文章编号：2095-2163(2020)12-0128-09 中图分类号：O431.2 文献标志码：A

连续变量量子密钥分发离散调制方案的安全性分析与比较

孙游东，邢永鑫，王天一
（贵州大学 大数据与信息工程学院，贵阳 550025）

摘 要：目前离散调制连续变量量子密钥分发(Continuous-Variable Quantum Key Distribution，CV-QKD)协议受到越来越多的关注。本文在基于相干态和后选择的离散调制协议基础上，根据调制方式的不同提出了圆形调制方案和方形调制方案，并在反向协调和集体攻击的情况下推导了协议的通用安全码率公式。数值仿真分析结果表明，在不同的信号态数量下，方形离散调制协议的性能普遍要优于圆形离散调制协议。而相比于其他协议，四态方形离散调制协议的性能是最优的。

关键词：连续变量；量子密钥分发；离散调制；集体攻击

Security analysis and performance comparison of continuous variable quantum key distribution protocols with discrete modulation

SUN Youdong, XING Yongxin, WANG Tianyi
(College of big data and information engineering, Guizhou University, Guiyang 550025, China)

【Abstract】 At present, the Discrete Modulation Continuous - Variable Quantum Key Distribution (CV - QKD) protocol has received more and more attention. Based on the use of coherent state and the discrete modulation protocol selected later, this paper divides it into circular modulation and square modulation through different modulation methods. In the case of reverse coordination and collective attack, the general security code rate formula of the protocol is derived. Numerical simulation analysis results show that the performance of the square discrete modulation protocol is generally better than that of the circular discrete modulation protocol under different modulation methods. Compared with other protocols, the performance of the four-state square discrete modulation protocol is the best, not only the longest transmission distance, but also the relatively highest security bit rate.

【Key words】 Continuous variable; Quantum key distribution; Discrete modulation; Collective attack

0 引 言

量子密钥分发(Quantum Key Distribution，QKD)是基于量子物理原理为两个合法通信方之间提供安全的通信技术。第一个量子密码通信协议由 C.H. Bennett 及 G.Brassard 于 1984 年提出，即 BB84 协议，它是以单光子作为信息的载体[1]。随着最近几十年的蓬勃发展，连续变量量子密钥分发(Continuous-Variable Quantum Key Distribution，CV-QKD)协议逐渐成为主流。这是因为相比离散变量量子密钥分发(Discrete-Variable Quantum Key Distribution，DV-QKD)协议来说，CV-QKD 协议可以完美结合当前经典通信设备进行工作，而在传输距离上也大大优于 DV-QKD 协议。而根据 Alice 发送的相干态的调制方法，CV-QKD 协议又可以分为两种类型，一种是高斯调制协议，另一种是离散调制协议。而目前，离散调制 CV-QKD 协议受到越来越多的关注。对于离散调制 CV-QKD 协议而言，最近有报道称，如果可以将量子信道验证为线性的，则可以实现更长的安全传输距离[2]。

本文主要研究了在 Ryo Namiki 和 Takuya Hirano 提出的基于不同离散调制的 CV-QKD 协议[3]。在假设窃听者 Eve 执行纠缠克隆攻击的前提下[4-5]，通过离散调制和集体攻击下四态协议的安全性分析方法[6]，从理论上讨论了不同离散调制协议的安全码率，并分别通过仿真比较了在不同调制方式下或者同种调制方式不同态协议之间的优劣。

1 离散调制 CV-QKD 协议

通过调制方式的不同，主要将离散调制 CV-QKD 协议分为圆形调制和方形调制。本文主要讨论了四态圆形 CV-QKD 协议(R4)、八态圆形离散协议(R8)和十二态协议(R12)；四态方形离散调制

基金项目：贵州省科技厅与贵州大学科技合作计划项目(黔科合 LH 字[2016]7431)。

作者简介：孙游东(1995-)，男，硕士研究生，主要研究方向：人工智能、量子通信；邢永鑫(1993-)，男，硕士研究生，主要研究方向：深度学习、目标检测；王天一(1989-)，男，博士，副教授，主要研究方向：量子通信、图像处理、计算机视觉。

通讯作者：王天一 Email：tywang@gzu.edu.cn

收稿日期：2020-09-10

CV-QKD 协议(S4)、八态方形离散调制 CV-QKD 协议(S8)和 N 态方形离散调制 CV-QKD 协议(SN)。

1.1　圆形离散调制 CV-QKD 协议

1.1.1　四态圆形离散调制 CV-QKD 协议(R4)

在相位空间上示意性地描述了 R4 的编码，如图 1 所示。

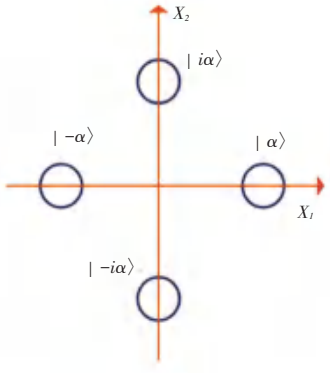

图 1　R4 的相空间示意图

Fig. 1　Phase space diagram of R4

由于光场的湮灭算符 $\hat{a}^{\dagger}$ 和产生算符 $\hat{a}$ 都不是厄米算符，为了便于对光场进行测量，两个正交分量算符 $\hat{x}_1$ 和 $\hat{x}_2$ 被定义为式(1)：

$$\hat{x}_1 = \frac{\hat{a} + \hat{a}^{\dagger}}{2}, \qquad \hat{x}_2 = \frac{\hat{a} - \hat{a}^{\dagger}}{2i}. \tag{1}$$

由公式(1)可以将相空间用平面直角坐标系表示，其中 x_1、x_2 分别表示为横纵坐标轴，也就是 $\hat{x}_1$ 和 $\hat{x}_2$ 和两个正交分量的取值，如图 1 所示。图 1 中的“1”和“0”代表与 Bob 基相关联的 Alice 的位编码。在发送端，Alice 发送相干态 $|S\rangle = |\alpha e^{i\varphi_A}\rangle$，其中，$\varphi_A = \{0, \pi/2, \pi, 3\pi/2\}$，$\alpha > 0$。Bob 通过随机选择其相位调制 $\varphi_B = \{0, \pi/2\}$ 去测量正交，式(2)：

$$\hat{x}(\varphi_B) = \hat{x}_1 \cos\varphi_B + \hat{x}_2 \sin\varphi_B, \tag{2}$$

