激光与光电子学进展

抗集体噪声的测量设备无关的量子安全直接通信

郭瀚，李云霞*，魏家华**，唐杰，曹跃翔
空军工程大学信息与导航学院通信系统教研室，陕西 西安 710077

摘要 量子安全直接通信(QSDC)突破了传统保密通信的通信方式，不需要提前准备密钥就可以直接通过量子信道进行秘密信息的传输。但是在实际的量子通信系统中，窃听者Eve对于测量设备的攻击会导致秘密信息的泄露，而且这种窃听不会被侦测到。此外由于现在的量子传输方式仍然以光纤传输为主，所以无法避免光纤传输过程中噪声的影响，在这些噪声中以集体退相位噪声和集体旋转噪声影响最甚。为解决这些问题，提出了两个分别可以抵抗集体退相位噪声和集体旋转噪声的测量设备无关的QSDC协议，通过不可信第三方的测量进行信息的传递，解决了窃听者对于测量设备攻击的问题，同时通过无消相干子空间来避免集体噪声的问题，通过分析发现该协议可以有效抵抗攻击，实现绝对安全的通信。

关键词 量子通信；量子安全直接通信；测量设备无关；集体噪声
中图分类号 0431.2 **文献标志码** A **DOI**：10.3788/LOP202259.1727001

Immune to Collective Noise Measurement-Device-Independent Quantum Secure Direct Communications

Guo Han, Li Yunxia*, Wei Jiahua**, Tang Jie, Cao Yuexiang
Teaching and Research Section of Communication Systems, Institute of Information and Navigation, Air Force Engineering University, Xi'an 710077, *Shaanxi, China*

Abstract Quantum secure direct communication (QSDC) breaks the structure of traditional secret communications. It directly sends a secret message through a quantum channel without first preparing the key. But in the actual quantum communication system, the eavesdropper Eve's attack on the device will lead to the leakage of secret information, and this eavesdropping will not be detected. In addition, since the current quantum transmission mode is still based on optical fiber transmission, it is impossible to avoid the influence of noise in the process of optical fiber transmission. Among these noises, collective dephasing noise and collective rotation noise are the most serious. In order to solve these problems, two measurement-device-independent QSDC protocols that can resist collective dephasing noise and collective rotation noise respectively are proposed. The information is transmitted through the measurement of an untrusted third party, which solves the problem of eavesdroppers' attack on measurement device. At the same time, the collective noise is avoided through no decoherence subspace. Through analysis, it is found that the protocol can effectively resist attacks and achieve absolutely secure communication.

Key words quantum communications; quantum secure direct communication; measurement-device-independent; collective noise

1 引 言

随着量子信息处理技术的发展，量子加密引起了相关研究人员的广泛关注。与经典加密方式的复杂算法不同的是，量子加密以量子物理的理论为基础来实现无条件的安全性。当前，已经出现了各种各样的量子加密协议，应用在不同的条件下。包括量子密钥分发(QKD)[1-7]、量子秘密共享(QSS)[8-9]、量子密钥协商(QKA)[10-11]、量子支付协议(EPP)[12]、量子签名(QS)[13]等。2002年，Long等[14]提出了一种新的量子加密方式：量子安全直接通信(QSDC)。众所周知，QKD通过随机生成密钥来实现通信的“一次一密”。而QSDC不需要提前准备共享密钥，就可以将信息通过不同的量子状态表示，从而进行秘密信息的传递。

收稿日期：2022-01-10；**修回日期**：2022-03-22；**录用日期**：2022-05-13
基金项目：国家自然科学基金(61971436,61803382)
通信作者：*yunxial@foxmail.com；**weijiahua@126.com

QSDC突破了传统保密通信的双信道结构，只有一个量子直通信道，提高了整个系统的安全性，同时扩展了量子通信的范围。没有事先的密钥生成过程，自然也就不需要分配资源进行密钥管理，同时也不需要后续的加密和解密过程，节约了量子资源。

近二十余年来，关于QSDC的研究也在逐步推进。2002年，Boström等[15]基于密集编码提出了Ping-Pong协议，该协议明确了QSDC的定义，具有相当的理论价值。2003年，Deng等[16]提出了一种利用EPR(Einstein-Podolsky-Rosen)对的“两步方案”实现QSDC，并明确了QSDC的含义和要求。2004年，Deng等[17]提出了利用单光子来实现“一次一密”的QSDC。2006年，Deng等[18]提出了QSDC网络的概念。自此之后，多方的安全直接通信领域展开了各种研究[19-21]。比如2006年，Jin等[20]提出了一个基于GHZ态的三方同时通信的QSDC。2011年，Wang等[22]利用光子对自由度超纠缠的EPR对实现高容量的QSDC。2013年，Yang等[23]提出了一个可认证的抵抗集体噪声的协议，该协议可以在不需要经典信道的条件下实现安全认证。2014年，Yang[24]提出了不需要量子寄存器的单光子QSDC方案。2015年，Li等[25]基于四粒子的簇态提出了一个QSDC方案，该方案通过四粒子纠缠态加强了安全性检测。2017年，He等[26]提出了两个分别可以抵抗集体退相位噪声以及集体旋转噪声的QSDC协议，通过六粒子纠缠态实现了三方的安全通信。2018年，Niu等[27]提出了第一个测量设备无关(MDI)的QSDC(MDI-QSDC)协议，通过第三方的Bell测量实现通信过程。2020年，Zhou等[28]在Niu等[27]的基础上，利用单光子和Bell态实现MDI-QSDC，进一步提高了通信效率。

QSDC在理论上是绝对安全的，但是在实际的量子通信系统中，仍然无法避免地存在一些实际问题。比如，现如今使用的量子信道大多是光纤，而光纤具有双折射的波动性，光子在量子信道中传输时会受到噪声的影响，光子传输的时间窗比噪声源变化短。因此，在信道中传输的这些光子都将受到相同噪声的影响，这便是集体噪声[29]。集体噪声包括集体退相位噪声和集体旋转噪声。此外，在量子通信系统中，窃听者如果对测量设备发起攻击，那么攻击行为很难被发现。基于以上存在的问题，本文基于四粒子GHZ态和类GHZ态，通过构造无消相干子空间来抵抗集体噪声的影响，提出了两个分别可以抵抗集体退相位噪声和集体旋转噪声的MDI-QSDC协议，通过不可信第三方的测量进行信息的传递，可以有效抵抗窃听攻击。

2 预备知识

集体噪声包括集体退相位噪声和集体旋转噪声。为了解决集体噪声的影响，引入无消相干子空间(DFS)的概念。DFS是系统希尔伯特空间的一种子空间，它不经历消相干，DFS的状态是由几个物理量子位元组成。由于DFS在量子信道中受到相同噪声的量子位元会补偿集体噪声的影响，因此DFS可以在集体噪声下保持不变性。该特性可用于集体噪声信道中的量子通信。

