第 58 卷 第 9 期/2021 年 5 月/激光与光电子学进展 研究论文

激光与光电子学进展

基于EPR态的罗兰C台识别码保密传输

赵露涵，杨春燕*，陈超，罗均文

空军工程大学信息与导航学院，陕西 西安 710077

摘要 罗兰C系统中台站相位码的识别和保密传输是判断台链及接收信号进行双曲线定位的前提。针对使用经典手段无法实现罗兰C系统高保密性传输的问题，提出了基于EPR态量子纠缠信号的相位码传输方案，并分析了该方案在纠缠攻击与分光镜攻击下的安全性，得到了信息传输效率与分光镜的透射系数、压缩度的关系，验证了该方案可以有效提高罗兰C系统中主副台间的台识别码传输的保密性。

关键词 量子光学；罗兰C；双模压缩态；台识别码；保密传输

中图分类号 O413.2 **文献标志码** A **doi**：10.3788/LOP202158.0927002

Secure Transmission of Identification Code in Loran C Station Based on EPR States

Zhao Luhan, Yang Chunyan*, Chen Chao, Luo Junwen

Information and Navigation College, Air Force Engineering University, Xi'an, Shaanxi 710077, *China*

Abstract The identification and secure transmission of the station phase codes in the Loran C system are the premise of judging chains and receiving signals for hyperbolic positioning. Aiming at the problem that the Loran C system cannot achieve high security transmission by classical means, we propose a phase code transmission scheme based on EPR state quantum signals and analyse the security of this scheme under the entanglement attack and spectroscopic attack. The relationship between the information transmission efficiency and the transmission coefficient of the spectroscope as well as that between the information transmission efficiency and the compression degree of the spectroscope is obtained, which verifies that the proposed scheme can effectively improve the security of phase code transmission between the main station and the secondary station in the Loran C system.

Key words quantum optics; Loran C; two mode squeezed states; station identification code; secure transmission

OCIS codes 270.6570; 270.5585

1 引 言

罗兰C系统是陆基低频无线电导航系统[1]，采用的是双曲线定位原理，飞机利用主、副台脉冲到达的时间差与相位差来确定位置，主副台间的脉冲包络与载频相位应有严格的同步关系，因此罗兰C系统中台站相位码的识别和保密传输是判断台链以及接收信号进行双曲线定位的前提[2-3]。有学者提出在罗兰C系统中运用全相位谱分析方法和基于神经网络的附加二次相位因子(additional second-phase factors，ASF)修正方法。这些方法能在高噪声背景下准确地识别出台站相位码并进行抗干扰快速检测[4-6]，但是没有涉及台识别码的保密性传输，而调制到载波上的导航数据是高度可预测的，

收稿日期：2020-09-02；**修回日期**：2020-09-19；**录用日期**：2020-09-30

基金项目：国家自然科学基金(61573372)

***E-mail**：ycy220@163.com

如果不对罗兰C信号采取任何保密措施，战时条件下台站无法辨识自由空间中无线电信号的真伪，极易受到敌方的欺骗，其正常导航活动受到扰乱，因此罗兰C台识别码的保密性研究具有十分重要的意义。

近年来，量子保密通信发展迅速，通过单光子的偏振和自旋来实现离散变量量子密钥分配（discrete variable quantum key distribution，DVQKD）的方案相继被提出[7-8]，但是信息传输效率普遍不高，信道容量偏低。因此，连续变量量子密钥分配[9-12]（continuous-variable quantum key distribution，CVQKD）引起了人们的广泛关注。连续变量的量子密码术以纠缠光束作为信息载体，虽然压缩度受传输介质损耗的影响比较大，但其单信号具有大容量编码和较高的信息传输与探测效率，有助于实现大信息量的保密通信[13]。何广强等[14-15]利用连续变量纠缠态，提出了一个量子安全直接通信（quantum secure direct communication，QSDC）协议。相比QKD方案，QSDC方案无需产生量子密钥，可以直接安全地传输秘密信息，提高了通信效率。因此，基于连续变量的量子安全直接通信可以兼具以上优点，具有很强的研究价值和实用性。同时，QSDC方案相较于现有的量子身份认证方案，省去了第三方验证过程，有效简化了通信流程，提高了通信效率[16]。