经过传输后，Bob 通知 Alice 其相移为 φ_B。如果 $|\varphi_A - \varphi_B| = \{0, \pi\}$，则称组合 (φ_A, φ_B) 为正确的基选择。对于正确的基选择情况，信号可以通过表 1 的方式将位信息从 Alice 传输到 Bob。Alice 根据 (φ_A, φ_B) 的组合对其比特进行编码。Bob 根据其结果 x 对比特值进行解码：如果 $x \geqslant 0$，则其比特值为“1”，否则其比特值为“0”。并且从表 1 中很容易得出 R4 的协议效率为：$p_e = \frac{1}{2}$。

1.1.2　八态圆形离散调制 CV-QKD 协议(R8)

R8 的编码可以在图 2 中的相空间上进行示意性描述。

表 1　R4 的 Alice 的位编码

Tab. 1　Alice's bit ending of the R4

φ_A	0	0	$\pi/2$	$\pi/2$	π	π	$3\pi/2$	$3\pi/2$
φ_B	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
$\langle x \rangle$	α	0	0	α	$-\alpha$	0	0	$-\alpha$
A	1			1	0			0

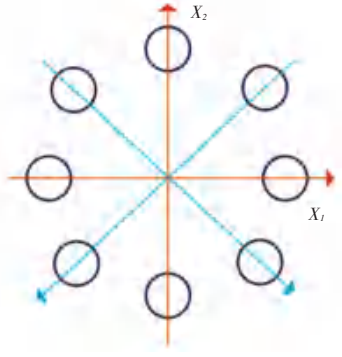

图 2　R8 的相空间示意图

Fig. 2　Phase space diagram of R8

在发送端，Alice 发送相干态 $|S\rangle = |\alpha e^{i\varphi_A}\rangle$，其中，$\varphi_A \in \{0, \pi/4, \pi/2, 3\pi/4, \pi, 5\pi/4, 3\pi/2, 7\pi/4\}$，$\alpha > 0$。Bob 选择其相位 $\varphi_B \in \{0, -\pi/4, -3\pi/4, \pi/2\}$ 测量正交 $\hat{x}(\varphi_B)$。且当 $(|\varphi_A - \varphi_B| \bmod \pi) = \pi/2$ 时，组合 (φ_A, φ_B) 称为正确的基组，反之，称为错误的基组。通过位编码规则得到其编码见表 2，其中，当测量值 φ_B 为 α 时，Alice 的编码为“1”；当测量值 φ_B 为 $-\alpha$ 时，Alice 的编码为“0”，其他情况则被丢弃。

1.1.3　十二态圆形离散调制 CV-QKD 协议(R12)

R12 的编码可以在图 3 中的相空间上进行示意性描述。

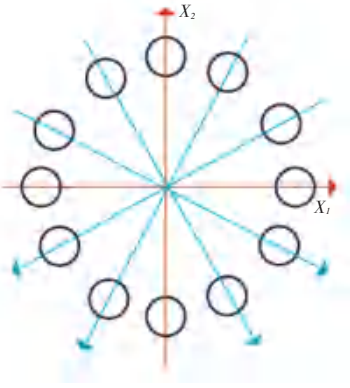

图 3　R12 的相空间示意图

Fig. 3　Phase space diagram of R12

在发送端，Alice 发送相干态 $|S\rangle = |\alpha e^{i\varphi_A}\rangle$，$\varphi_A \in \{0, \pi/6, \pi/3, \pi/2, 2\pi/3, 5\pi/6, \pi, 7\pi/6, 4\pi/3,$

$3\pi/3,5\pi/3,11\pi/3,2\pi\}$,$\alpha > 0$。Bob 选择其相位 $\varphi_B \in \{0, -\pi/6, -\pi/3, -2\pi/3, -5\pi/6, \pi/2\}$ 测量正交 $\hat{x}(\varphi_B)$。且当 $(|\varphi_A - \varphi_B| \bmod \pi) = \pi/2$ 时,组合 (φ_A, φ_B) 称为正确的基组,反之称为错误的基组。通过 $-\alpha$ 位编码规则得到其编码见表 3。

其中,当测量值 φ_B 为 α 时,Alice 的编码为“1”;当测量值 φ_B 为时,Alice 的编码为“0”,其他情况则被丢弃。

表 2 R8 的 Alice 的位编码

Tab. 2 Alice's bit ending of the R8

φ_A	0	0	0	0	$\pi/4$	$\pi/4$	$\pi/4$	$\pi/4$
φ_B	0	$-\pi/4$	$-3\pi/4$	$\pi/2$	0	$-\pi/4$	$-3\pi/4$	$\pi/2$
$\langle x\rangle$	α	$-\sqrt{2}\alpha/2$	$\sqrt{2}\alpha/2$	0	$\sqrt{2}\alpha/2$	0	$-\alpha$	$-\sqrt{2}\alpha/2$
A	1						0	
φ_A	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$	$3\pi/4$	$3\pi/4$	$3\pi/4$	$3\pi/4$
φ_B	0	$-\pi/4$	$-3\pi/4$	$\pi/2$	0	$-\pi/4$	$-3\pi/4$	$\pi/2$
$\langle x\rangle$	0	$-\sqrt{2}\alpha/2$	$-\sqrt{2}\alpha/2$	α	$-\sqrt{2}\alpha/2$	$-\alpha$	0	$\sqrt{2}\alpha/2$
A				1		0		
φ_A	π	π	π	π	$5\pi/4$	$5\pi/4$	$5\pi/4$	$5\pi/4$
φ_B	0	$-\pi/4$	$-3\pi/4$	$\pi/2$	0	$-\pi/4$	$-3\pi/4$	$\pi/2$
$\langle x\rangle$	$-\alpha$	$-\sqrt{2}\alpha/2$	$\sqrt{2}\alpha/2$	0	$-\sqrt{2}\alpha/2$	α	0	$-\sqrt{2}\alpha/2$
A	0					1		
φ_A	$3\pi/2$	$3\pi/2$	$3\pi/2$	$3\pi/2$	$7\pi/4$	$7\pi/4$	$7\pi/4$	$7\pi/4$
φ_B	0	$-\pi/4$	$-3\pi/4$	$\pi/2$	0	$-\pi/4$	$-3\pi/4$	$\pi/2$
$\langle x\rangle$	0	$\sqrt{2}\alpha/2$	$\sqrt{2}\alpha/2$	$-\alpha$	$\sqrt{2}\alpha/2$	0	α	$-\sqrt{2}\alpha/2$
A				0			1	