2.1 集体退相位噪声

集体退相位噪声对于量子状态的影响可以表示为

$$U_{\mathrm{dp}}|0\rangle=|0\rangle,U_{\mathrm{dp}}|1\rangle=\mathrm{e}^{\mathrm{i}\theta}|1\rangle, \tag{1}$$

幺正算子U_{dp}表示为

$$U_{dp}=\begin{pmatrix}1 & 0\\ 0 & \mathrm{e}^{\mathrm{i}\theta}\end{pmatrix}, \tag{2}$$

式中，θ表示噪声参数，且随时间变化。

而逻辑粒子$\left|0_{\mathrm{dp}}\right\rangle=|01\rangle,\left|1_{\mathrm{dp}}\right\rangle=|10\rangle$以及它们的叠加态

$$\begin{cases}\left|+_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|0_{\mathrm{dp}}\right\rangle+\left|1_{\mathrm{dp}}\right\rangle\right)=\dfrac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right)=\left|\varphi^{+}\right\rangle\\ \left|-_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|0_{\mathrm{dp}}\right\rangle-\left|1_{\mathrm{dp}}\right\rangle\right)=\dfrac{1}{\sqrt{2}}\left(|01\rangle-|10\rangle\right)=\left|\varphi^{-}\right\rangle\end{cases}, \tag{3}$$

都可以不受集体退相位噪声的影响。

为了抵抗集体退相位噪声的影响，本文用到的四粒子GHZ态为

$$\begin{cases}|G_1\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0_{\mathrm{dp}}\right\rangle\left|0_{\mathrm{dp}}\right\rangle+\left|1_{\mathrm{dp}}\right\rangle\left|1_{\mathrm{dp}}\right\rangle\right)=\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|01\rangle_{34}+|10\rangle_{12}|10\rangle_{34}\right)=\dfrac{1}{\sqrt{2}}\left(|\Phi^{+}\rangle_{13}|\Phi^{+}\rangle_{24}-|\Phi^{-}\rangle_{13}|\Phi^{-}\rangle_{24}\right)\\ |G_2\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0_{\mathrm{dp}}\right\rangle\left|0_{\mathrm{dp}}\right\rangle-\left|1_{\mathrm{dp}}\right\rangle\left|1_{\mathrm{dp}}\right\rangle\right)=\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|01\rangle_{34}-|10\rangle_{12}|10\rangle_{34}\right)=\dfrac{1}{\sqrt{2}}\left(|\Phi^{-}\rangle_{13}|\Phi^{+}\rangle_{24}-|\Phi^{+}\rangle_{13}|\Phi^{-}\rangle_{24}\right)\\ |G_3\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0_{\mathrm{dp}}\right\rangle\left|1_{\mathrm{dp}}\right\rangle+\left|1_{\mathrm{dp}}\right\rangle\left|0_{\mathrm{dp}}\right\rangle\right)=\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|10\rangle_{34}+|10\rangle_{12}|01\rangle_{34}\right)=\dfrac{1}{\sqrt{2}}\left(|\Psi^{+}\rangle_{13}|\Psi^{+}\rangle_{24}-|\Psi^{-}\rangle_{13}|\Psi^{-}\rangle_{24}\right)\\ |G_4\rangle_{1234}=\dfrac{1}{\sqrt{2}}\left(\left|0_{\mathrm{dp}}\right\rangle\left|1_{\mathrm{dp}}\right\rangle-\left|1_{\mathrm{dp}}\right\rangle\left|0_{\mathrm{dp}}\right\rangle\right)=\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34}\right)=\dfrac{1}{\sqrt{2}}\left(|\Psi^{-}\rangle_{13}|\Psi^{+}\rangle_{24}-|\Psi^{+}\rangle_{13}|\Psi^{-}\rangle_{24}\right)\end{cases}。 \tag{4}$$

2.2 集体旋转噪声

集体旋转噪声对于量子状态的影响可以表示为

$$\begin{cases}U_{\mathrm{r}}|0\rangle=\cos\theta|0\rangle+\sin\theta|1\rangle\\ U_{\mathrm{r}}|1\rangle=-\sin\theta|0\rangle+\cos\theta|1\rangle\end{cases}, \tag{5}$$

式中幺正算子

$$U_r=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}。\tag{6}$$

逻辑粒子$|0\rangle_r=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=|\Phi^+\rangle$,$|1\rangle_r=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)=|\Psi^+\rangle$,以及它们的叠加态

$$\begin{cases}|+_r\rangle=\frac{1}{\sqrt{2}}(|0_r\rangle+|1_r\rangle)=\frac{1}{\sqrt{2}}(|\Phi^+\rangle+|\Psi^-\rangle)\\ |-_r\rangle=\frac{1}{\sqrt{2}}(|0_r\rangle-|1_r\rangle)=\frac{1}{\sqrt{2}}(|\Phi^+\rangle-|\Psi^-\rangle)\end{cases},\tag{7}$$

都可以不受集体旋转噪声的影响。

基于以上理论基础,本文用到的四粒子类GHZ态分别表示为

$$\begin{cases}|L_1\rangle_{1234}=\frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle+|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle)_{1234}=\\ \quad\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}+|\Psi^-\rangle_{12}|\Psi^-\rangle_{34})=\frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle+|1_r\rangle|1_r\rangle)=\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24}+|\Psi^-\rangle_{13}|\Psi^-\rangle_{24})\\ |L_2\rangle_{1234}=\frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle-|0101\rangle+|0110\rangle+|1001\rangle-|1010\rangle)_{1234}=\\ \quad\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}-|\Psi^-\rangle_{12}|\Psi^-\rangle_{34})=\frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle-|1_r\rangle|1_r\rangle)=\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24}+|\Psi^-\rangle_{13}|\Psi^-\rangle_{24})\\ |L_3\rangle_{1234}=\frac{1}{2\sqrt{2}}(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle+|0100\rangle+|0111\rangle-|1000\rangle-|1011\rangle)_{1234}=\\ \quad[12\Phi+12\Psi-34+\Psi-12\Phi+34=120r1r+1r0r=12\Phi-13\Psi+24-\Psi+13\Phi-24]\\ |L_4\rangle_{1234}=\frac{1}{2\sqrt{2}}(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle-|0100\rangle-|0111\rangle+|1000\rangle+|1011\rangle)_{1234}=\\ \quad\frac{1}{\sqrt{2}}(|\Phi^+\rangle_{12}|\Psi^-\rangle_{34}-|\Psi^-\rangle_{12}|\Phi^+\rangle_{34})=\frac{1}{\sqrt{2}}(|0_r\rangle|1_r\rangle-|1_r\rangle|0_r\rangle)=\frac{1}{\sqrt{2}}(|\Phi^-\rangle_{13}|\Psi^+\rangle_{24}-|\Psi^+\rangle_{13}|\Phi^-\rangle_{24})\end{cases}。\tag{8}$$

