文章编号：2095-2163(2023)06-0154-09 中图分类号：TP309 文献标志码：A

BB84 与 B92 量子通信加密协议的仿真分析

吴佳怡[1]，周芃玮[1]，赵 男[2]，周 伟[1]，谭振江[1]
（1 吉林师范大学 数学与计算机学院，吉林 四平 136000；2 四平市第二十五中学，吉林 四平 136001）

摘 要：本文针对量子 BB84 协议和 B92 协议的仿真实验开展研究，采用 qiskit（pycharm 软件数据包）设计了一种仿真实验模型。通过引入误码率、纠错率、协议可靠率指标，仿真分析了两种协议在有无窃听者存在且传输环境有噪声情况下，协议的安全性及传输内容的准确性和健壮性。实验结果表明，B92 协议比 BB84 协议传输效果更佳。

关键词：量子加密；量子密钥分配；仿真；量子不可克隆定理；窃听检测

Simulation analysis of BB84 and B92 quantum communication encryption protocol

WU Jiayi[1], ZHOU Pengwei[1], ZHAO Nan[2], ZHOU Wei[1], TAN Zhenjiang[1]
(1 School of Mathematics and Computer Science, Jilin Normal University, Siping Jilin 136000, China;
2 Siping the twenty-fifth Middle School, Siping Jilin 136001, China)

【Abstract】 This paper mainly studies the simulation implementation of quantum BB84 protocol and B92 protocol and uses qiskit (pycharm software package) to design a simulation experimental model. By introducing bit error rate, error correction rate, and protocol reliability index, the security, accuracy and robustness of the two protocols are simulated under the condition of eavesdropper and noise in the transmission environment. Experimental results show that B92 protocol is better than BB84 protocol in the transmission process.

【Key words】 quantum cryptography; quantum key distribution(QKD); simulation; quantum no-cloning theorem; eavesdropping detection

0 引 言

网络安全是人们目前最关注的问题之一，大数据时代的到来使人们的隐私信息变得透明化，人们对个人的隐私信息也变得越来越重视[1]。如何保障人们信息不被他人窃取变得格外重要，为此也引起专家学者和研究人员的关注。根据柯克霍夫原则，信息加密的安全性并不是依赖于加密算法而是密钥本身[2]，而量子加密的密钥是依据一次性密码本的加密算法设计的，一次性密码本的加密算法是 1882 年被弗兰克·米勒发明的[3]，并且是被信息论之父香农证明其理论上是绝对安全的[4]。而相较于经典通信来看，量子加密是基于量子力学理论基础设计的，其中海森堡测不准原理、波包塌缩、不可克隆定理、单光子不可再分特性，保障了量子加密在通信中是绝对安全的，且通信双方每次传输的数据都是绝对随机的，一旦窃听者存在并且在传输中进行窃听，这就会导致误码率提升，一旦误码率高于一定阈值或双方最后的传输字符串等于 0，则通信双方就会约定舍弃此次通信内容。由于量子密钥分发系统的建立，以及利用量子信道实现信息保密已经逐渐成为现实，这将极大地推动量子密码技术发展，同时也是近年来国际学术界关注的热点之一，受到广泛重视，得到迅速发展，应用前景广阔。

基金项目：中国高校产学研创新基金(2021ITA05034，2021ITA05024)；吉林省高等教育研究课题(JLJJ719920190723194557)；吉林师范大学校级项目“三基一新”型计算机专业人才培养模式研究与实践；吉林师范大学博士启动项目(吉师博 2022014)。

作者简介：吴佳怡(1999-)，女，硕士研究生；主要研究方向：计算机应用技术；周芃玮(1999-)，女，硕士研究生，主要研究方向：计算机应用技术；赵 男(1991-)，女，硕士，中学二级教师，主要研究方向：学科教学；周 伟(1979-)，女，博士，副研究员，主要研究方向：计算机应用技术；谭振江(1965-)，男，博士，教授，博士生导师，主要研究方向：计算机科学与技术。

通讯作者：周 伟 Email：867458539@qq.com

收稿日期：2023-03-15

2008 年 Shuang Zhao 等人[5]采用一种基于事件过程的新方法来验证 BB84 协议。2009 年陈莹[6]通过 Qcircuit 软件设计 BB84 协议电路图，实验引入截取重发机制，通过误码率和协议可靠率来对 BB84 协议进行仿真安全性分析。2010 年 Mohamed Elboukhari 等人[7]使用模型检查器 PRISM 对 B92 协议的安全性进行了分析。2011 年路松峰等人[8]使用 QCircuit 软件设计量子线路图，通过引入截取重发攻击模型以及协议可靠率和有效平均互信息量两个变量，来验证 BB84 协议的安全性。2012 年朱丽娟等人[9]利用 C#语言通过 Windows 窗体达到可视化条件，通过调节窗体条件变量来对 BB84 协议进行仿真模拟。2014 年付益兵等人[10]通过 MATLAB 实现 BB84 协议的仿真。2016 年陈实等人[11]基于 Qcircuit 软件设计了 B92 协议的模拟电路，实验引入了相位阻尼、去极化、幅度阻尼 3 种噪声信道模型，通过误码率和协议可靠率来验证协议的安全性。2017 年孙茂珠等[12]通过对光的偏振的调制和对偏振光的测量，设计了有窃听者和无窃听者的实验示意图，模拟出了量子密钥分发 BB84 协议的通信情况。2020 年周争艳[13]采用蒙卡罗特方法来验证 B92 协议的安全性。2022 年 AkwasiAdu－Kyere 等人[14]基于 BB84 协议构建通信结构体系模型，通过模拟重复迭代，设置窃听者和拦截-重发干扰机制，引入参数窃听率、纠错率和量子位概率来验证协议可靠性。