从表 2 能得到 R8 的协议效率:$p_e = \frac{1}{4}$。

表 3 R12 的 Alice 的位编码

Tab. 3 Alice's bit ending of the R12

φ_A	0	0	0	0	0	0	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$	$\pi/6$
φ_B	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$
$\langle x\rangle$	α	$\sqrt{3}\alpha/2$	$\alpha/2$	$-\alpha/2$	$-\sqrt{3}\alpha/2$	0	$\sqrt{3}\alpha/2$	$\alpha/2$	0	$-\sqrt{3}\alpha/2$	$-\alpha$	$\alpha/2$
A	1										0	
φ_A	$\pi/3$	$\pi/3$	$\pi/3$	$\pi/3$	$\pi/3$	$\pi/3$	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$	$\pi/2$
φ_B	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$
$\langle x\rangle$	$\alpha/2$	0	$-\alpha/2$	$-\alpha$	$-\sqrt{3}\alpha/2$	$\sqrt{3}\alpha/2$	0	$-\alpha/2$	$-\sqrt{3}\alpha/2$	$-\alpha/2$	$-\sqrt{3}\alpha/2$	α
A				0								1
φ_A	$2\pi/3$	$2\pi/3$	$2\pi/3$	$2\pi/3$	$2\pi/3$	$2\pi/3$	$5\pi/6$	$5\pi/6$	$5\pi/6$	$5\pi/6$	$5\pi/6$	$5\pi/6$
φ_B	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$
$\langle x\rangle$	$-\alpha/2$	$-\sqrt{3}\alpha/2$	$-\alpha$	$-\alpha/2$	$-\sqrt{3}\alpha/2$	0	$-\sqrt{3}\alpha/2$	$-\alpha$	$-\sqrt{3}\alpha/2$	0	$\alpha/2$	$\alpha/2$
A			0					0				
φ_A	π	π	π	π	π	π	$7\pi/6$	$7\pi/6$	$7\pi/6$	$7\pi/6$	$7\pi/6$	$7\pi/6$
φ_B	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$
$\langle x\rangle$	$-\alpha$	$-\sqrt{3}\alpha/2$	$-\alpha/2$	$\alpha/2$	$\sqrt{3}\alpha/2$	0	$-\sqrt{3}\alpha/2$	$-\alpha/2$	0	$\sqrt{3}\alpha/2$	α	$\alpha/2$
A	0										1	
φ_A	$4\pi/3$	$4\pi/3$	$4\pi/3$	$4\pi/3$	$4\pi/3$	$4\pi/3$	$3\pi/2$	$3\pi/2$	$3\pi/2$	$3\pi/2$	$3\pi/2$	$3\pi/2$
φ_B	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$
$\langle x\rangle$	$-\alpha/2$	0	$\alpha/2$	α	$\sqrt{3}\alpha/2$	$-\sqrt{3}\alpha/2$	0	$\alpha/2$	$\sqrt{3}\alpha/2$	$\sqrt{3}\alpha/2$	$\alpha/2$	$-\alpha$
A				1								0
φ_A	$5\pi/3$	$5\pi/3$	$5\pi/3$	$5\pi/3$	$5\pi/3$	$5\pi/3$	$11\pi/6$	$11\pi/6$	$11\pi/6$	$11\pi/6$	$11\pi/6$	$11\pi/6$
φ_B	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$	0	$-\pi/6$	$-\pi/3$	$-2\pi/3$	$-5\pi/6$	$\pi/2$
$\langle x\rangle$	$\alpha/2$	$\sqrt{3}\alpha/2$	α	$\alpha/2$	0	$-\sqrt{3}\alpha/2$	$\sqrt{3}\alpha/2$	α	$\sqrt{3}\alpha/2$	0	$-\alpha/2$	$-\alpha/2$
A			1					1				

从表 3 得到 R12 的协议效率：$p_e = \frac{1}{6}$。

由上述对于圆形离散调制 CV-QKD 协议的讨论可以看出：随着其态数 N 的增加，其编码的复杂度越来越高，而其协议的效率反而越来越低。对于 R4，其编码的情况数为 8，协议效率为 1/2；对于 R8，其编码的情况数为 32，协议效率为 1/4；对于 R12，其编码的情况数为 72，协议效率为 1/6。通过简单的推论容易得到：对于 RN，其编码的情况数为 $N^2/2$，协议效率为 $2/N$。所以对于圆形离散调制的 CV-QKD 协议而言，在其状态数 N 不断增加时，其编码的复杂度是随着其状态数 N 呈指数级上升，协议效率随着 N 呈反向减小的趋势。所以这里也只讨论了 $N = 12$ 时的情况。

1.2　方形离散调制 CV-QKD 协议

1.2.1　四态方形离散调制 CV-QKD 协议(S4)

S4 的编码可以在图 4 中的相空间上进行示意性描述。

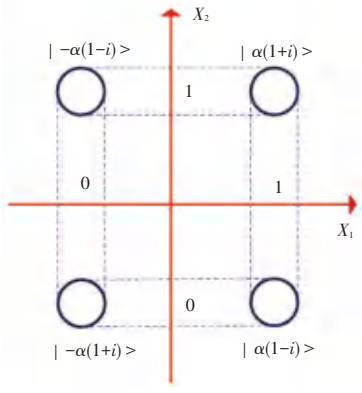

图 4　S4 的相空间示意图

Fig. 4　Phase space diagram of S4

Alice 发送相干态 $|S\rangle = |\alpha'' e^{i\varphi_A}\rangle$，其中，$\varphi_A = \{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$，$\alpha' = \sqrt{2}\alpha$。Bob 测量 $\hat{x}(\varphi_B)$，其中，$\varphi_B = \{0, \pi/2\}$。使用位编码规则，得到表 4。