3　具体方案

假设Alice发送信息给Bob。Charlie为不可信第三方,负责量子的测量,每个逻辑单光子由粒子1和粒子2组成。下文用大写字母区分不同逻辑粒子,带下标的字母表示构成逻辑粒子的实际物理粒子。如逻辑粒子A由粒子A_1和A_2组成。通过式(4)和式(8)可以看出,通过对特定的粒子组合进行Bell测量,就可以确定收到的量子是4种状态中的哪一种,Charlie据此进行测量。

3.1　抗集体退相位噪声的MDI-QSDC协议

1) 准备阶段。Alice制备$n+\sigma$个四粒子GHZ态$|G_2\rangle$、$|G_4\rangle$,每个四粒子GHZ态都由逻辑粒子A、C构成,Alice将其分为序列S_A、S_C,S_A序列中加入m个逻辑单光子E,从$\{|0_{dp}\rangle,|1_{dp}\rangle,|+_{dp}\rangle,|-_{dp}\rangle\}$中任意选择,构成$P_A$。同样地,Bob制备$n+\sigma$个四粒子GHZ态,由$|G_2\rangle$、$|G_4\rangle$任意组成,每个四粒子GHZ态由逻辑粒子$B$、$D$构成,Bob将其分为序列$S_B$、$S_D$,$S_B$序列中加入$m$个逻辑单光子$F$,从$\{|0_{dp}\rangle,|1_{dp}\rangle,|+_{dp}\rangle,|-_{dp}\rangle\}$中任意选择,构成$P_B$。其中,四粒子GHZ态用于编码进行信息的传递,而逻辑单光子E、F作为诱骗光子用于窃听检测。

2) 发送阶段。Alice和Bob分别将P_A和P_B发送给Charlie,同时将S_C和S_D保留在自己手中,用于后续的编码。

3) 测量阶段。Charlie对P_A和P_B中的粒子1和粒子2分别进行Bell测量(如图1所示),并公布结果。对于Charlie进行测量的两个逻辑粒子,Alice和Bob将会分为3种情况进行讨论:

a)如果两个逻辑粒子都来自四粒子纠缠对,那么将其用于编码;

b)如果两个逻辑粒子都来自诱骗光子则用于窃听检测;

c)如果两个逻辑粒子一个来自纠缠对,一个来自诱骗光子则舍弃不用。

根据情况a),通过Charlie的测量,相当于进行了纠缠交换,保留在Alice和Bob手中的S_B和S_D相对应的逻辑粒子形成纠缠:

$$\begin{cases}|G_2\rangle_{AC}|G_2\rangle_{BD}=\frac{1}{2}(|G_1\rangle_{AB}|G_1\rangle_{CD}+|G_2\rangle_{AB}|G_2\rangle_{CD}-|G_3\rangle_{AB}|G_3\rangle_{CD}-|G_4\rangle_{AB}|G_4\rangle_{CD})\\ |G_4\rangle_{AC}|G_4\rangle_{BD}=\frac{1}{2}(|G_1\rangle_{AB}|G_1\rangle_{CD}-|G_2\rangle_{AB}|G_2\rangle_{CD}-|G_3\rangle_{AB}|G_3\rangle_{CD}+|G_4\rangle_{AB}|G_4\rangle_{CD})|G_2\rangle_{AC}\\ |G_4\rangle_{BD}=\frac{1}{2}(|G_1\rangle_{AB}|G_3\rangle_{CD}+|G_2\rangle_{AB}|G_4\rangle_{CD}-|G_3\rangle_{AB}|G_1\rangle_{CD}-|G_4\rangle_{AB}|G_2\rangle_{CD})|G_4\rangle_{AC}\\ |G_2\rangle_{BD}=\frac{1}{2}(|G_1\rangle_{AB}|G_3\rangle_{CD}-|G_2\rangle_{AB}|G_4\rangle_{CD}-|G_3\rangle_{AB}|G_1\rangle_{CD}+|G_4\rangle_{AB}|G_2\rangle_{CD})\end{cases}。\tag{9}$$

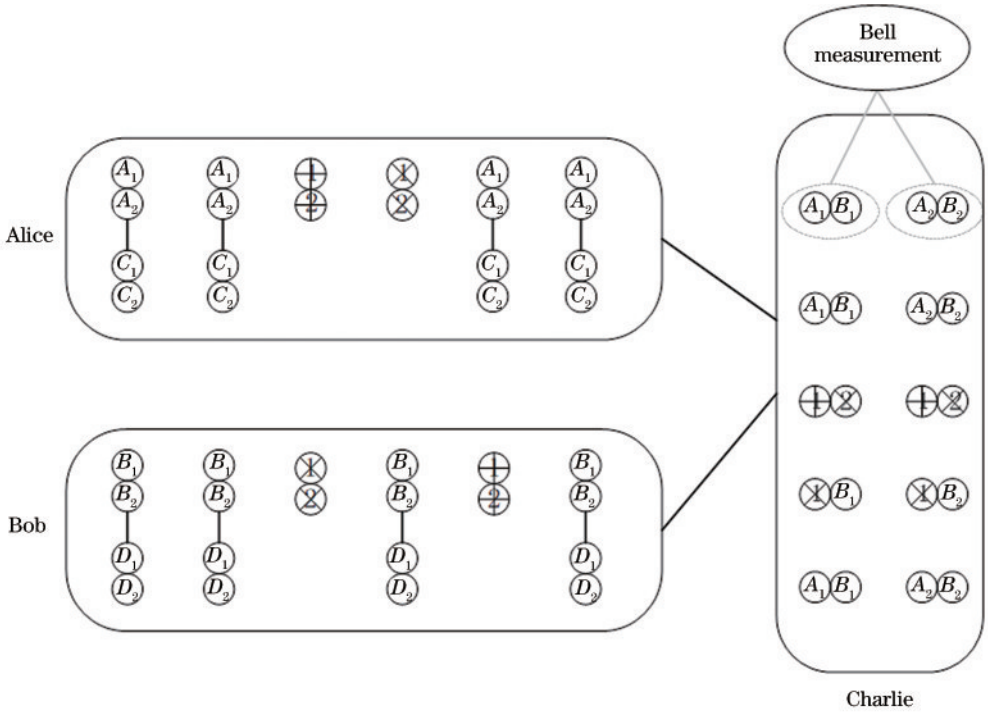

图 1　提出的 MDI-QSDC 的测量过程。A、B、C、D 表示逻辑光子，带数字下标的圆表示实际的粒子。比如逻辑粒子 A 由 A_1 和 A_2 组成。(+)、(×)分别表示 Z 基和 X 基的单光子。圈在一起的两个粒子表示一起执行 Bell 测量