本文提出了基于双模压缩态实现罗兰C系统台识别码保密传输的方案。双模压缩真空态是一种EPR态，连续变量的量子纠缠特性及在随机时隙处插入的诱骗态信息保证了该方案的安全性。安全性分析结果显示，该方案可以实现台识别码的安全传输，为罗兰C系统提供了较好的信息保护效果。

2　罗兰C系统主副台识别码

罗兰C脉冲信号的载频是100 kHz，脉冲电流$i_0(t)$的表达式为

$$i_0(t)=A(t-\tau)^2\exp\left[-2\frac{(t-\tau)}{65}\right]\sin(0.2\pi t+p_0),\quad(1)$$

式中：p_0为脉冲信号的初相位，0°时用“＋”表示，180°时用“－”表示；A为归一化常数；t为时间；τ为包周差（ECD）。

在罗兰C系统的一个台链中，为了识别主副台的信号，系统采用的是脉冲组的发射形式，如图1所示，主台每一组有9个脉冲，前8个脉冲的间隔为1000 μs，第9个脉冲与前一个脉冲间隔为2000 μs；副台每一组里有8个脉冲，间隔时间为1000 μs。主台、副台的台识别码是不同的，因此具有不同的初相位，初相位的相位码识别是判断主台和副台并建立初同步的关键。传统罗兰C系统进行主台台站识别时，主台先发射脉冲信号，副台收到脉冲信号后，与自身内部产生的主台基准信号作比对，如果正确则会有超过某个门限值的最大值输出，副台识别出主台。由于主台台识别码在空间传输过程中可被敌方轻易获取，如果不采取任何保密措施，一旦敌方捕获识别码并利用其进行误导，罗兰C系统就无法进行准确定位，这会给导航活动带来极大的风险。

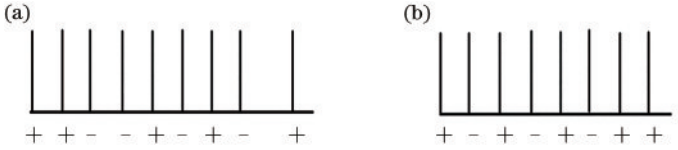

图1　罗兰C台站脉冲信号的相位码。(a)主台；(b)副台

Fig. 1　Phase codes of pulse signals in Loran C station. (a) Main station; (b) secondary station

3　基于EPR态的台站相位码及传输方案

3.1　相位码规则

在传统罗兰C系统中，主副台分别采用9个和8个脉冲。所提方案是在原有脉冲设置的基础上，采用了以6个相位码为一组的传输形式，既满足了相位码的保密性传输，又满足了一定的传输效率。如果以8或10个相位码为一组，一次传输即可完成整个台站相位码的传输，一旦敌方进行拦截攻击，一次即可获取全部的台站相位码，因此采用较长的相位码不利于保密性传输。如果以2或4个相位码为一组，那么需要多次传输才能完成整个台站相位码的传输，效率较低。

为了使罗兰C系统中的副台更准确快速识别主台，主副台间必须共享一套编码规则。使用二进制编码“1”、“0”分别表示主副台脉冲信号的“＋”、“－”，编码区间大致规定为$(-\infty,-3]$，$(-3,-2]$，$(-2,-1]$，$(-1,0]$，$(0,1]$，$(1,2]$，$(2,3]$，$(3,+\infty]$，如图2所示，且每个编码区间对应3 bit信息。若主台

