
0.02	0.717 1	0.615 8	85.87
0.03	0.611 2	0.493 8	80.79
0.04	0.515 4	0.387 6	75.20
0.05	0.427 2	0.292 0	68.35
0.06	0.345 1	0.205 4	59.52
0.07	0.268 2	0.125 5	46.80
0.08	0.195 6	0.051 7	26.43

由表 1 的实验结果可知，当量子比特误码率为 0.01 时，理论安全容量 $C_{sec}=0.838\ 4$，实际的安全编码码率 $R_c=0.762\ 6$，安全编码码率可达安全容量的比率为 $R_c:C_{sec}=90.96\%$; 当量子比特误码率为 0.08 时，$R_c:C_{sec}=26.43\%$. 当量子比特误码率由 0 变化到 0.08 时，基于极化码的单步量子密钥分发后处理算法可令 Bob 和 Eve 的译码误码率分别趋近于 0 和 0.5，满足可靠性条件(纠错后误码率 $\beta\leqslant 10^{-7}$) 和安全性条件(窃听信息量 $\delta_N\leqslant 10^{-14}$ bit). 在 Inter(R) Core(TM) i7-4790 CPU(主频 3.60 GHz) 上实现的软件译码器吞吐率可达 3 Mb/s，采用 CPU 并行处理后的译码吞吐率可达 86 Mb/s，而在不考虑密性放大步骤的前提下，利用 CPU 并行实现 LDPC 译码的吞吐率未达到 10 Mb/s [21]. 另外，实际 QKD 系统中用于量子比特传输阶段的硬件已稳定支持 1 Mb/s 的原始密钥生成速率 [22-23]，而本文后处理算法的处理速度大于实际 QKD 系统在量子比特传输阶段的处理速度，因此满足目前的实际 QKD 后处理在处理延时方面的需求. 目前在 100 km 级别通信距离的光纤上完成量子密钥分发系统的量子比特误码率通常小于 0.08 [20,24]，因此本文所提算法能被直接应用于城域网范围内的中短距离 QKD 系统，进一步降低了后处理延时.

根据不同量子比特误码率下的实际安全编码码率可达安全容量的比率变化曲线(图 4) 可知，当满足上述可靠性条件(纠后误码率 $\beta\leqslant 10^{-7}$) 和安全性条件(窃听信息量 $\delta_N\leqslant 10^{-14}$ bit) 时，随着量子比特误码率的增加，比率非线性下降; 当 $p>0.08$ 时，无法设计出满足上述可靠性和安全性的编码方案.

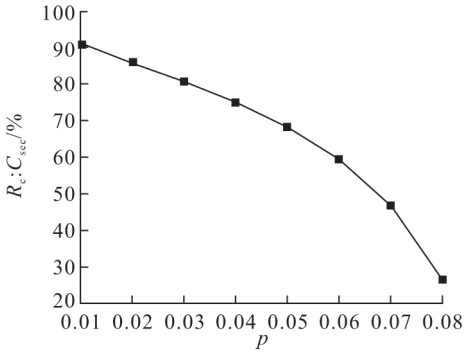

图 4　不同量子比特误码率下实际安全编码码率可达安全容量的比率

Figure 4　The ratio of practical secret coding rate to security capacity at different quantum bit error rates

这是因为随着量子比特误码率的增加，主信道 W 的虚拟比特子信道越来越差(即 $P_{e,m}(W_N^{(i)})$ 更大)，则对 Bob 的优化信道集 $G_N(W,\beta)$ 减小; 而窃听信道 W^* 的虚拟比特子信道越来越好(即 $C_w(W_N^{*(i)})$ 更大)，则对 Eve 的劣化信道集 $P_N(W^*,\delta_N)$ 减小，从而导致放置筛选密钥的集合 $A=P_N(W^*,\delta_N)\cap G_N(W,\beta)=\Phi$; 另外，极化码的有限码长效应也会导致虚拟比特子信道的译码误码率计算存在偏差，从而影响极化码码字的构建.

4　结论

QKD 技术基于量子力学特性有效解决了经典通信分发密钥的安全性问题，为保密通信系统提供理论上无条件安全的密钥. 但是，后处理中的误码纠错和密性放大所引入的高延时不利于高速 QKD 系统的发展与应用. 本文提出一种基于极化码的单步量子密钥后处理算法，可同时实现误码纠错和密性放大，降低了系统复杂度和处理延时. 实验仿真结果表明: 在量子比特误码率范围 [0,0.08] 内，本文提出的算法可以保证在提取密钥的同时满足可靠性条件(纠错后误码率 $\beta\leqslant 10^{-7}$) 和安全性条件(窃听信息量 $\delta_N\leqslant 10^{-14}$ bit)，实现了误码纠错和密性放大，降低了后处理延时，提高了量子密钥的提取效率.