本文基于上述研究背景，通过引入误码率、纠错率、协议可靠率指标，仿真分析了两种协议在有无窃听者发起攻击时的误码率、纠错率、协议可靠率，并仿真验证研究问题的真实性和有效性，通过对比折线图直观性验证两种协议在实际应用中协议的健壮性、安全性和协议传递数据的准确性。

1　问题分析

不同于传统加密协议，量子通信加密协议是基于量子态和量子的特殊物理性质，是有别于传统通信加密的一种特殊通信加密形式，其具有无条件安全性、传输速率快、免疫电磁干扰、通信容量大等优势。

虽然现在量子通信加密协议已有很多，但是 BB84 和 B92 协议是量子加密协议的经典协议，是量子通信加密的开始，后续的一切协议皆是基于两者协议进行参考的。本文针对 BB84 协议和 B92 协议进行实验模拟后进一步形成对比分析，通过引入误码率、纠错率、协议可靠性指标，重点对比分析了是否存在窃听者使用攻击的情况下两种协议的安全性。

1.1　理论推导

以下的仿真公式借用经典量子公式，具有良好的普适性[15-16]。

假设 Alice 和 Bob 共享量子信道 $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$，其中 $|\alpha|^2 + |\beta|^2 = 1$。Alice 要传输一种未知的量子态 $|\Psi\rangle = \left(\frac{\alpha}{\beta}\right)$，整个量子系统的态为 $|\Psi\rangle_{123} = |\varphi\rangle_1 |\Psi\rangle_{23} = \left(\frac{\alpha}{\beta}\right)_1 \left(\frac{1}{\sqrt{2}}|01\rangle_{23} \pm \frac{1}{\sqrt{2}}|10\rangle_{23}\right)$[15]。式中的下标用于表示粒子的去向，下标 1 表示要被传送的粒子，下标 2 表示 Alice 在传送中量子的分配，下标 3 表示 Bob 在传送中量子的分配。瞬间传态基于初始状态也可表示为

$$|\Psi\rangle_{123} = \frac{1}{2}\left[|\Phi^+\rangle_{12}\left(\frac{-\beta}{\alpha}\right)_3 + |\Phi^-\rangle_{12}\left(\frac{\beta}{\alpha}\right)_3 + |\Psi^+\rangle_{12}\left(\frac{-\alpha}{\beta}\right)_3 - |\Psi^-\rangle_{12}\left(\frac{\alpha}{\beta}\right)_3\right] \quad (1)$$

式中：$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$，$|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$，$|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$，$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$。如果 Alice 测量的结果是 $|\Psi^+\rangle_{12}$，则 Bob 得到的量子态是 $|\Psi\rangle = \frac{1}{\sqrt{(\alpha^2+\beta^2)}}\left(\frac{\alpha}{\beta}\right)$[16]。

Alice 和 Bob 共享一对 EPR 对，考虑 POVM 测量传输以下 4 种矩阵状态：

$$\boldsymbol{A}_1 = \frac{1}{2}|\Phi_1\rangle|\Phi_1| = \frac{1}{2}\begin{pmatrix}|\alpha|^2 & \beta\alpha^* \\ \beta^*\alpha & |\beta|^2\end{pmatrix};$$

$$\boldsymbol{A}_2 = \frac{1}{2}|\Phi_2\rangle\langle\Phi_2| = \frac{1}{2}\begin{pmatrix}|\beta|^2 & -\beta^*\alpha \\ -\beta\alpha^* & |\alpha|^2\end{pmatrix};$$

$$\boldsymbol{A}_3 = \frac{1}{2}|\Phi_3\rangle\langle\Phi_3| = \frac{1}{2}\begin{pmatrix}|\beta|^2 & \beta^*\alpha \\ \beta\alpha^* & |\alpha|^2\end{pmatrix};$$

$$\boldsymbol{A}_4 = \frac{1}{2}|\Phi_4\rangle\langle\Phi_4| = \frac{1}{2}\begin{pmatrix}|\alpha|^2 & -\beta\alpha^* \\ -\beta^*\alpha & |\beta|^2\end{pmatrix} \quad [16] \quad (2)$$

其中，$\langle\Phi_1| = (\alpha,\beta)$，$\langle\Phi_2| = (\beta, -\alpha)$，$\langle\Phi_3| = (\beta,\alpha)$，$\langle\Phi_4| = (\alpha, -\beta)$。对 Alice 传输的量子态进行贝尔基测量会随意塌缩到公式(2)4 种情况

中的任意一种,Alice 通过经典信道把测量结果告诉 Bob,Bob 会做一定的幺正变换恢复结果。具体步骤如下:

当 Alice 对属于他的配额做出测量结果塌缩后,Bob 的部分配额会发生变化,由 $|\Phi\rangle$ 转化为正交态 $|\Psi\rangle$,可得到 4 种结果:$|\Psi_1\rangle = \begin{pmatrix}\beta\\-\alpha\end{pmatrix}$;$|\Psi_2\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$;$|\Psi_3\rangle = \begin{pmatrix}\alpha\\-\beta\end{pmatrix}$;$|\Psi_4\rangle = \begin{pmatrix}\beta\\\alpha\end{pmatrix}$。需要注意的是,Bob 恢复量子态是依据 Alice 通过经典信道传送的塌缩后的结果,而不是 α 和 β。Bob 得到量子态 $|\Psi\rangle$ 后,为了恢复 Alice 传输的态,进行了如下操作。以 M_1 为例遵循公式(3)恢复 Alice 传给其的量子态:

$$(M_1)_{ij} = \sum ab\ (C_1)_{ia,jb}\ (\rho_{ser})_{ba} \tag{3}$$

在公式(3)中,M_1 塌缩的结果是 $C_1 = |\Phi^+\rangle\langle\Phi^-|$,辅助位 $\rho_{ser} = |\Phi\rangle\langle\Phi|$,下角标 ij 代表传输的量子,ba 代表的是辅助的量子。令 $i=0, j=0$ 时,通过辅助位 ρ_{ser} 乘以 C_1 得出结果 Res $\begin{pmatrix}\frac{1}{2} & 0\\0 & 0\end{pmatrix}_{ab}\begin{pmatrix}|\alpha|^2 & \beta\alpha^*\\\beta^*\alpha & |\beta|^2\end{pmatrix} = \frac{1}{2}|\alpha|^2$[16],对应 M_1 的左上角。当 $i=1, j=0$ 时,对应结果是 M_1 的第二行左下角,以此类推。用这种方法,无论结果传输的是哪种态(公式(2))Bob 都可以得到对应的结果。

1.1.1 误码率

误码是指在一次通信传输过程中由于外界因素(如:噪音、窃听者攻击等)干扰,使原本传输的信号由 0 变为 1 或由 1 变为 0。误码率是判断协议安全性的一个常见指标,在本文中误码率的计算公式如下:

$$nErrors = \frac{dif(key_{AB})}{len(key_A)} \tag{4}$$

其中,$nErrors$ 代表误码率;$dif(key_{AB})$ 代表协议发送方 Alice 与接收方 Bob 最后确定密钥的每位比特对比后,结果不同的数量;$len(key_A)$ 代表发送方 Alice 最后确定的密钥长度。

1.1.2 纠错率

纠错率又叫容错率,代表一次通讯中允许犯错的概率,纠错率越高协议的准确性越高,反之准确性越低。本文中纠错率的计算公式如下:

$$Ecr = \frac{wn}{toalnum} \tag{5}$$

式中:Ecr 代表纠错率,wn 代表一次协议中双方舍去的比特数,toalnum 代表一次协议中发送方初始产生的比特数。

1.1.3 协议可靠率

协议可靠率也是检验协议可靠性和安全性的手段之一,协议可靠率越高证明协议可靠性和安全性越高,反之协议可靠性及安全性越低。本文协议可靠率的计算公式如下:

$$Prel = herrRate - nerrRate \tag{6}$$

式中:$Prel$ 代表协议可靠率,$herrRate$ 代表有窃听者时协议的误码率,$nerrRate$ 代表没有窃听者时协议的误码率。

1.2 影响因素分析

在实际运行环境中,受诸多因素影响导致在通信中误码率的提升。如:窃听者、外界拦截—重发攻击、噪声、实际物理外界因素等,都会对通信过程产生影响。

1.2.1 窃听者

窃听者的存在使发送双方在通信时,会舍弃掉一半以上的传输比特。因为一旦窃听者对发送内容进行窃听,就会“触碰”到量子,而基于量子力学的波包塌缩特性,使得量子快速塌缩到任意偏振态。然而窃听者 Eve 并不知道接收方 Bob 与发送方 Alice 约定使用那种正交归一基作为测量塌缩结果,则导致发送双方舍弃掉量子比特的数量增加,进而导致误码率的提升。

1.2.2 拦截—重发攻击

常见的网络通讯攻击有很多种,其中最为常见的就是拦截—重发攻击。本文引入窃听者变量,以窃听者为第三方变量对通信双方的通信过程进行拦截—重发攻击。协议开始,Alice 生成一段随机字符串并发送给 Bob,发送途中 Eve 对信息进行拦截测量,并对字符串进行重新编码后发送给 Bob,这个过程就是拦截—重发的攻击过程。

1.2.3 噪声

通信过程中噪声是最不可避免的影响因素,实验中设置噪声信道影响参数,当信号由 Eve 发送给 Bob 的过程中引入,传输的每个比特信号将会以噪声信道影响参数的概率进行翻转。实验结果表明,噪声信道影响参数越大误码率越高,纠错率越高,协议可靠率越低。