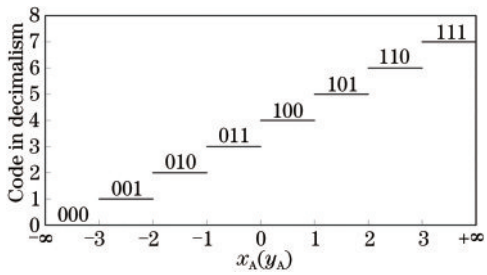

图 2　相位码规则

Fig. 2　Phase code rule

需要将一组相位码 110010 发送给副台，根据编码规则，有 $(2,3]\rightarrow 110$，$(-2,-1]\rightarrow 010$，则 110010 对应 $x_A\in(2,3]$，$y_A\in(-2,-1]$。在基于 EPR 态的相位码传输过程中，可以通过平移操作 $D_A(x_A+\mathrm{i}y_A)$ 将信息 x_A 与 y_A 编码到纠缠光学模中。

3.2　基于 EPR 态的罗兰 C 台站相位码传输方案

相位码的保密传输过程如图 3 所示，其中 a_A 表示载有相位码信息的光学模，a_M 表示载有诱骗信息的光模，g 表示线性放大器。以二进制方式将台识别码随机编码在双模压缩态中，采用正交振幅和正交相位作为观测参量，通过比对纠缠度的变化，判断敌方是否存在窃听行为，进而保护台识别码信息的安全。由于主副台位置固定，因此主副台之间可以进行光缆铺设，光缆中的光纤作为量子信道和经典信道可传输光学模。

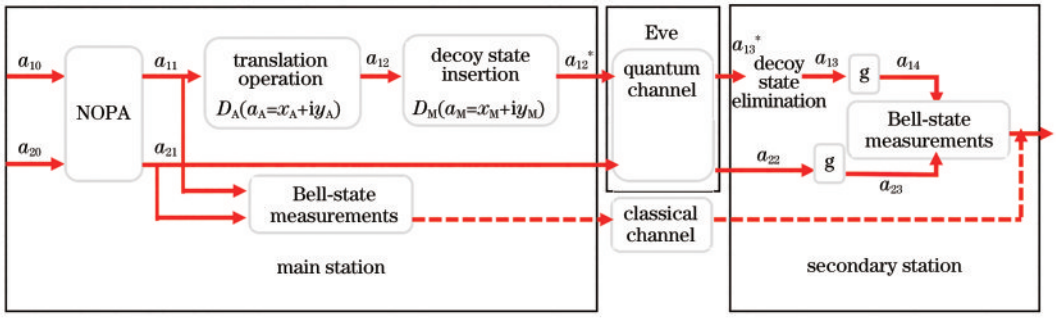

图 3　基于 EPR 态的罗兰 C 台相位码传输框图

为了制备双模压缩真空态，将两个光学模真空态输入至非简并光学参量放大器（NOPA）中以产生两个纠缠光束。$S(r,\varphi)$ 为双模压缩算符，输入与输出的表达式为

$$\begin{cases} a_{11}=S(r,\phi)^{+}a_{10}S(r,\phi)=a_{10}\cosh(r)+a_{20}^{+}\sinh(r) \\ a_{21}=S(r,\phi)^{+}a_{20}S(r,\phi)=a_{20}\cosh(r)+a_{10}^{+}\sinh(r) \end{cases}, \tag{2}$$

式中：r 为压缩幅；ϕ 为压缩角；$S(r,\phi)^{+}$ 为 $S(r,\varphi)$ 的产生算符；a_{10} 和 a_{20} 为两个真空态；a_{11} 和 a_{21} 为双模压缩真空态；a_{20}^{+} 与 a_{10}^{+} 分别为 a_{20} 与 a_{10} 的产生算符。双模压缩算符表达式为

$$S(r,\phi)=\exp\left[r\exp(-\mathrm{i}\phi)a_{10}a_{20}-r\exp(\mathrm{i}\phi)a_{10}^{+}a_{20}^{+}\right], \tag{3}$$