参考文献:

[1] SCARANI V,BECHMANN-PASQUINUCCI H,CERF N J,et al. The security of practical quantum key distribution [J]. Reviews of Modern Physics,2009,81(3):1301-1345.

[2] 杜炎雄,程爱琴,郑翔,等. 量子网络研究进展 [J]. 华南师范大学学报(自然科学版),2016,48(1):16-22.
DU Y X,CHENG A Q,ZHENG X,et al. Research progress on quantum network [J]. Journal of South China Normal University (Natural Science Edition),2016,48(1):16-22.

[3] LI J,LI N,ZHANG Y,et al. Special issue on quantum communication: a survey on quantum cryptography [J]. Chinese Journal of Electronics,2018,27(2):223-228.

[4] KURTSIEFER C,ZARDA P,HALDER M,et al. Quantum cryptography: a step towards global key distribution [J]. Nature,2002,419:450-450.

[5] 郭邦红,郭建军,张程贤,等. 旋涡光学与轨道角动量高维编码量子通信研究 [J]. 华南师范大学学报(自然科学版),2015,47(4):1-7.
GUO B H,GUO J J,ZHANG C X,et al. Research on vortex optics and high dimensional orbital angular momentum coding and quantum communication [J]. Journal of South China Normal University (Natural Science Edition),2015,47(4):1-7.

[6] DIAMANTI E,LO H K,QI B,et al. Practical challenges in quantum key distribution [J]. NPJ Quantum Information,2016,2:16025/1-12.

[7] FUNG C H F,MA X,CHAU H F. Practical issues in quantum-key-distribution postprocessing [J]. Physical Review A,2010,81:15780-15787.

[8] BENNETT C H,BESSETTE F,BRASSARD G,et al. Experimental quantum cryptography [J]. Journal of Cryptology,1992,5(1):3-28.

[9] BRASSARD G,SALVAIL L. Secret-key reconciliation by public discussion [C] //Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Eurocrypt,1993:410-423.

[10] BUTTLER W T,LAMOREAUX S K,TORGERSON J R,et al. Fast,efficient error reconciliation for quantum cryptography [J]. Physical Review A,2003,67(5):125-128.

[11] ELKOUSS D,LEVERRIER A,ALLEAUME R,et al. Efficient reconciliation protocol for discrete-variable quantum key distribution [C] //IEEE International Symposium on Information Theory. Souel: IEEE,2009:1879-1883.

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

[13] BENNETT C H,BRASSARD G,CRÉPEAU C,et al. Generalized privacy amplification [J]. IEEE Transactions on Information Theory,1995,41(6):1915-1923.

[14] WYNER A D. The wire-tap channel [J]. Bell Labs Technical Journal,1975,54(8):1355-1387.

[15] AHDAVIFAR H,VARDY A. Achieving the secrecy capacity of wiretap channels using polar codes [J]. IEEE Transactions on Information Theory,2011,57(10):6428-6443.

[16] GOTTESMAN D,LO H K,LÜTKENHAUS N,et al. Security of quantum key distribution with imperfect devices [J]. Quantum Information & Computation,2004,4(5):325-360.

[17] ARIKAN E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels [J]. IEEE Transactions on Information Theory,2008,55(7): 3051-3073.

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

[19] ARIKAN E. Systematic polar coding [J]. IEEE Communications Letters,2011,15(8):860-862.

[20] KORZH B,LIM C C W,HOULMANN R,et al. Provably secure and practical quantum key distribution over 307 km of optical fibre [J]. Nature Photonics,2014,9(3):163-168.

[21] DIXON A R,SATO H. High speed and adaptable error correction for megabit/s rate quantum key distribution [J]. Scientific Reports,2014,4:7275/1-6.

[22] GARCÍA-MARTÍNEZ M J,DENISENKO N,SOTO D,et al. High-speed free-space quantum key distribution system for urban daylight applications [J]. Applied Optics,2013,52(14):3311-3317.

[23] DIXON A R,YUAN Z L,DYNES J F,et al. Continuous operation of high bit rate quantum key distribution [J]. Applied Physics Letters,2010,96(16):161102/1-3.

[24] TAKEMOTO K,NAMBU Y,MIYAZAWA T,et al. Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors [J]. Scientific Reports,2015,5:14383/1-7.

【责任编辑:谭春林 责任校对:谭春林 英文审校:程杰】