表 4　S4 的 Alice 的位编码

Tab. 4　Alice´s bit ending of the S4

φ_A	$\pi/4$	$\pi/4$	$3\pi/4$	$3\pi/4$	$5\pi/4$	$5\pi/4$	$7\pi/4$	$7\pi/4$
φ_B	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
$\langle x\rangle$	α	α	$-\alpha$	α	$-\alpha$	$-\alpha$	α	$-\alpha$
A	1	1	0	1	0	0	1	0

从表 4 得到 S4 的协议效率：$p_e = 1$。

1.2.2　八态方形离散调制 CV-QKD 协议(S8)

S8 的编码可以在图 5 所示的相空间上进行示意性描述。

Alice 发送相干态 $|S\rangle = \{|\alpha e^{im/2\pi}\rangle, |\alpha' e^{i(2m'+1)/4\pi}\rangle\}$，其中，$\varphi_A = m\pi/2, m = \{0,1,2,3\}$，对于 $\alpha' = \sqrt{2}\alpha, \varphi_A = (2m'+1)\pi/4, m = \{0,1,2,3\}$。Bob 选择他的相位 $\varphi_B = \{0, \pi/2\}$ 进行测量。使用位编码规则，得到表 5。

从表 5 能得到八态协议的协议效率：$p_e = \frac{3}{4}$。

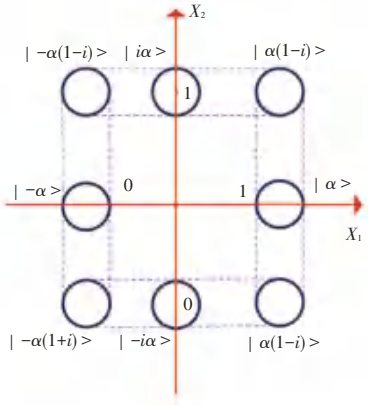

图 5　S8 协议的相空间示意图

Fig. 5　Phase space diagram of eight-state protocol

表 5　S8 的 Alice 的位编码

Tab. 5　Alice´s bit ending of the S8

φ_A	0	0	$\pi/4$	$\pi/4$	$\pi/2$	$\pi/2$	$3\pi/4$	$3\pi/4$	π	π	$5\pi/4$	$5\pi/4$	$3\pi/2$	$3\pi/2$	$7\pi/4$	$7\pi/4$
φ_B	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$	0	$\pi/2$
$\langle x\rangle$	α	0	α	α	0	α	$-\alpha$	α	α	$-\alpha$	0	$-\alpha$	$-\alpha$	0	α	$-\alpha$
A	1		1	1		1	0	1	0	0		0	0		1	0

1.2.3 N 态方形离散调制 CV-QKD 协议(SN)

SN 的编码在图 6 所示的相位空间上进行示意性描述。

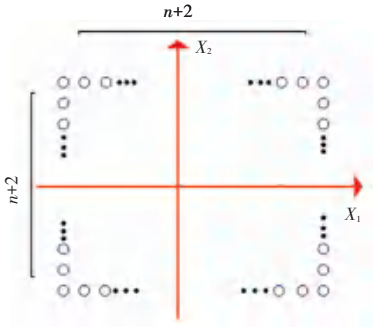

图 6 SN 的相空间示意图

Fig. 6 Phase space diagram of SN

Alice 随机选择了 $N = 4n + 4$ 态之一发送,其中,Alice 准备的相干态 $|S\rangle = \{|\alpha(\pm 1 + i(\frac{2k}{n+1} - 1))\rangle, |\alpha(\pm i + (\frac{2m}{n+1} - 1))\rangle\}, k = 0,1,2,\cdots,n+1, m = 1,2,\cdots,n$。Bob 选择正交 $\hat{x}_1$ 和 $\hat{x}_2$ 之一进行测量。在 Bob 测量 $\hat{x}_1$ 时,Alice 对 $|\alpha(1 + i(\frac{2k}{n+1} - 1))\rangle$ 编码为“1”;对 $|\alpha(-1 + i(\frac{2k}{n+1} - 1))\rangle$ 编码为“0”。在 Bob 测量 $\hat{x}_2$ 时,Alice 对 $|\alpha(i + (\frac{2k}{n+1} - 1))\rangle$ 编码为“1”;对 $|\alpha(-i + (\frac{2k}{n+1} - 1))\rangle$ 编码为“0”。其它情况将被丢弃。在此协议中,Alice 的状态准备被认为是 n + 2 状态等概率混合。可以看到 $n = 0$ 时对应于方形四态协议,$n = 1$ 时对应于方形八态协议。

其协议效率为式(3):

$$p_e = \frac{2+n}{2+2n}. \tag{3}$$

基于上述分别给出的离散调制协议,通过离散调制和集体攻击下的安全性分析方法,从理论上分别给出了圆形离散调制和方形离散调制下的协议的通用安全码率公式。在理论分析中,假设 Bob 还揭示了其结果 m 的绝对值 $|m|$。Bob 通过分别为所选测量值 m 的负值分配 0、为正值分配 1 来制作位串。

由于假设了量子信道不是理想的,但其特征由过量噪声 ξ 和传输率 η 描述。可以得出以 S 为条件的 Bob 的测量值 m 的概率密度为式(4)[7]:

$$P(m|S) = \sqrt{\frac{2}{\pi(1+\xi)}} e^{-2\frac{(m-\sqrt{\eta}S)^2}{1+\xi}}, \tag{4}$$

其中,真空噪声方差为 1/4。

概率 ε 被定义为 Alice 发送 0 或 1,而 Bob 收到 1 或 0 的概率,简称为误码率(BER)式(5):

$$\varepsilon = [1 + e^{8\frac{\sqrt{\eta}}{1+\xi}|m|\alpha}]^{-1}, \tag{5}$$

使用 Shannon 公式并可以将 Alice 和 Bob 之间的互信息 I_{AB} 表示为式(6):

$$I_{AB} = 1 - h(\varepsilon), \tag{6}$$

其中,$h(\varepsilon) = -\varepsilon\log_2\varepsilon - (1-\varepsilon)\log_2(1-\varepsilon)$ 是二元熵。