Fig. 1　Measuring process of proposed MDI-QSDC. A, B, C, and D are logical qubits. Circles with numeric subscripts represent physical particles. For example, the logical particle A is composed of A_1 and A_2. (+) and (×) stand for decoy qubits constructed by single photons in Z-basis and X-basis. Photons framed together represent combination of particles to be performed Bell measurement

以上情况如表 1 所示，表中 E 表示来自于纠缠光子，S 表示来自于单光子。

表 1　执行测量时的不同粒子组合所起的作用

Table 1　Effects for measurement of different combinations in communication process of role

Logical photon from C_A	Logical photon from C_B	Function of photons
S	S	Channel eavesdropping detection
E	S	Discard
S	E	
E	E	Entanglement swapping for message coding

4) 安全检测。在 Charlie 公布测量结果后，Alice 和 Bob 分别公布 P_A 和 P_B 中插入诱骗光子的位置，此时应该存在 $m+t$ 对被执行测量的光子其中至少一方是来自诱骗光子的，然后 Alice 和 Bob 交换诱骗光子对应的基，如果 Alice 和 Bob 中对应位置的诱骗光子使用的是不同的测量基，那么这对光子则无法进行安全性检测，因为测量可能会出现全部的 4 种结果[如式(10)]，无法判断是否存在窃听者 Eve；相反，如果 Alice 和 Bob 使用的是相同的测量基，则只可能出现 4 种结果中的 2 种[如式(11)]，在这种情况下，如果 Eve 或者 Charlie 进行测量攻击时就可能会引入错误，从而导致错误率偏高。如果错误率超过阈值则终止通信，否则进行下一步。当 P_A 和 P_B 中的诱骗光子使用不同的基时：

$$\begin{cases} |0_{dp}\rangle|+_{dp}\rangle=\dfrac{1}{\sqrt{2}}\left(|0_{dp}\rangle|0_{dp}\rangle+|0_{dp}\rangle|1_{dp}\rangle\right)=\dfrac{1}{2}\left(|G_1\rangle+|G_2\rangle+|G_3\rangle+|G_4\rangle\right) \\ |0_{dp}\rangle|-_{dp}\rangle=\dfrac{1}{\sqrt{2}}\left(|0_{dp}\rangle|0_{dp}\rangle-|0_{dp}\rangle|1_{dp}\rangle\right)=\dfrac{1}{2}\left(|G_1\rangle+|G_2\rangle-|G_3\rangle-|G_4\rangle\right) \\ |1_{dp}\rangle|+_{dp}\rangle=\dfrac{1}{\sqrt{2}}\left(|1_{dp}\rangle|0_{dp}\rangle+|1_{dp}\rangle|1_{dp}\rangle\right)=\dfrac{1}{2}\left(|G_1\rangle-|G_2\rangle+|G_3\rangle-|G_4\rangle\right) \\ |1_{dp}\rangle|-_{dp}\rangle=\dfrac{1}{\sqrt{2}}\left(|1_{dp}\rangle|0_{dp}\rangle-|1_{dp}\rangle|1_{dp}\rangle\right)=\dfrac{1}{2}\left(-|G_1\rangle+|G_2\rangle+|G_3\rangle-|G_4\rangle\right) \end{cases};\tag{10}$$

当P_A和P_B中的诱骗光子使用相同的基时：

$$\begin{cases}\left|0_{\mathrm{dp}}\right\rangle\left|0_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|G_1\right\rangle_{1234}+\left|G_2\right\rangle_{1234}\right)\\ \left|1_{\mathrm{dp}}\right\rangle\left|1_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|G_1\right\rangle_{1234}-\left|G_2\right\rangle_{1234}\right)\\ \left|0_{\mathrm{dp}}\right\rangle\left|1_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|G_3\right\rangle_{1234}+\left|G_4\right\rangle_{1234}\right)\\ \left|+_{\mathrm{dp}}\right\rangle\left|+_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|G_1\right\rangle_{1234}+\left|G_3\right\rangle_{1234}\right)\\ \left|-_{\mathrm{dp}}\right\rangle\left|-_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|G_1\right\rangle_{1234}-\left|G_3\right\rangle_{1234}\right)\\ \left|+_{\mathrm{dp}}\right\rangle\left|-_{\mathrm{dp}}\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|G_2\right\rangle_{1234}-\left|G_4\right\rangle_{1234}\right)\end{cases}。\tag{11}$$

5）编码阶段。在安全检测阶段后，Alice和Bob剔除掉所有不能形成纠缠的粒子，剩下$n+\delta-t$个逻辑光子。Alice用S_C中剩下的逻辑粒子组成序列M_A，Bob用S_D中剩下的逻辑粒子组成序列M_B。然后Alice对M_A中所有原始状态是$\left|G_2\right\rangle$的逻辑粒子C执行幺正操作$\Omega_x=\delta_x\otimes\delta_x$，其中，$\sigma_x=|1\rangle\langle 0|+|0\rangle\langle 1|$。这样等同于最初Alice制备的所有粒子状态都是$\left|G_4\right\rangle$，而Bob的初始状态包括$\left|G_2\right\rangle$、$\left|G_4\right\rangle$。接下来Alice进行编码，如果编码为0，则对相应的逻辑粒子执行幺正操作$\Omega_I=I\otimes I$，其中，$I=|0\rangle\langle 0|+|1\rangle\langle 1|$；若编码为1，则执行幺正操作$\Omega_x=\delta_x\otimes\delta_x$。为了保证完整性和安全性，Alice利用剩下的单光子进行随意编码，并且打乱顺序构成新的序列M_A'。然后Alice和Bob分别将M_A'和M_B发送给Charlie。

$$\begin{cases}\Omega_I\left|G_2\right\rangle_{1234}=\Omega_I\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|01\rangle_{34}-|10\rangle_{12}|10\rangle_{34}\right)=\\ \quad\dfrac{1}{\sqrt{2}}\left(\left|\Phi^-\right\rangle_{13}\left|\Phi^+\right\rangle_{24}-\left|\Phi^+\right\rangle_{13}\left|\Phi^-\right\rangle_{24}\right)=\left|G_2\right\rangle_{1234}\\ \Omega_x\left|G_2\right\rangle_{1234}=\Omega_x\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|01\rangle_{34}-|10\rangle_{12}|10\rangle_{34}\right)=\\ \quad\dfrac{1}{\sqrt{2}}\left(\left|\Psi^-\right\rangle_{13}\left|\Psi^+\right\rangle_{24}-\left|\Psi^+\right\rangle_{13}\left|\Psi^-\right\rangle_{24}\right)=\left|G_4\right\rangle_{1234}\\ \Omega_I\left|G_4\right\rangle_{1234}=\Omega_I\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34}\right)=\\ \quad\dfrac{1}{\sqrt{2}}\left(\left|\Psi^-\right\rangle_{13}\left|\Psi^+\right\rangle_{24}-\left|\Psi^+\right\rangle_{13}\left|\Psi^-\right\rangle_{24}\right)=\left|G_4\right\rangle_{1234}\\ \Omega_x\left|G_4\right\rangle_{1234}=\Omega_x\dfrac{1}{\sqrt{2}}\left(|01\rangle_{12}|10\rangle_{34}-|10\rangle_{12}|01\rangle_{34}\right)=\\ \quad\dfrac{1}{\sqrt{2}}\left(\left|\Phi^-\right\rangle_{13}\left|\Phi^+\right\rangle_{24}-\left|\Phi^+\right\rangle_{13}\left|\Phi^-\right\rangle_{24}\right)=\left|G_2\right\rangle_{1234}\end{cases}。\tag{12}$$