1.3 仿真分析与设计

1.3.1 BB84 协议

经典 BB84 协议流程如图 1 所示。

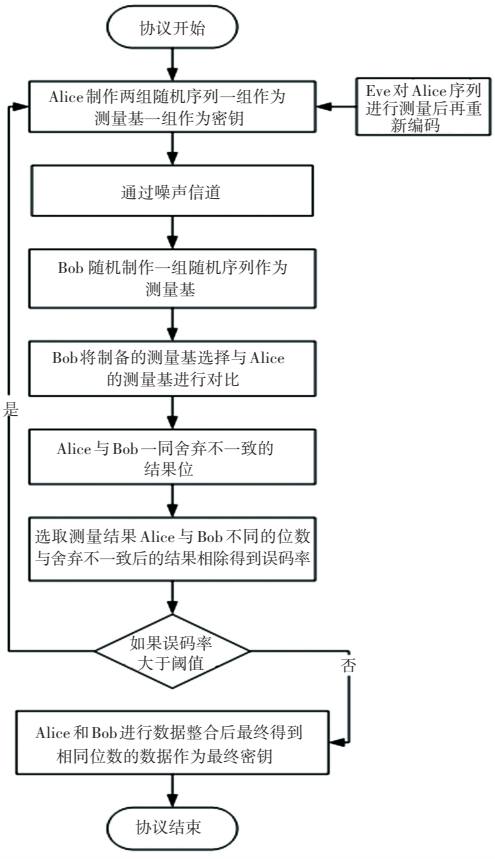

图 1　BB84 协议流程图

Fig. 1　BB84 protocol flowchart

Alice 随机选取两组序列 $\{a_n\}$、$\{b_n\}$，序列长度为 $2n$，Alice 随机制备 $2n$ 单光子偏振非正交态，即 $2n$ 个单量子态发送给 Bob。在此，量子偏振态采取希尔伯特二维空间，利用 Dirac 记号记录 4 种量子偏振态结果如下：

$$|H\rangle = |0\rangle, |V\rangle = |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{7}$$

式中：$|H\rangle$ 和 $|V\rangle$ 是一组完备的正交归一基，称为水平垂直基简称 Z 基。其中，$|H\rangle$ 是水平偏振态，$|V\rangle$ 是垂直偏振态。$|+\rangle$ 和 $|-\rangle$ 是一组完备的正交归一基，称为对角基，简称 X 基。其中，$|+\rangle$ 是 45° 偏振态，$|-\rangle$ 是 135° 偏振态。这里 Z 基和 X 基的任意形态都是非正交的，而且塌缩概率皆为 50%[17]。

其中，偏振态形状如图 2 所示。

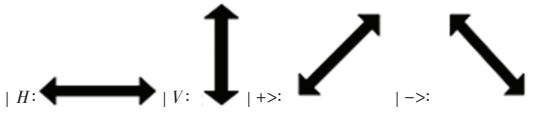

图 2　量子 4 种偏振态

Fig. 2　The four polarization states of the quantum

当 Bob 收取到 $2n$ 个量子态后，用传统信道公布收到信号的事实，然后选取一组长度为 $2n$ 的序列 $\{x_n\}$ 作为决定测量基。Bob 随机选取 Z 基或 X 基作为测量基，当取 Z 基作为测量基时 Bob 取为“0”，取 X 基作为测量基时 Bob 取为“1”，测量结果存储在一组序列并将其命名为 $\{y_n\}$。之后，Alice 公布序列 $\{a_n\}$ 所用的测量基结果，Bob 将选择 $\{x_n\}$ 的测量基与 $\{a_n\}$ 进行对比后，将对比结果的“不一致位”发送给 Alice，Alice 收到 Bob 发送的结果后也删去“不一致位”。Alice 将剩余的 n 个数据随机选取 $n/2$ 用于进行窃听检测，如果达到一定的误码率值，则终止协议重新开始，否则 Alice 和 Bob 进行数据整合后，最终得到 m 比特相同数据作为最终密钥。

1.3.2　B92 协议

B92 协议流程如图 3 所示：

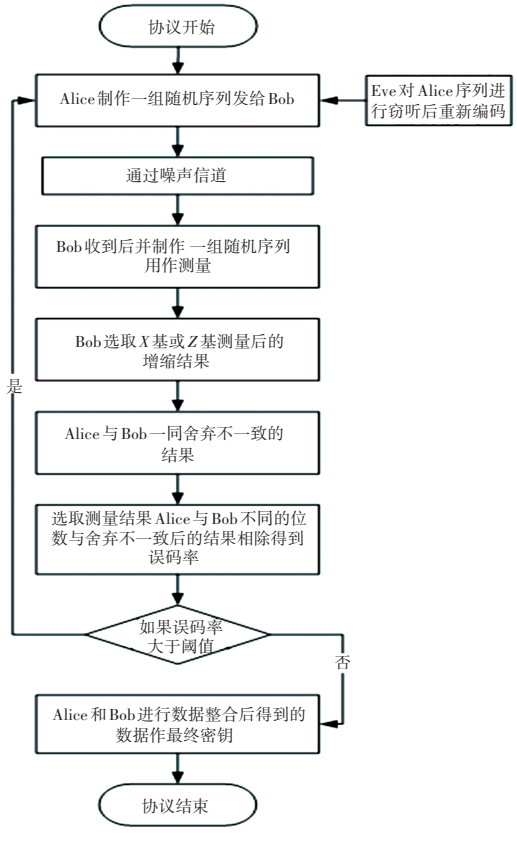

图 3　B92 协议流程图

Fig. 3　B92 Protocol flow chart

Alice 随机选取一组序列 $\{a_n\}$，序列长度为 $4n$，Alice 随机制备 $4n$ 单光子偏振非正交态，即 $4n$ 个单量子态发送给 Bob，在此量子偏振态多采取希尔伯特二维空间水平垂直基的水平偏振态和对角基中的 45° 偏振态，利用 Dirac 记号记录两种量子偏振态结果如下：