2 集体攻击下的安全码率

2.1 平均调制方差的计算

在假设过量噪声 ξ 和传输率 η 相同的情形下,Alice 和 Bob 之间的互信息 I_{AB} 主要取决于误码率 ε。本文舍弃了 Bob 端测量不为 $\pm\alpha$ 的测量值,则测量值 $m = \pm\alpha$。所以互信息 I_{AB} 的计算值取决于 Alice 端的平均调制方差。分别讨论在圆形离散调制和方形离散调制下的平均调制方差。

2.1.1 圆形离散调制协议

在圆形离散调制时,由于 Alice 准备的量子态均匀的分布在以原点为圆心,以 α 为半径的圆上。所以很容易得到在圆形离散调制时其平均调制方差为式(7):

$$\bar{\alpha}_R = \alpha. \tag{7}$$

2.1.2 方形离散调制协议

在方形离散调制方式中,Alice 的状态准备被认为是 $n+2$ 状态等概率混合。可以看到 $n=0$ 时对应于 S4 协议,$n=1$ 时对应于 S8 协议。对于 S4 协议和 S8 协议可以很容易计算出其平均调制方差分别为式(8)和式(9):

$$\alpha_{S4} = \sqrt{2}\alpha, \tag{8}$$

$$\alpha_{S8} = \frac{1}{2}\alpha + \frac{1}{2}\sqrt{2}\alpha, \tag{9}$$

而 SN 的平均调制方差并不能直接给出,对其讨论如下:

如图 6 所示,对于方形调制的 N 态协议来说,其每边有 $n+2$ 个态,由于其对称性,只需要取其一半的状态数 $\frac{n}{2}+1$ 来讨论即可。当 n 为奇数或者偶数时为分别不同的两种情况。

(1)当 n 为偶数时,有式(10):

$$\alpha_{SN} = \frac{2\alpha}{n+1}\left(\frac{\sqrt{2}}{2} + \frac{R_1 + R_3 + R_5 + \cdots + R_{n-2}}{n+1}\right), \tag{10}$$

其中,$R_i = \sqrt{(n+1)^2 + i^2}, i = 1,3,5,\cdots,n-2$。

（2）当 n 为奇数时，有式（11）：

$$\alpha_{SN}=\frac{2\alpha}{n+1}\left[2+\frac{\sqrt{2}}{2}+\frac{D_1+D_2+D_3+\cdots+D_{\frac{n-1}{2}}}{\frac{1}{2}(n+1)}\right], \tag{11}$$

其中，$D_i=\sqrt{(n+1)^2+i^2}$，$i=1,2,3,\cdots\dfrac{n-1}{2}$。

2.2　克隆纠缠攻击

如图 7 所示，假设量子信道是高斯型的，在协议的每一次运行中，Eve 都会准备一份 CV EPR 状态，并在她的一对 EPR 对和从 Alice 发送给 Bob 的对之间进行干扰。Eve 将自己的状态保存在量子记忆中。Eve 对自己保持的状态进行集体攻击，并获得有关 Alice 和 Bob 共享的比特序列的信息。本文将考虑针对集体攻击协议的密钥率。当量子信道是对称的并且是高斯的时，所有集体攻击都被认为是酉等价的[8]。

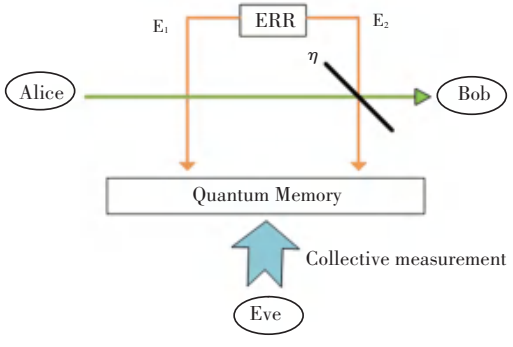

图 7　纠缠克隆攻击的示意图

Fig. 7　Schematic diagram of entangled clone attack

下面计算对抗纠缠克隆攻击的安全密钥率。

对于纠缠克隆攻击来说，Eve 准备了模式 E_1 和 E_2 的一个 EPR 态如式（12）所示：

$$|EPR\rangle=\sqrt{\frac{\pi}{2}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}dx_1dx_2e^{-Vx_1^2-x_2^2/V}\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\frac{x_1-x_2}{\sqrt{2}}\right\rangle_{E_2}, \tag{12}$$

其中，$|E_i\rangle$ 表示特征值为 x 的模式 E_i 的正交算子 x 的本征态。$V\geqslant 1$ 且满足式（13）：

$$\frac{1}{2}\left(V+\frac{1}{V}\right)=\frac{1-\eta+\xi}{1-\eta}, \tag{13}$$

相干态 $|S\rangle$ 表示为式（14）：

$$|S\rangle=\left(\frac{2}{\pi}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}dxe^{-(x-s)^2}|x\rangle, \tag{14}$$

由于通过透射率为 η 分束器变换有式（15）：

$$|x\rangle_A|x_2\rangle_{E_2}\rightarrow|\sqrt{\eta}x-\sqrt{1-\eta}x_2\rangle_A|\sqrt{1-\eta}x+\sqrt{\eta}x_2\rangle_{E2}, \tag{15}$$

将 $m=\sqrt{\eta}x-\sqrt{1-\eta}(x_1-x_2)/\sqrt{2}$ 代入等式（14）与等式（12）中可以得到式（16）：

$$|x\rangle_A\left|\frac{x_1-x_2}{\sqrt{2}}\right\rangle_{E_2}\rightarrow|m\rangle_A\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}, \tag{16}$$

由于模式 E_1 不需要通过分束器变换，所以最后整合公式（12）、（14）、（16）得出了最终的整合干扰模式为式（17）：

$$|\varphi(S,\mathrm{m})\rangle=\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}dx_1dx_2\varphi(\mathrm{S},\mathrm{m})\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E_1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2}, \tag{17}$$