6）安全性检测和解码阶段。由于纠缠交换，$(M_A'、M_B)$依旧是四粒子GHZ态。Charlie对$(C_1、D_1)$、$(C_2、D_2)$进行Bell测量，并公布测量结果。由于只有Bob知道自己粒子的状态，他可以根据在3）中以及本次的测量结果，根据式(9)进行解码。比如，上一次测量结果为$\left|G_1\right\rangle_{AB}$，这次测量结果为$\left|G_3\right\rangle_{CD}$，而对应的Bob的粒子初态为$\left|G_4\right\rangle_{BD}$，则可以确定Alice对应的粒

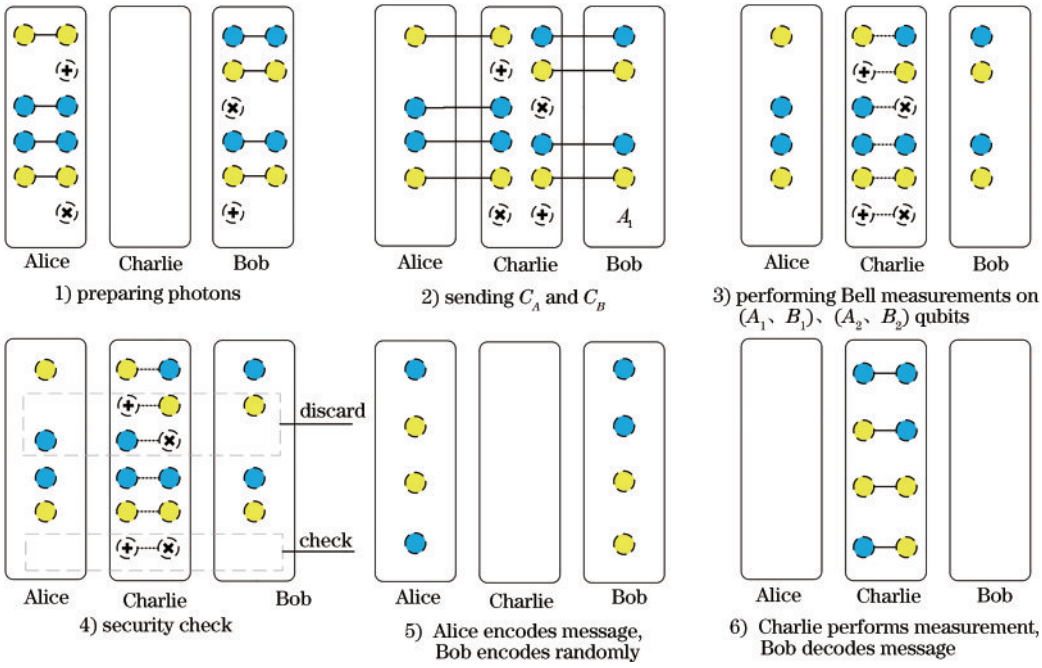

图2　提出的MDI-QSDC的通信过程。虚线圆表示逻辑光子，(+)、(×)表示不同基的诱骗光子。在步骤4)中，标“check”的表示用于窃听检测的情况，标“discard”的表示舍弃不用的情况，其余的用于编码

Fig. 2　Communication process of proposed MDI-QSDC. Circles surrounded by dotted lines represent logical particles. (+), (×) stand for decoy photons. In step 4), photons labeled “check” are used for security check. Photons labeled “discard” mean case of discarding. Remaining ones are for coding message

子为$\left|G_2\right\rangle_{AC}$，则说明编码为1。Alice公布随意插入的编码，Bob据此来检查信息的完整性，并同时进行窃听检测，如果错误率过高则说明有窃听存在，但是由于只有Bob自己知道对M_B所进行的幺正操作，因此窃听者并不会得到任何信息，只能是对通信造成干扰。如果错误率在阈值范围内，则没有窃听，Alice公布正确的编码顺序，通信完成。协议过程如图2所示。

3.2　抗集体旋转噪声的MDI-QSDC协议

由于抗集体旋转噪声的MDI-QSDC协议与抗集体退相位噪声的MDI-QSDC协议的方案过程相同，因此不过多赘述。在此仅描述抗集体旋转噪声的MDI-QSDC与抗集体退相位噪声MDI-QSDC的不同之处，省略相同过程。

1）准备阶段。Alice准备$n+\delta$个四粒子类GHZ态$\left|L_4\right\rangle$，Bob准备$n+\delta$个四粒子类GHZ态，由$\left|L_2\right\rangle$、$\left|L_4\right\rangle$任意组成。诱骗光子从$\left\{\left|0_r\right\rangle,\left|1_r\right\rangle,\left|+_r\right\rangle,\left|-_r\right\rangle\right\}$中任意选择。

2）在测量阶段的情况c)中，发生以下纠缠交换：

$$\begin{cases}\left|L_2\right\rangle_{AC}\left|L_2\right\rangle_{BD}=\dfrac{1}{2}\left(\left|L_1\right\rangle_{AB}\left|L_1\right\rangle_{CD}+\left|L_2\right\rangle_{AB}\left|L_2\right\rangle_{CD}-\left|L_3\right\rangle_{AB}\left|L_3\right\rangle_{CD}-\left|L_4\right\rangle_{AB}\left|L_4\right\rangle_{CD}\right)\\ \left|L_4\right\rangle_{AC}\left|L_4\right\rangle_{BD}=\dfrac{1}{2}\left(\left|L_1\right\rangle_{AB}\left|L_1\right\rangle_{CD}-\left|L_2\right\rangle_{AB}\left|L_2\right\rangle_{CD}-\left|L_3\right\rangle_{AB}\left|L_3\right\rangle_{CD}+\left|L_4\right\rangle_{AB}\left|L_4\right\rangle_{CD}\right)\\ \left|L_2\right\rangle_{AC}\left|L_4\right\rangle_{BD}=\dfrac{1}{2}\left(\left|L_1\right\rangle_{AB}\left|L_3\right\rangle_{CD}+\left|L_2\right\rangle_{AB}\left|L_4\right\rangle_{CD}-\left|L_3\right\rangle_{AB}\left|L_1\right\rangle_{CD}-\left|L_4\right\rangle_{AB}\left|L_2\right\rangle_{CD}\right)\\ \left|L_4\right\rangle_{AC}\left|L_2\right\rangle_{BD}=\dfrac{1}{2}\left(\left|L_1\right\rangle_{AB}\left|L_3\right\rangle_{CD}-\left|L_2\right\rangle_{AB}\left|L_4\right\rangle_{CD}-\left|L_3\right\rangle_{AB}\left|L_1\right\rangle_{CD}+\left|L_4\right\rangle_{AB}\left|L_2\right\rangle_{CD}\right)\end{cases}。\tag{13}$$