$$|H\rangle = |0\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (8)$$

式中:用 0 代表水平偏振态 $|H\rangle$,1 代表 45° 偏振态 $|+\rangle$。

当 Bob 收取到 $4n$ 个量子态后,用传统信道公布收到信号的事实,然后选取一组长度为 $4n$ 的序列 $\{b_n\}$ 作为决定测量基。Bob 随机选取 Z 基或 X 基作为测量基,当取 Z 基作为测量基时,Bob 取为“0”,取 X 基作为测量基时 Bob 取为“1”,测量结果存储在一组序列并将其命名为 $\{c_n\}$。当 Z 基和 X 基的测量结果为“0”时,则为“不确定结果”,且不保存在序列 $\{c_n\}$ 中。因为当 Alice 发送量子态 $|+\rangle$ 时,使用 X 基测量也可得到量子态 $|+\rangle$;同理,当 Alice 发送量子态 $|H\rangle$ 时,使用 Z 基测量也可得到量子态 $|H\rangle$。当测量 Z 基的结果为“1”时,将测量结果确定为 1 并存储到序列 $\{c_n\}$ 中。因为当测量结果为“1”时,Bob 可以确认 Alice 发送的量子态为 $|+\rangle$;而当测量 X 基的结果为“1”时,把测量结果确定为 0 并存储到序列 $\{c_n\}$ 中。因为当测量结果为“1”时,Bob 可以确认 Alice 发送的量子态为 $|H\rangle$。这样通信双方也不必对比测量基就可以确定最后保留哪些信息,减少 Eve 窃取信息得到密钥结果,大大增强了通信双方信息的安全性。测量结束后,Bob 将 Z 基和 X 基测量结果为“0”的“不确定结果”发给 Alice,Alice 收到 Bob 发送的结果后也删去“不确定结果”位,将剩余的 n 个数据随机选取 $n/2$ 用于窃听检测。如果达到一定的误码率值则协议终止重新开始;若结果低于一定的误码率,则 Alice 和 Bob 进行数据整合后,最终得到 m 比特相同数据作为最终密钥。

1.4 协议对比

Bennett[17] 提出的 B92 协议是对 BB84 协议的一种修改方案,是一个二态协议,不同于 BB84 协议中使用了 4 个非正交的量子态,而 B92 协议只利用两个非正交量子态就能够完成量子密钥分发。就协议本身来说,BB84 协议传输的是测量基,B92 协议传输的是塌缩后的结果。B92 协议的校验过程与 BB84 协议完全相同,区别在于存在窃听时的量子比特误码率。B92 协议对实验设备的要求比 BB84 协议低,其量子比特制备相对简单,只需要制造两个方向的信号即可。由于 B92 协议的效率只有 25%,仅为 BB84 协议的一半,B92 通信双方平均只有 25% 的量子态可以成为有效的传输结果,75% 的量子信号则被损失掉[18]。

2 仿真实验及结果分析

仿真实验使用 Python 语言编写量子密钥分配协议程序。主要实现了无窃听、有窃听两种情况下的量子密钥分配过程。程序中引入了参数变量 eve 来控制窃听者的存在,N 用来控制产生的量子比特数量,noise parameters 用以控制噪声参数。实验步骤如下:

(1)定义两组函数 runBB84、runB92 分别代表 BB84 和 B92 两个协议,函数过程即 BB84 和 B92 协议的通信加密过程;

(2)设置随机生成序列函数 list(np.random.randint(0,2,N))用于发送方 Alice 和接收方 Bob 的初始密钥或测量基;

(3)发送方 Alice 选取量子位发送给接收方 Bob,如果有窃听者 Eve 存在则 Alice 发送给 Bob 的字符串就会被 Eve 拦截后重新编码后发送给 Bob,如果存在噪声则引入噪声引起的误差;

(4)接收方 Bob 根据其随机生成的测量基来测量量子位;

(5)接收方 Bob 识别出与 Alice 字符串不一致的量子位;

(6)得出最终密钥。

实验分别模拟了有、无窃听时的量子密钥分配过程。假设产生 256 个量子比特位,信道噪声为 0.5。初始密钥分配完成后,选取 10 个数据对比,通过误码率、协议可靠率对比,以检测协议的可靠性和安全性。

2.1 无窃听者

BB84 和 B92 协议无窃听者时实验结果见表 1。

表 1 是 BB84 协议和 B92 协议在无窃听者存在时一次通信过程中的十组数据对比。BB84 与 B92 协议不同的是:BB84 协议设置了 Alice 最初密钥而 B92 协议没有设置,B92 协议的 Alice 仅制备水平偏振量子态 $|H\rangle$ 和 45°偏振态 $|+\rangle$。

2.2 有窃听者

BB84 和 B92 协议有窃听者时结果见表 2。

表 2 是 BB84 协议和 B92 协议在有窃听者存在时一次通信过程中的十组数据对比。BB84 与 B92 协议不同的是:BB84 协议设置了 Alice 最初密钥而 B92 协议没有,B92 协议 Alice 仅制备水平偏振量子态 $|H\rangle$ 和 45°偏振态 $|+\rangle$;与无窃听者时不同,窃听者会对信道上的量子态进行窃听,而根据波包塌缩原则和量子不可克隆定理,一旦窃听者进行窃听必然会导致量子态的改变进而影响传输结果。