这里：

$$\varphi(S,m)=\mathrm{e}^{-\left[\sqrt{\frac{1-\eta}{\eta}}(x_1-x_2)+\frac{m}{\sqrt{\eta}}-S\right]^2-Vx_1^2-x_2^2/V}, \tag{18}$$

注意，$|\varphi(S,m)\rangle$ 具有以下归一性，式（19）：

$$\langle\varphi(S,m)|\varphi(S,m)\rangle=P(m/S), \tag{19}$$

为了后面计算方便本文引入式（20）：

$$|e_{ij}\rangle=N|\varphi((-1)^i|S|,\varphi(-1)^j|m|)\rangle, \tag{20}$$

这里 $i,j=0,1$ 并且 N 是一个依赖于 i,j 的归一化因子，其具体表达式分别如式（21）：

$$\begin{aligned}
|e_{00}\rangle&=N\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}dx_1dx_2e^{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{|m|}{\sqrt{\eta}}-|s|\right]^2-Vx_1^2-x_2^2/V}|m\rangle_A\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2},\\
|e_{01}\rangle&=N\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}dx_1dx_2e^{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{-|m|}{\sqrt{\eta}}-|s|\right]^2-Vx_1^2-x_2^2/V}|m\rangle_A\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2},\\
|e_{10}\rangle&=N\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}dx_1dx_2e^{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{|m|}{\sqrt{\eta}}+|s|\right]^2-Vx_1^2-x_2^2/V}|m\rangle_A\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2},\\
|e_{11}\rangle&=N\left(\frac{8}{\pi^3\eta^2}\right)^{\frac{1}{4}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}dx_1dx_2e^{-\left[\sqrt{\frac{1-\eta}{2\eta}}(x_1-x_2)+\frac{-|m|}{\sqrt{\eta}}+|s|\right]^2-Vx_1^2-x_2^2/V}|m\rangle_A\left|\frac{x_1+x_2}{\sqrt{2}}\right\rangle_{E1}\left|\sqrt{\frac{1-\eta}{\eta}}m+\frac{x_1-x_2}{\sqrt{2\eta}}\right\rangle_{E_2},
\end{aligned} \tag{21}$$

假设 Bob 对模式 A 执行 x 基测量,并找到结果 m。在这种情况下,对于 *RR*,*Eve* 攻击 *Bob* 的目的是估计他的比特。则有式(22)和式(23):

$$\rho_B^0 = (1-\varepsilon)\,|\,e_{00}\rangle\langle e_{00}\,|\,+\varepsilon\,|\,e_{10}\rangle\langle e_{10}\,|\,, \quad (22)$$

$$\rho_B^1 = (1-\varepsilon)\,|\,e_{11}\rangle\langle e_{11}\,|\,+\varepsilon\,|\,e_{01}\rangle\langle e_{01}\,|\,, \quad (23)$$

Eve 的可访问信息χ受 Holevo 界的影响,其通式如式(24)[9]:

$$\chi = S(\rho) - S(\rho_B^0)/2 - S(\rho_B^1)/2, \quad (24)$$

这里,$\rho = (\rho_B^0 + \rho_B^1)/2$,且 $S(\rho) = -Tr(\rho\log_2\rho) = -\sum_k n_k \log_2 n_k$ 表示冯·诺依曼熵。其中,n_k 表示密度矩阵 ρ 所对应的特征值。

根据冯·诺依曼熵的定义可知,要想求出(24)中的χ,我们将算出等式(24)中出现的所有密度矩阵的特征值。根据 Takuya Hirano 等人的证明,通过 Gramian 矩阵可以轻松的找到其特征值:

对于 ρ_B^i,其 Gramian 矩阵表示为式(25):

$$\boldsymbol{G} = \begin{bmatrix} 1-\varepsilon & \delta t \\ \delta t & \varepsilon \end{bmatrix}. \quad (25)$$

其中:

$$t = \langle e_{00}\,|\,e_{10}\rangle = \langle e_{11}\,|\,e_{01}\rangle = e^{-2\frac{1+\xi-\eta}{1+\xi}\alpha^2}, \quad (26)$$

$$\delta = \sqrt{\varepsilon(1-\varepsilon)}, \quad (27)$$

所以其特征值为式(28):

$$\frac{1}{2}\left[1 \pm \sqrt{1-4\delta^2(1-t)^2}\right], \quad (28)$$

且因为其与 m 无关,所以有式(29):

$$S(\rho_B^0) = S(\rho_B^1), \quad (29)$$

对于 ρ,有式(30):

$$\boldsymbol{G} = \begin{bmatrix} 1-\varepsilon & \delta s & \delta t & (1-\varepsilon)stu \\ \delta s & \varepsilon & \varepsilon st/u & \delta t \\ \delta t & \varepsilon st/u & \varepsilon & \delta s \\ (1-\varepsilon)stu & \delta t & \delta s & 1-\varepsilon \end{bmatrix} \quad (30)$$

其中:

$$s = \langle e_{00}\,|\,e_{01}\rangle = \langle e_{11}\,|\,e_{10}\rangle = e^{-2\frac{\xi(2+\xi)}{1+\xi}m^2}, \quad (31)$$

$$u = e^{4\frac{\xi\sqrt{\eta}}{1+\xi}\alpha\,|\,m\,|}, \quad (32)$$

则求出特征值为:

$$\frac{1}{4u}\left(v_+ \pm \sqrt{v_+ - w_+}\right), \quad \frac{1}{4u}\left(v_- \pm \sqrt{v_- + w_-}\right),$$