3）安全检测阶段。当诱骗光子的基相同时，

$$\begin{cases}\left|0_r\right\rangle\left|0_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|L_1\right\rangle_{1234}+\left|L_2\right\rangle_{1234}\right)\quad\left|1_r\right\rangle\left|1_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|L_1\right\rangle_{1234}-\left|L_2\right\rangle_{1234}\right)\\ \left|0_r\right\rangle\left|1_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|L_3\right\rangle_{1234}+\left|L_4\right\rangle_{1234}\right)\quad\left|+_r\right\rangle\left|+_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|L_1\right\rangle_{1234}+\left|L_3\right\rangle_{1234}\right)\\ \left|-_r\right\rangle\left|-_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|L_1\right\rangle_{1234}-\left|L_3\right\rangle_{1234}\right)\quad\left|+_r\right\rangle\left|-_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|L_2\right\rangle_{1234}-\left|L_4\right\rangle_{1234}\right)\end{cases},\tag{14}$$

当诱骗光子的基不同时，

$$\begin{cases}\left|0_r\right\rangle\left|+_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|0_r\right\rangle\left|0_r\right\rangle+\left|0_r\right\rangle\left|1_r\right\rangle\right)=\dfrac{1}{2}\left(\left|L_1\right\rangle+\left|L_2\right\rangle+\left|L_3\right\rangle+\left|L_4\right\rangle\right)_{1234}\\ \left|0_r\right\rangle\left|-_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|0_r\right\rangle\left|0_r\right\rangle-\left|0_r\right\rangle\left|1_r\right\rangle\right)=\dfrac{1}{2}\left(\left|L_1\right\rangle+\left|L_2\right\rangle-\left|L_3\right\rangle-\left|L_4\right\rangle\right)_{1234}\\ \left|1_r\right\rangle\left|+_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|1_r\right\rangle\left|0_r\right\rangle+\left|1_r\right\rangle\left|1_r\right\rangle\right)=\dfrac{1}{2}\left(\left|L_1\right\rangle-\left|L_2\right\rangle+\left|L_3\right\rangle-\left|L_4\right\rangle\right)_{1234}\\ \left|1_r\right\rangle\left|-_r\right\rangle=\dfrac{1}{\sqrt{2}}\left(\left|1_r\right\rangle\left|0_r\right\rangle-\left|1_r\right\rangle\left|1_r\right\rangle\right)=\dfrac{1}{2}\left(-\left|L_1\right\rangle+\left|L_2\right\rangle+\left|L_3\right\rangle-\left|L_4\right\rangle\right)_{1234}\end{cases}。\tag{15}$$

4）编码阶段。首先Alice对原始状态为$\left|L_2\right\rangle$的逻辑粒子C进行幺正操作$\Theta_x=\sigma_z\otimes\sigma_x$，其中$\sigma_z=\left|0\right\rangle\left\langle0\right|-\left|1\right\rangle\left\langle1\right|$。等同于Alice最初制备的状态均为$\left|L_4\right\rangle$，而Bob所包含的粒子状态包括$\left|L_2\right\rangle$和$\left|L_4\right\rangle$。之后Alice进行编码，编码为0时进行幺正操作$\Theta_I=I\otimes I$，编码为1时进行幺正操作$\Theta_x=\sigma_z\otimes\sigma_x$。

$$\Theta_I\left|L_2\right\rangle_{1234}=\Theta_I\frac{1}{2\sqrt{2}}\left(\left|0000\right\rangle+\left|0011\right\rangle+\left|1100\right\rangle+\left|1111\right\rangle-\left|0101\right\rangle+\left|0110\right\rangle+\left|1001\right\rangle-\left|1010\right\rangle\right)_{1234}=$$
$$\frac{1}{2\sqrt{2}}\left(\left|0000\right\rangle+\left|0011\right\rangle+\left|1100\right\rangle+\left|1111\right\rangle-\left|0101\right\rangle+\left|0110\right\rangle+\left|1001\right\rangle-\left|1010\right\rangle\right)_{1234}=\frac{1}{\sqrt{2}}$$
$$\left(\left|\Phi^+\right\rangle_{12}\left|\Phi^+\right\rangle_{34}-\left|\Psi^-\right\rangle_{12}\left|\Psi^-\right\rangle_{34}\right)=\frac{1}{\sqrt{2}}\left(\left|\Phi^-\right\rangle_{13}\left|\Phi^-\right\rangle_{24}+\left|\Psi^+\right\rangle_{13}\left|\Psi^+\right\rangle_{24}\right)=\left|L_2\right\rangle_{1234},$$

$$\Theta_x\left|L_2\right\rangle_{1234}=\Theta_x\frac{1}{2\sqrt{2}}\left(\left|0000\right\rangle+\left|0011\right\rangle+\left|1100\right\rangle+\left|1111\right\rangle-\left|0101\right\rangle+\left|0110\right\rangle+\left|1001\right\rangle-\left|1010\right\rangle\right)_{1234}=$$
$$\frac{1}{2\sqrt{2}}\left(\left|0001\right\rangle-\left|0010\right\rangle+\left|1101\right\rangle-\left|1110\right\rangle-\left|0100\right\rangle-\left|0111\right\rangle+\left|1000\right\rangle+\left|1011\right\rangle\right)_{1234}=$$
$$\frac{1}{\sqrt{2}}\left(\left|\Phi^+\right\rangle_{12}\left|\Psi^-\right\rangle_{34}-\left|\Psi^-\right\rangle_{12}\left|\Phi^+\right\rangle_{34}\right)=\frac{1}{\sqrt{2}}\left(\left|\Phi^-\right\rangle_{13}\left|\Psi^+\right\rangle_{24}-\left|\Psi^+\right\rangle_{13}\left|\Phi^-\right\rangle_{24}\right)=\left|L_4\right\rangle_{1234},$$