表 1　无窃听者时 BB84 和 B92 协议密钥分配数据对比

Tab. 1　Comparison on key distribution data of BB84 and B92 protocol without eavesdropper

	BB84										B92									
	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10
Alice 测量基	0	1	1	0	1	0	1	1	1	1	0	0	0	1	0	0	1	0	1	1
Alice 最初密钥	1	1	0	1	0	1	0	0	0	0										
Bob 测量基	0	1	0	1	1	1	0	0	0	1	0	1	0	1	1	0	0	1	1	1
Alice 塌缩结果	90°	135°	45°	90°	45°	90°	45°	45°	45°	45°	0°	0°	0°	45°	0°	0°	45°	0°	45°	45°
Bob 塌缩结果	90°	135°	0°	45°	45°	135°	90°	90°	90°	45°	0°	45°	0°	45°	135°	0°	90°	135°	45°	45°
Alice 最终密钥	0	0	1	1	1	0	1	1	1	1	0	1	0	1	0	0	0	0	1	0
Bob 最终密钥	0	0	1	1	1	0	1	1	1	1	0	1	0	1	0	0	0	0	1	0

表 2　有窃听者时 BB84 和 B92 协议密钥分配数据对比

Tab. 2　Comparison on key distribution data of BB84 and B92 protocol with eavesdropper

	BB84										B92									
	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	10
Alice 测量基	1	1	0	0	0	0	0	1	1	1	0	0	1	0	0	1	0	0	0	1
Alice 最初密钥	1	1	1	0	0	0	0	0	1	1										
Bob 测量基	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	0	0	1
Alice 塌缩结果	135°	135°	90°	0°	0°	0°	0°	45°	135°	135°	0°	0°	45°	0°	0°	45°	0°	0°	0°	45°
Eve 塌缩结果	135°	135°	135°	0°	45°	0°	0°	45°	135°	90°	135°	0°	45°	45°	0°	45°	45°	45°	135°	45°
Bob 塌缩结果	135°	135°	135°	0°	90°	0°	0°	90°	135°	90°	90°	0°	45°	45°	45°	45°	45°	0°	0°	45°
Alice 最终密钥	1	1	0	0	0	0	1	0	1	0	0	0	1	0	0	1	0	0	1	1
Bob 最终密钥	1	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	1	0	1	1

2.3　结果对比分析

图 4 是输入 256 比特，噪声参数为 0.5，在无窃听者存在时，经过 10 次遍历后每一次误码率形成的折线图。从图中可以明显看出，在同一时间下且没有窃听者存在时，BB84 协议的误码率明显高于 B92 协议，说明 B92 协议的安全性远远高于 BB84 协议。图 5 是输入 256 比特，噪声参数为 0.5，在无窃听者存在时，经过 150 次遍历后每一次误码率形成的折线图。从图中可以明显看出，经过多次遍历后，在同一时间下、没有窃听者存在时，BB84 协议的误码率仍然明显高于 B92 协议。在 150 次遍历下，蓝色实线高于橘色虚线的概率是 98%，此时 B92 协议的安全性远远高于 BB84 协议。图 6 展现了输入 256 比特，噪声参数为 0.5，在有窃听者存在时且对传输过程发起拦截—攻击的情况下，经过 10 次遍历后每一次误码率形成的折线图。可以明显看出，在同一时间下、有窃听者且进行拦截—重发攻击存在时，B92 协议的误码率明显高于 BB84 协议。虽然在 10 次遍历下有部分重合但是可以明显看出蓝色实线高于橘色虚线的概率为 36.4%，这时 BB84 协议的安全性高于 B92 协议。图 7 是输入 256 比特，噪声参数为 0.5，在有窃听者且进行拦截—重发攻击存在的情况下，经过 150 次遍历后每一次误码率形成的折线图。在多次遍历后可以看出，BB84 协议和 B92 协议的误码率开始有部分重合，但是橘色虚线还是普遍高于蓝色实线，在 150 次遍历下蓝色实线高于橘色虚线的概率是 48%。通过结果数据和图中对比可知，在同一时间下、有窃听者且进行拦截—重发攻击存在时，B92 协议的误码率明显高于 BB84 协议，这时 BB84 协议的安全性高于 B92 协议。

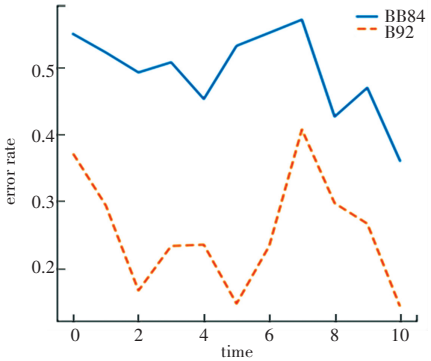

图 4　无窃听者时的两协议 10 次误码率对比

Fig. 4　Comparison of 10 bits error rate between the two protocols without eavesdropper