其中:

$$v_\pm = u \pm st\left[\varepsilon + (1-\varepsilon)u^2\right],$$

$$w_\pm = 4\delta^2 u\left[st\,(1-u)^2 \pm (1-s^2)\,(1-t^2)\,u\right].$$

2.3 协议的安全码率

根据互信息 I_{AB} 和 Eve 的可访问信息χ以及各个协议的效率 p_e,可以直接给出一般态协议的通用安全码率公式(33):

$$K = p_e(I_{AB} - \chi), \quad (33)$$

但由于在不同的离散调制方式下的互信息 I_{AB} 以及协议效率 p_e 都不一样,所以下面本文分别给出了在圆形离散调制和方形离散调制下的协议的安全码率公式。

2.3.1 圆形离散调制协议的安全码率

在态数为 $N = 4n + 4$ 的圆形离散调制协议中,其协议的效率为 $2/N$,为了与方形离散调制协议对应起来将圆形离散调制协议的协议效率表示为式(34):

$$P_e^R = \frac{1}{2n+2}, \quad (34)$$

同时由于在圆形离散调制时,可以算出圆形离散调制下 Alice 和 Bob 之间的互信息,为了与方形离散调制下的互信息进行区别,表示为 I_{AB}^R。则圆形离散调制协议的安全码率表示为式(35):

$$K_R = \frac{1}{2n+2}(I_{AB}^R - \chi), \quad (35)$$

2.3.2 方形离散调制协议的安全码率

在态数为 $N = 4n + 4$ 的方形离散调制协议中,其协议的效率为 $\frac{n+2}{2n+2}$,为了与圆形离散调制协议对应起来将方形离散调制协议的协议效率表示为式(36):

$$P_e^S = \frac{n+2}{2n+2}, \quad (36)$$

由于在方形离散调制时,可以算出方形离散调制下 Alice 和 Bob 之间的互信息,为了与圆形离散调制下的互信息进行区别,表示为 I_{AB}^S。则方形离散调制协议的安全码率表示为式(37):

$$K_S = \frac{n+2}{2n+2}(I_{AB}^S - \chi). \quad (37)$$

3 仿真结果及其比较

基于上述给出的安全码率公式,对各个协议进行了仿真分析,并对各个协议的性能进行了比较。其中各种参数设置如下:信道透射率 $\eta = 10^{-\tau L/10}$,L 代表 Alice 与 Bob 之间的通信距离,光纤损耗 τ = 0.2 dB/km,过量噪声 $\xi = 0.01$,调制方差 $\alpha = 0.5$。

不同调制方式下的安全码率仿真比较图如图 8 所示。可以看出对于圆形离散调制方式而言,在小

于 30 km 的短距离内，R4 的安全码率高于 R8 和 R12，且随着传输距离的增加安全码率越来越接近，并在接近其极限距离处完全汇合。其原因在于在圆形离散调制下，态数 N 的变化对 Alice 和 Bob 之间的互信息 I_{AB}^{R} 并没有多大影响，而对其协议效率的影响比较大。而对于方形离散调制方式而言，S4 的整体性能更加优于 S8 和 S12，并且传输距离达到了最远的 107km。对于 S8 和 S12 有相交的部分而言，正是由于方形离散调制方式在 n 取到奇数和偶数时其平均调制方差的计算不一样，从而导致 Alice 和 Bob 之间的互信息 I_{AB}^{S} 不一致造成的。最后对于不同离散调制方式的比较而言，得出方形离散调制的协议性能要优于圆形离散调制的结论，而其中以 S4 的协议性能为最优。这是由于方形离散调制方案无论是在编码的效率还是协议效率都要明显高于圆形离散调制方案。

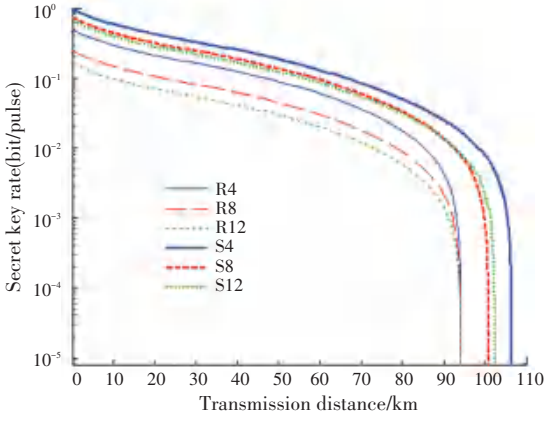

图 8　不同调制方差下的安全码率比较图

Fig. 8　Comparison chart of security code rate under different modulation variances

在图 8 中已经明确了无论是圆形离散调制还是方形离散调制方式下，都是态数 N 最小时所对应协议性能为最优。所以本文针对 R4 和 S4 分别绘制了在不同过量噪声下的安全码率曲线图，如图 9 所示，其中左边为 R4、右边为 S4。

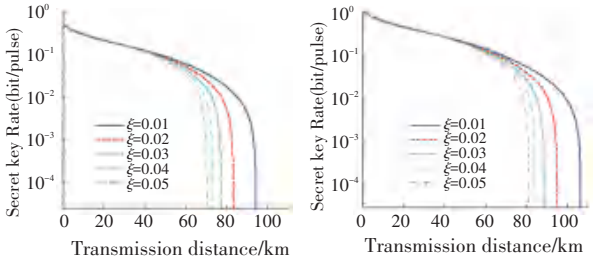

图 9　R4 和 S4 在不同过量噪声下的安全码率曲线图

Fig. 9　Curves of safe bit rate of R4 and S4 under different excess noise

从图 9 中可以清晰的看到，不管是在哪种调制方式下，在过量噪声取到 0.01 时协议的性能最优，并都会随着过量噪声的增加而减弱。而随着过量噪声均匀增加的同时这种衰弱是逐渐递减的。而在小于 40 km 的短距离内，过量噪声的变化对协议的性能几乎没有影响。这种影响只体现在长距离的情况下，并随着传输距离的增加而增大。而从图 9 中很容易看出 S4 的抗过量噪声性能要优于 R4。

R4 和 S4 在不同调制方差下的安全码率曲线图，如图 10 所示。其中左边为 R4、右边为 S4。可以明显的看到不管是在哪种调制方式下，协议的性能都随着调制方差的增大而减小。这是由于离散调制的调制方差越来越小时，其概率分布更加接近高斯分布，从而使得其安全码率更高。在调制方差相同时，可以明显看到 S4 的协议性能要优于 R4。

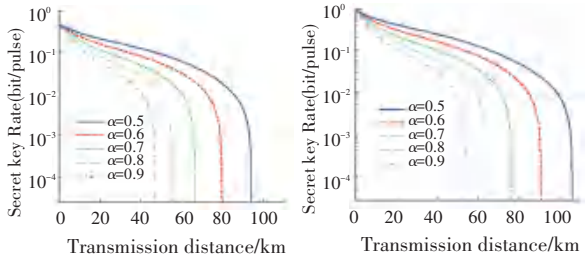

图 10　R4 和 S4 在不同调制方差下的安全码率曲线图

Fig. 10　R4 and S4 safe code rate curve diagram under different modulation variances