$$\Theta_I\left|L_4\right\rangle_{1234}=\Theta_I\frac{1}{2\sqrt{2}}\left(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle-|0100\rangle-|0111\rangle+|1000\rangle+|1011\rangle\right)_{1234}=$$
$$\frac{1}{2\sqrt{2}}\left(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle-|0100\rangle-|0111\rangle+|1000\rangle+|1011\rangle\right)_{1234}=\frac{1}{\sqrt{2}}$$
$$\left(|\Phi^+\rangle_{12}|\Psi^-\rangle_{34}-|\Psi^-\rangle_{12}|\Phi^+\rangle_{34}\right)=\frac{1}{\sqrt{2}}\left(|\Phi^-\rangle_{13}|\Psi^+\rangle_{24}-|\Psi^+\rangle_{13}|\Phi^-\rangle_{24}\right)=\left|L_4\right\rangle_{1234},$$
$$\Theta_x\left|L_4\right\rangle_{1234}=\Theta_x\frac{1}{2\sqrt{2}}\left(|0001\rangle-|0010\rangle+|1101\rangle-|1110\rangle-|0100\rangle-|0111\rangle+|1000\rangle+\right.$$
$$\left.|1011\rangle\right)_{1234}=\frac{1}{2\sqrt{2}}\left(|0000\rangle+|0011\rangle+|1100\rangle+|1111\rangle-|0101\rangle+|0110\rangle+|1001\rangle-|1010\rangle\right)_{1234}=$$
$$\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{12}|\Phi^+\rangle_{34}-|\Psi^-\rangle_{12}|\Psi^-\rangle_{34}\right)=\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{13}|\Phi^+\rangle_{24}+|\Psi^-\rangle_{13}|\Psi^-\rangle_{24}\right)=\left|L_2\right\rangle_{1234}。\tag{16}$$

4 安全性分析

4.1 测量攻击

在本文的MDI-QSDC协议中，Charlie作为不可信的第三方，与潜在的窃听者是一体的。当Charlie想要窃取Alice和Bob之间传递的信息时，他可以有两种方式。

一是Charlie直接实施窃听操作，那么在4)的窃听检测阶段中可能被发现，因为Charlie的窃听行为会引入错误，在Alice和Bob公布自己插入诱骗单光子的位置和状态后，对于使用相同测量基的粒子有50%的可能性出现非法状态。一旦错误率超过阈值，此次通信便终止了。此外，在发送序列M_A'和M_B前，Bob对M_B中的光子随机地进行酉变操作，而对应哪些光子，只有Bob自己知道，因此Charlie是无法窃取到信息的。

二是Charlie假装对P_A和P_B进行了Bell测量并且宣布错误的结果。由于在编码测量前，Alice对M_A中所有原始状态是$\left|G_2\right\rangle$的逻辑粒子C执行幺正操作。经过这样的操作后，等同于Alice最初制备的所有粒子状态都是$\left|G_4\right\rangle$，所以Charlie这样做可以使P_A、P_B以及S_C、S_D保持状态保持不变，进而可以窃取信息的编码操作。但这种手段同样也是不可行的，因为Charlie在公布结果时并不能知道哪些位置是单光子，哪些是纠缠光子，错误率同样会上升，从而被Alice和Bob发现并终止通信。

4.2 特洛伊木马攻击

本文所提出的两个免疫集体噪声的MDI-QSDC中的所有粒子在信道中都只进行了一次性传输，因此窃听者无法对其进行特洛伊木马攻击。所以本文的协议可以不使用任何设备就能抵抗特洛伊木马攻击[30]。

4.3 纠缠测量攻击

在通信过程中，假如Eve想要执行纠缠测量攻击，则他需要利用攻击光子$|e\rangle_E$，并且对截获的信道中的光子执行辅助操作U_E使之产生纠缠[31]，以集体退相位噪声为例，则结果如下：

$$\begin{cases}
U_E\left|0_{\mathrm{dp}}\right\rangle|e\rangle_E=a_0|00\rangle|e_{00}\rangle_E+b_0|01\rangle|e_{01}\rangle_E+c_0|0\rangle|e_{10}\rangle_E+d_0|1\rangle|e_{11}\rangle_E\\
U_E\left|1_{\mathrm{dp}}\right\rangle|e\rangle_E=a_1|00\rangle|e'_{00}\rangle_E+b_1|01\rangle|e'_{01}\rangle_E+c_1|0\rangle|e'_{10}\rangle_E+d_1|1\rangle|e'_{11}\rangle_E\\
U_E\left(\left|+_{\mathrm{dp}}\right\rangle|e\rangle_E\right)=\frac{1}{\sqrt{2}}\left(U_E\left|0_{\mathrm{dp}}\right\rangle|e\rangle_E+U_E\left|1_{\mathrm{dp}}\right\rangle|e\rangle_E\right)=\frac{1}{2}\left[|\Phi^+\rangle\left(a_0|e_{00}\rangle_E+d_0|e_{11}\rangle_E+a_1|e'_{00}\rangle_E+d_1|e'_{11}\rangle_E\right)+\right.\\
\quad|\Phi^-\rangle\left(a_0|e_{00}\rangle_E-d_0|e_{11}\rangle_E+a_1|e'_{00}\rangle_E-d_1|e'_{11}\rangle_E\right)+|\Psi^+\rangle\left(b_0|e_{01}\rangle_E+c_0|e_{10}\rangle_E+b_1|e'_{01}\rangle_E+c_1|e'_{10}\rangle_E\right)+\\
\quad\left.|\Psi^-\rangle\left(b_0|e_{01}\rangle_E-c_0|e_{10}\rangle_E+b_1|e'_{01}\rangle_E-c_1|e'_{10}\rangle_E\right)\right]\\
U_E\left(\left|-_{\mathrm{dp}}\right\rangle|e\rangle_E\right)=\frac{1}{\sqrt{2}}\left(U_E\left|0_{\mathrm{dp}}\right\rangle|e\rangle_E-U_E\left|1_{\mathrm{dp}}\right\rangle|e\rangle_E\right)=\frac{1}{2}\left[|\Phi^+\rangle\left(a_0|e_{00}\rangle_E+d_0|e_{11}\rangle_E-a_1|e'_{00}\rangle_E-d_1|e'_{11}\rangle_E\right)+\right.\\
|\Phi^-\rangle\left(a_0|e_{00}\rangle_E-d_0|e_{11}\rangle_E-a_1|e'_{00}\rangle_E+d_1|e'_{11}\rangle_E\right)+|\Psi^+\rangle\left(b_0|e_{01}\rangle_E+c_0|e_{10}\rangle_E-b_1|e'_{01}\rangle_E-c_1|e'_{10}\rangle_E\right)+\\
\left.|\Psi^-\rangle\left(b_0|e_{01}\rangle_E+c_0|e_{10}\rangle_E-b_1|e'_{01}\rangle_E-c_1|e'_{10}\rangle_E\right)\right]
\end{cases},\tag{17}$$