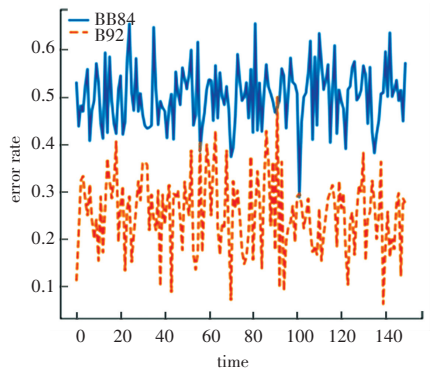

图 5 无窃听者时的两协议 150 次误码率的对比

Fig. 5 Comparison of 150 bits error rate between the two protocols without eavesdropper

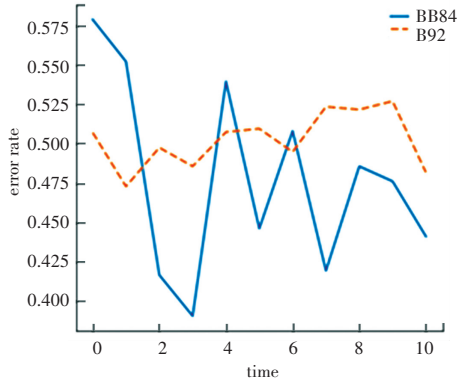

图 6 有窃听者时的两协议 10 次误码率的对比

Fig. 6 Comparison of 10 bits error rate between the two protocols with eavesdropper

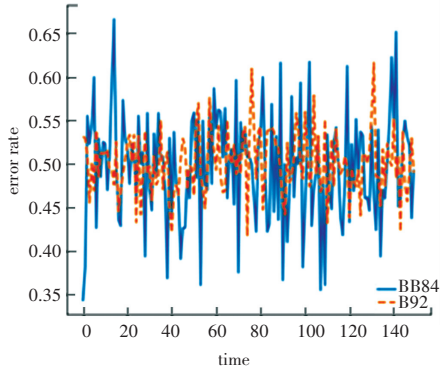

图 7 有窃听者时的两协议 150 次误码率的对比

Fig. 7 Comparison of 150 bits error rate between the two protocols with eavesdropper

图 8 是输入 256 比特,噪声参数为 0.5,在无窃听者存在时,经过 10 次遍历后每一次纠错率形成的折线图。图中可以明显看出在同一时间下、没有窃听者存在时 BB84 协议的纠错率是明显低于 B92 协议的,这时 B92 协议的安全性和协议传输内容的准确性是远远高于 BB84 协议的。图 9 是输入 256 比特,噪声参数为 0.5,在无窃听者存在时,经过 150 次遍历后每一次纠错率形成的折线图。图中可以明显看出在经过更多次遍历后在同一时间下、没有窃听者存在时 BB84 协议的纠错率还是明显低于 B92 协议的,这时 B92 协议的安全性和协议传输内容的准确性是远远高于 BB84 协议的。图 10 是输入 256 比特,噪声参数为 0.5,在有窃听者且进行拦截——重发攻击存在时,经过 10 次遍历后每一次纠错率形成的折线图。图中可以明显看出在同一时间下、有窃听者且进行拦截——重发攻击存在时 BB84 协议的纠错率是明显低于 B92 协议的,这时 B92 协议的安全性和协议传输内容的准确性是远远高于 BB84 协议的。图 11 是输入 256 比特,噪声参数为 0.5,在有窃听者进行拦截——重发攻击存在时,经过 150 次遍历后每一次纠错率形成的折线图。由图中可以明显看出在经过更多次遍历后在同一时间下、有窃听者且进行拦截——重发攻击存在时 BB84 协议的纠错率还是明显低于 B92 协议的,这时 B92 协议的安全性和协议传输内容的准确性是远远高于 BB84 协议的。

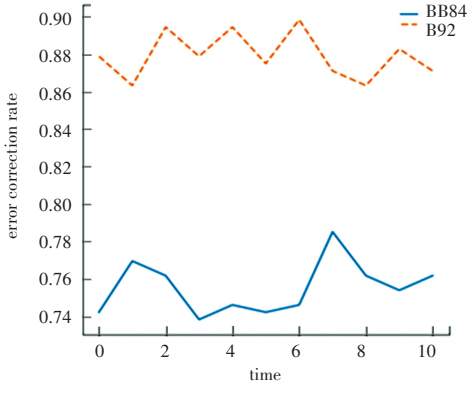

图 8 无窃听者时的两协议 10 次纠错率的对比

Fig. 8 Comparison of 10 error correction rate between two protocols without eavesdropper

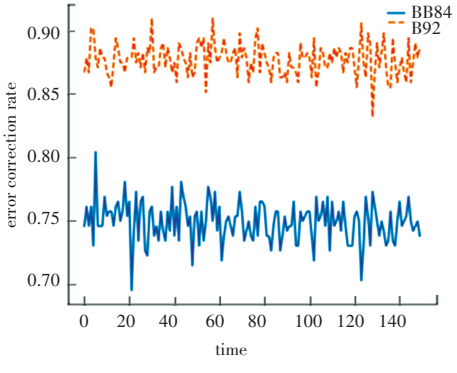

图 9 无窃听者时的两协议 150 次纠错率的对比

Fig. 9 Comparison of 150 error correction rate between two protocols without eavesdropper