式中：$r\exp(-\mathrm{i}\phi)$ 为压缩参量。信号的正交分量振幅和相位表示为

$$\begin{cases} X_{a_{11}}=X_{a_{10}}\cosh(r)+X_{a_{10}}\sinh(r) \\ X_{a_{21}}=X_{a_{20}}\cosh(r)+X_{a_{10}}\sinh(r) \\ P_{a_{11}}=P_{a_{10}}\cosh(r)-P_{a_{20}}\sinh(r) \\ P_{a_{21}}=P_{a_{20}}\cosh(r)-P_{a_{10}}\sinh(r) \end{cases}, \tag{4}$$

式中：$X_{a_{11}}$、$X_{a_{10}}$、$X_{a_{21}}$、$X_{a_{20}}$ 分别为光学模 a_{11}、a_{10}、a_{21}、a_{20} 的正交振幅分量；$P_{a_{11}}$、$P_{a_{10}}$、$P_{a_{21}}$、$P_{a_{20}}$ 分别为光学模 a_{11}、a_{10}、a_{21}、a_{20} 的正交相位分量。当 $r\rightarrow+\infty$ 时，双模压缩真空态 $X_{a_{11}}$ 与 $X_{a_{21}}$ 正相关，$P_{a_{11}}$ 与 $P_{a_{21}}$ 负相关，即

$$\begin{cases} \lim\limits_{r\rightarrow+\infty}X_{a_{11}}=X_{a_{21}} \\ \lim\limits_{r\rightarrow+\infty}P_{a_{11}}=-P_{a_{21}} \end{cases}。 \tag{5}$$

该方案可分为两个阶段，第一阶段验证通信双方是否建立了可靠的量子通信信道，为下一阶段主台相位码量子信息的传输提供安全性检验。

1）主台将真空态光学模 a_{10} 和 a_{20} 输入到 NOPA 以制备出双模压缩态 a_{11} 和 a_{21}，并直接对其进行 Bell 基联合测量，通过经典信道告知副台测量结果 X_{u0} 和 P_{u0}：

$$\begin{cases} X_{u0}=\dfrac{1}{\sqrt{2}}\left(X_{a_{11}}-X_{a_{21}}\right) \\ P_{u0}=\dfrac{1}{\sqrt{2}}\left(P_{a_{11}}+P_{a_{21}}\right) \end{cases}。 \tag{6}$$

2)主台用同样的方式再制备一对相同的双模压缩态 a_{11} 和 a_{21},主台保留光学模 a_{11},另一路光学模 a_{21} 通过量子信道发给副台。

3)副台通过经典信道告知主台收到的光学模 a_{22}。

4)主台随机选择时隙 τ_1 并对光学模 a_{11} 的正交分量振幅或相位进行测量,并公布所选取的时隙、测量的分量及结果。

5)副台选择主台公布的测量分量,在 τ_1 时隙处对 a_{22} 进行测量,并对结果进行比较。若结果基本一致,则副台确定该信道是安全的,通过经典信道告知主台,并将继续进行相位编码的实际传输。

第二阶段是相位码的实际传输阶段,方案通过加入诱骗态操作,可以有效抵御纠缠测量攻击,确保信道的安全性和信息传输的保密性。协议将罗兰C台脉冲信号的相位码进行分组传输,每次传输6个相位码即6 bit的信息,副台验证比特信息正确后才会开始下一组的传送,如果发现相位码被窃听,敌方也不会获取全部的台识别码,此时主台将结束此次传送[17]。

6)主台将自身的相位码进行分组传输。假设要传输的相位码为110010,参照统一的编码规则,秘密信息110和010分别对应$(2,3]$和$(-2,-1]$,主台选择随机变量 $x_A\in(2,3]$,$y_A\in(-2,-1]$,在随机时隙 τ_2 处对 a_{11} 进行平移操作 $D_A(x_A+\mathrm{i}y_A)$ 以生成 a_{12},并通过经典信道将所选择的时隙 τ_2 告知副台。