式中，$|a_0|^2+|b_0|^2+|c_0|^2+|d_0|^2=1$，$|a_1|^2+|b_1|^2+|c_1|^2+|d_1|^2=1$。Eve如果想要在此过程中避免引入错误，那么辅助攻击U_E就必须要满足：$a_0=c_0=d_0=0$，$a_1=b_1=d_1=0$，$\left|e_{01}\right\rangle_E=|e'_{10}\rangle_E$，可以看出，当攻击粒子与目标粒子为直积状态时可以避免引入错误，然而此时，Eve也无法获得有用的信息。

5 结 论

提出了两个分别可以抵抗集体退相位噪声和集体旋转噪声的MDI-QSDC协议，该协议通过纠缠粒子对有效地消除了测量设备缺陷造成的漏洞，这些漏洞已经威胁到了实际QSDC系统的安全。此外通过逻辑粒子抵抗信道中集体噪声的影响。在实际的应用中，不同的条件和场景对信息安全的等级有不同的要求和等级。提出的MDI-QSDC协议同其他各种新生的协议一样，为不同的应用场景提供新的选择。

参 考 文 献

[1] Bennett C H. Quantum cryptography using any two nonorthogonal states[J]. Physical Review Letters, 1992, 68(21): 3121-3124.

[2] Grosshans F, van Assche G, Wenger J, et al. Quantum key distribution using Gaussian-modulated coherent states [J]. Nature, 2003, 421(6920): 238-241.

[3] Lo H K, Ma X F, Chen K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23): 230504.

[4] Wang C, Yin Z Q, Wang S, et al. Measurement-device-independent quantum key distribution robust against environmental disturbances[J]. Optica, 2017, 4(9): 1016-1023.

[5] Yuan G J F, Lu F Y, Wang S, et al. Measurement-device-independent quantum key distribution for nonstandalone networks[J]. Photonics Research, 2021, 9 (10): 1881-1891.

[6] Wang S, He D Y, Yin Z Q, et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system[J]. Physical Review X, 2019, 9(2): 021046.

[7] Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre[J]. Nature Photonics, 2022, 16(2): 154-161.

[8] Gottesman D. Theory of quantum secret sharing[J]. Physical Review A, 2000, 61(4): 042311.

[9] Shi R H, Zhong H. Multiparty quantum secret sharing with the pure entangled two-photon states[J]. Quantum Information Processing, 2012, 11(1): 161-169.

[10] Zhou N, Zeng G, Xiong J. Quantum key agreement protocol[J]. Electronics Letters, 2004, 40(18): 1149-1150.

[11] 唐杰, 石磊, 魏家华, 等. 免疫集体噪声的量子密钥协商协议[J]. 激光与光电子学进展, 2020, 57(17): 172703.
Tang J, Shi L, Wei J H, et al. Quantum key agreement protocols immune to collective noise[J]. Laser & Optoelectronics Progress, 2020, 57(17): 172703.

[12] 何业锋, 陈思昊, 强雨薇, 等. 一种基于量子稠密编码的电子支付协议[J]. 光学学报, 2021, 41(10): 1027001.
He Y F, Chen S H, Qiang Y W, et al. Electronic payment protocol based on quantum dense coding[J]. Acta Optica Sinica, 2021, 41(10): 1027001.

[13] 王俊辉, 李云霞, 蒙文, 等. 基于两粒子和三粒子最大纠缠态的量子盲签名协议[J]. 激光与光电子学进展, 2021, 58(7): 0727002.
Wang J H, Li Y X, Meng W, et al. Protocol of quantum blind signature based on two-qubit and three-qubit maximally entangled states[J]. Laser & Optoelectronics Progress, 2021, 58(7): 0727002.

[14] Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme[J]. Physical Review A, 2002, 65(3): 032302.

[15] Boström K, Felbinger T. Deterministic secure direct communication using entanglement[J]. Physical Review Letters, 2002, 89(18): 187902.

[16] Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. Physical Review A, 2003, 68(4): 042317.

[17] Deng F G, Long G L. Secure direct communication with a quantum one-time pad[J]. Physical Review A, 2004, 69 (5): 052319.

[18] Deng F G, Li X H, Li C Y, et al. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs[J]. Physics Letters A, 2006, 359(5): 359-365.

[19] Chen S S, Zhou L, Zhong W, et al. Three-step three-party quantum secure direct communication[J]. Science China Physics, Mechanics & Astronomy, 2018, 61(9): 090312.

[20] Jin X R, Ji X, Zhang Y Q, et al. Three-party quantum secure direct communication based on GHZ states[J]. Physics Letters A, 2006, 354(1/2): 67-70.

[21] Man Z X, Xia Y J. Improvement of security of three-party quantum secure direct communication based on GHZ states[J]. Chinese Physics Letters, 2007, 24(1): 15-18.

[22] Wang T J, Li T, Du F F, et al. High-capacity quantum secure direct communication based on quantum hyperdense coding with hyperentanglement[J]. Chinese Physics Letters, 2011, 28(4): 040305.

[23] Yang C W, Hwang T. Fault tolerant authenticated quantum direct communication immune to collective noises[J]. Quantum Information Processing, 2013, 12 (11): 3495-3509.

[24] Yang Y Y. A quantum secure direct communication protocol without quantum memories[J]. International Journal of Theoretical Physics, 2014, 53(7): 2216-2221.

[25] Li J, Song D J, Li R F, et al. A quantum secure direct communication protocol based on four-qubit cluster state [J]. Security and Communication Networks, 2015, 8(1): 36-42.

[26] He Y F, Ma W P. Three-party quantum secure direct communication against collective noise[J]. Quantum Information Processing, 2017, 16(10): 252.

[27] Niu P H, Zhou Z R, Lin Z S, et al. Measurement-device-independent quantum communication without encryption [J]. Science Bulletin, 2018, 63(20): 1345-1350.

[28] Zhou Z R, Sheng Y B, Niu P H, et al. Measurement-device-independent quantum secure direct communication [J]. Science China Physics, Mechanics & Astronomy, 2019, 63(3): 230362.

[29] 吴贵铜, 周南润, 龚黎华, 等. 集体噪声信道上带身份认证的无信息泄露的量子对话协议[J]. 物理学报,

2014, 63(6): 060302.
Wu G T, Zhou N R, Gong L H, et al. Quantum dialogue protocols with identification over collection noisy channel without information leakage[J]. Acta Physica Sinica, 2014, 63(6): 060302.
[30] Jain N, Stiller B, Khan I, et al. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems[J]. IEEE Journal of Selected Topics in Quantum Electronics, 2015, 21(3): 168-177.
[31] Tang J, Shi L, Wei J H, et al. Novel multi-party quantum key agreement protocols under collective noise [J]. Modern Physics Letters B, 2021, 35(8): 2150137.