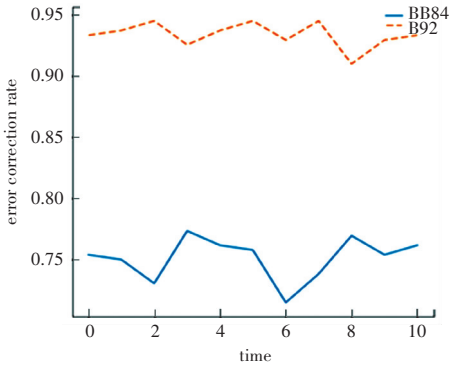

图 10　有窃听者时的两协议 10 次纠错率的对比

Fig. 10　Comparison of 10 error correction rate between two protocols with eavesdropper

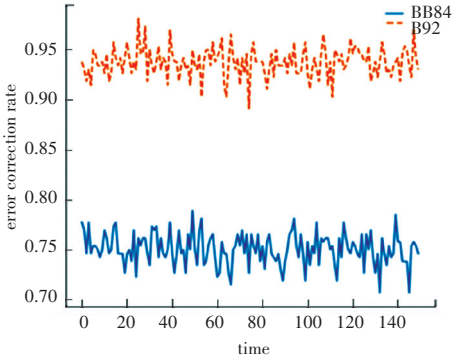

图 11　有窃听者时的两协议 150 次纠错率的对比

Fig. 11　Comparison of 150 error correction rate between two protocols with eavesdropper

图 12 是输入 256 比特，噪声参数为 0.5，经过 10 次遍历后每次协议可靠率形成的折线图。由图中可以明显看出，在同一时间下 BB84 协议的协议可靠率明显低于 B92 协议，这时 B92 协议的安全性和协议健壮性远远高于 BB84 协议。图 13 是输入 256 比特，噪声参数为 0.5，经过 150 次遍历后每次协议可靠率形成的折线图。可以明显看出，经过多次遍历后在同一时间下，BB84 协议的可靠率虽然有部分重合但还是明显低于 B92 协议。在 150 次遍历下，橘色虚线低于蓝色实线的概率是 40%，这时 B92 协议的安全性和协议健壮性远远高于 BB84 协议。

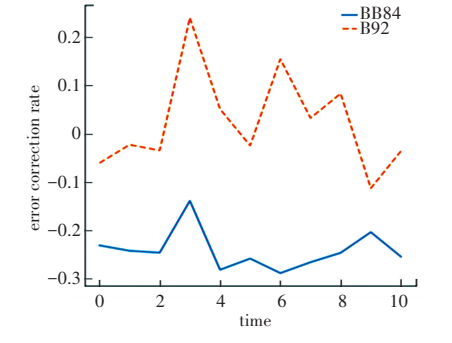

图 12　两协议 10 次协议可靠率对比

Fig. 12　Comparison of 10 protocol reliability between the two protocols

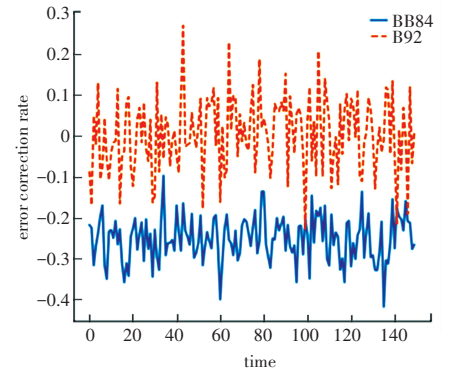

图 13　两协议 150 次协议可靠率对比

Fig. 13　Comparison of 150 protocol reliability between the two protocols

3　结束语

经过上述对比分析可知：在无窃听者存在时，BB84 协议的误码率远高于 B92 协议；引入窃听者后，B92 协议的误码率就会上升并高于 BB84 协议。但是，当引入纠错率和协议可靠率时，无论窃听者存在与否 B92 协议传输内容的准确性及协议的健壮性都远高于 BB84 协议，所以传输内容时选择 B92 协议要好于 BB84 协议。

随着量子技术的飞速发展，量子加密协议变得更加严谨，协议对环境外界干扰的要求也越来越小，协议的鲁棒性与安全性逐步增强。对量子态的制备也不再要求是在理想的条件下[19]，量子传输速率越来越快，传输公里数越来越长，量子通信加密协议也越来越适用在各种复杂多样的场景中。关于如何仿真 BB84 协议和 B92 协议，除了窃听者和误码率、纠错率、协议可靠率以外是否可以引入其他因素和变量来验证安全性，都可以进一步研究和讨论。

参考文献

[1] 康鹏，杨文忠，马红桥. TLS 协议恶意加密流量识别研究综述[J]. 计算机工程与应用，2022，58(12)：1-11.

[2] 孔小琴，李琴，李远科，等. 基于纠缠的量子密钥分配协议仿真[J]. 计算机工程与应用，2017，53(1)：113-117.

[3] ERSKINE R. Enigma′s Security：What the Germans really knew[J]. Ralph Erskine and Michael Smith，2001：370-386.

[4] SHANNON C E. Communication theory of secrecy systems. 1945.[J]. M.D. computing ： computers in medical practice，1998，15(1).

[5] ZHAO S，DE RAEDT H. Event-by-event simulation of quantum cryptography protocols [J]. Journal of Computational and Theoretical Nanoscience，2008，5(4)：490-504.

[6] 陈莹. BB84 量子密钥分配及其后处理的仿真分析[D]. 武汉：华中科技大学，2009.

（下转第 167 页）