7)主台插入诱骗态[18],即在随机时隙 τ_3 处对 a_{12} 进行诱骗态平移操作 $D_M(x_M+\mathrm{i}y_M)$ 以生成 a_{12}^*,其中 x_M 和 y_M 为诱骗信息根据编码规则对应的码值。

8)主台通过量子信道将 a_{12}^* 发送给副台并公布时隙 τ_3。平移算符 D_A 和 D_M 作用于光学模,即

$$\begin{cases} a_{12}=D_A^{+}a_{11}D_A \\ a_{12}^*=D_M^{+}a_{12}D_M \end{cases}, \tag{7}$$

式中:D_A^{+} 为平移算符 D_A 的产生算符;D_M^{+} 为 D_M 的产生算符。可以得到

$$\begin{cases} X_{a_{12}}=X_{a_{11}}+x_A \\ X_{a_{12}^*}=X_{a_{12}}+x_M \end{cases}, \tag{8}$$

式中:$X_{a_{12}}$ 为光学模 a_{12} 的正交振幅分量;$X_{a_{12}^*}$ 为 a_{12}^* 的正交振幅分量。

9)副台接收到光学模 a_{13}^* 后,在时隙 τ_3 处对它的正交分量振幅或相位进行测量,并通过经典信道告知主台测量结果。

10)根据测量结果,主台判断信道是否安全。如果信道安全,那么主台通过经典信道将诱骗态 $D_M(x_M+\mathrm{i}y_M)$ 发送给副台,否则主台将终止此次相位码的传输。

11)副台将诱骗态 $D_M(x_M+\mathrm{i}y_M)$ 从 a_{13}^* 中剔除以得到 a_{13},并通过增益为 $g=\dfrac{1}{\sqrt{\eta_0}}$ 的线性放大器(η_0 为主副台量子信道的传输效率)对纠缠模 a_{13} 和 a_{22} 进行还原放大,产生 a_{14} 和 a_{23}。副台在时隙 τ_2 处对纠缠光学模 a_{14} 和 a_{23} 进行联合Bell基测量,得到的结果为

$$\begin{cases} X_{u1}=\dfrac{1}{\sqrt{2}}\left(X_{a_{14}}-X_{a_{23}}\right)=\dfrac{1}{\sqrt{2}}\left(X_{a_{11}}+X_{x_A}-X_{a_{21}}\right) \\ P_{u1}=\dfrac{1}{\sqrt{2}}\left(P_{a_{14}}+P_{a_{23}}\right)=\dfrac{1}{\sqrt{2}}\left(P_{a_{11}}+P_{y_A}+P_{a_{21}}\right) \end{cases}, \tag{9}$$

式中:X_{u1} 为副台剔除诱骗态信息后测量的正交振幅;$X_{a_{14}}$、$X_{a_{23}}$ 分别为光学模 a_{14}、a_{23} 的正交振幅分量;X_{x_A} 为含有相位码信息的光学模 x_A 的正交振幅分量;P_{u1} 为副台剔除诱骗态信息后测量的正交相位;$P_{a_{14}}$、$P_{a_{23}}$ 分别为光学模 a_{14}、a_{23} 的正交相位分量;P_{y_A} 为含有相位码信息的光学模 y_A 的正交相位分量。

副台通过步骤1)和11)恢复出主台的相位码 x_A 和 y_A,至此可实现一组密钥信息传递,然后返回步骤6)继续传输。

4 方案安全性分析

4.1 纠缠测量攻击

纠缠测量攻击[18]是指敌方制备一对纠缠度与主台 a_{12} 和 a_{21} 相同的纠缠光学模 a_p 和 a_q,敌方拦截主台发送的光学模 a_{12} 和 a_{21},将光学模 a_q 和 a_p 发给副台,信道传输效率为 η_0。之后敌方对 a_{12} 和 a_{21} 进行纠缠测量并记录测量结果:

$$\begin{cases} X_u'=\dfrac{1}{\sqrt{2}}\left(X_{a_{11}}+x_A-X_{a_{21}}\right) \\ P_u'=\dfrac{1}{\sqrt{2}}\left(P_{a_{11}}+y_A+P_{a_{21}}\right) \end{cases}。 \tag{10}$$