通过上述对不同离散调制方式下协议性能的仿真比较可以看出：方形离散调制的性能要优于圆形离散调制。相比于圆形离散调制而言，方形离散调制的编码更简单，理论上也可以表示出态数为 N 时的协议 SN。而在方形离散调制中，4 态的方形离散调制 S4 的性能是最好的。

5　结束语

本文针对离散调制 CV-QKD 协议，提出了方形调制和圆形调制两种调制方案，并分析了两种方案的安全性。数值仿真结果表明，在信号态数量相同时，方形调制协议的性能要优于圆形调制协议。在两种调制方案中，信号态数量的增加都不会带来系统性能的提升，其原因在于随着信号态数量的增加会导致 Alice 与 Bob 之间的误码率增大，从而导致其互信息减小。在未来的工作中，将考虑实际实验环境下的非理想因素对离散调制协议的影响。

参考文献

[1] BENNETT C H. Quantum cryptography: Public key distribution and coin tossing[C]// Proc of IEEE International Conference on Computers. Institute of Electrical and Electronics Engineers, 1984:

175-179.
[2] Anthony Leverrier, Philippe Grangier. Erratum: Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation [J]. Physical Review Letters, 2011, 106(106):259902.
[3] NAMIKI R, HIRANO T. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection[J]. OALib Journal, 2006,74: 032302.
[4] Grosshans F and Grangier P 2003 Quant. Info. Comp. 3 535.
[5] HEID M , LÜtkenhaus, Norbert. Security of coherent state quantum cryptography in the presence of Gaussian noise[J]. Phys. rev.a, 2009, 76(5):1188-1190.
[6] HIRANO T, ICHIKAWA T, MATSUBARA T, et al. Implementation of continuous-variable quantum key distribution with discrete modulation[J]. Quantum Science and Technology, 2017, 2(2):024010.
[7] SYMUL T, ALTO D J, ASSAD S M, et al. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise[J]. Physical Review A,2007, 76: 030303.
[8] HEID M, LÜtkenhaus, Norbert. Security of coherent state quantum cryptography in the presence of Gaussian noise [J]. Physical Review A, 2009, 76(5):1188-1190.
[9] HOLEVO A S. Bounds for the quantity of information transmittable by a quantum communications channel [J]. Probl. Inf. Transm.,1973, 9: 177-183.

(上接第 127 页)

缘,三维交变 hdl - 64 激光雷达在车顶用于探测和跟踪周围的行人。安装在挡风玻璃中央的视觉传感器(摄像头)用于检测交通信号。

将由车获取得精确的数字地图导入类人驾驶模拟器,提高司机的提前预判能力,通过学习人类驾驶员解决复杂和潜在危险情况的策略,制定决策算法[3]。

模拟器允许实时收集多个人工输入,并放置在相同的虚拟环境中。这一方法能够研究人类的决策过程,特别是在选择在行人通过之前或之后行驶时。通用属性是指在同一软件中同时运行人工输入、录音和自动车辆的能力。

本文采用了子弹物理引擎的方法,以便在一个服务器上模拟运行,该服务器为架构的每个客户端集中物理计算。车辆通过设置 3 个参数来控制:方向盘角度、油门和刹车。物理发动机根据地面摩擦滑移和车辆模计算下一个世界状态[4]。后者包括 4 个独立的车轮与他们的悬架系统和一个身体质量在顶部,为动力系统重现了俯仰和弹跳自由度,为人类驾驶员提供了油门变化的真实视觉反馈。每个悬架系统包括刚度、压缩、阻尼和最大行程。

为了保持轨迹和决策的真实性,以下两种控制被应用于辅助驾驶员:

(1)自动横向控制。指示驾驶员沿着 3D 视图中高亮显示的路线行驶。由于行人的互动只有通过或让路,因此没有理由逃离预先设定的路线走廊。在这种人工环境中,转向任务既不需要,也不容易,自动横向控制有助于按照预定义的路径保持车道,人类司机只需要设定车辆的速度。

(2)半自动纵向控制。根据上述情况,定义驾驶行为剩下的唯一关键任务就是速度层面的设定。辅助纵向控制就像巡航控制系统,用户设定一个目标速度,纵向控制系统调整制动,以平稳、自然的方式达到目标速度。

为了实现客观的比较,一个自动化车辆与描述的算法是在相同的设置测试,被用来检索速度层面。行人有碰撞实验用假人代替。测试结果见表 1。

表 1 安全实验测试

Tab. 1 Safety experimental test

车辆速度(km/h)	安全评估(个案数)	
	安全	危险碰撞
10	23/25	2/25
20	23/25	2/25
30	22/25	3/25
40	22/25	3/25
50	21/25	4/25

不同速度下均实验 25 次,其中安全通过约占 88%。

4 结束语

本文算法能够安全通过交叉路口。驾驶策略是合理的,似乎复制了类似人类的行为,且有提前预估威胁风险的能力。在某种程度上,这种特性可以在目前的模拟环境中评估。在对算法的客观验证中,用了不同速度下的车辆进行实验,在速度层面给出结果,由数据结果清晰可知,本文的算法具有较高的安全性,对自动驾驶安全通过十字路口具有指导意义。

参考文献

[1] 戴荣健,丁川,鹿应荣,等. 自动驾驶环境下车辆轨迹及交通信号协同控制[J]. 汽车安全与节能学报, 2019, 10(4): 531-539.
[2] 陈无畏,李进,王檀彬,等. 视觉导航智能车辆的路径跟踪预瞄控制[J]. 机械工程学报,2008,44(10):277-282.
[3] 耿新力. 城区不确定环境下无人驾驶车辆行为决策方法研究[D].合肥:中国科学技术大学, 2017.
[4] 刘凯,龚建伟,陈舒平,等. 高速无人驾驶车辆最优运动规划与控制的动力学建模分析 [J]. 机械工程学报,2018,54(14): 141-151.