敌方等待主台公布时间间隙进行Bell测量,由于敌方制备的光学模与主台传输的光学模的压缩

度相同，因此没插入诱骗态时主副台不会发现窃听行为，敌方恢复出的信息为

$$\begin{cases} x_{\mathrm{A}} = \sqrt{2}\left(X_{\mathrm{u}}' - X_{\mathrm{u0}}\right) \\ y_{\mathrm{A}} = \sqrt{2}\left(P_{\mathrm{u}}' - P_{\mathrm{u0}}\right) \end{cases}。 \tag{11}$$

因此，此方案为了防止纠缠测量攻击，在主台通过量子信道传输 a_{12} 之前，在步骤 7）中引入了诱骗态，因此敌方无法确定特定时隙处的压缩系数和插入的随机变量，进而在纠缠测量时无法消除诱骗信息。同时，由于主副台在步骤 9）中检测到的正交分量测量结果不准确，主台将会发现敌方的窃听行为，从而可以抵御纠缠测量攻击。

4.2　分光镜攻击

纠缠攻击会引起纠缠度发生变化[19]，导致窃听暴露，敌方可采用分光镜攻击方式，如图 4 所示。分光镜攻击就是敌方为了获得足够的信息并且要保持窃取信息行为的秘密性而采取的一种攻击手段，敌方截取主台发出的光束，让其通过透射系数为 η 的分光镜，自己截取其中 $1-\eta$ 的部分，让剩余部分通过无损信道传送给副台，然后通过主台公布的信息进行相应的操作[20]，进而获取信息。

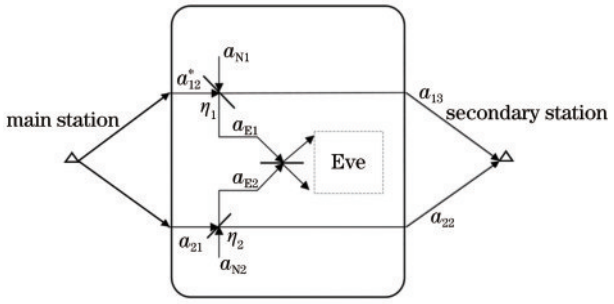

图 4　分光镜攻击框图

敌方的分光镜攻击手段就是将自己等效于信道噪声，其很难被发现。图 4 中 a_{N1} 和 a_{N2} 为量子信道的噪声，敌方先截取主台发出的一对纠缠光束，然后让其分别经过透射率为 η_1 和 η_2 的分光镜，并进行联合测量，可得

$$\begin{cases} X_{a_{13}} = \sqrt{\eta_1}\, X_{a_{12}^{*}} + \sqrt{1-\eta_1}\, X_{a_{\mathrm{N1}}} \\ X_{a_{\mathrm{E1}}} = \sqrt{1-\eta_1}\, X_{a_{12}^{*}} - \sqrt{\eta_1}\, X_{a_{\mathrm{N1}}} \end{cases}, \tag{12}$$

$$\begin{cases} X_{a_{22}} = \sqrt{\eta_2}\, X_{a_{21}} + \sqrt{1-\eta_2}\, X_{a_{\mathrm{N2}}} \\ X_{a_{\mathrm{E2}}} = \sqrt{1-\eta_2}\, X_{a_{21}} - \sqrt{\eta_2}\, X_{a_{\mathrm{N2}}} \end{cases}, \tag{13}$$

$$\begin{cases} P_{a_{13}} = \sqrt{\eta_1}\, P_{a_{12}^{*}} + \sqrt{1-\eta_1}\, P_{a_{\mathrm{N1}}} \\ P_{a_{\mathrm{E1}}} = \sqrt{1-\eta_1}\, P_{a_{12}^{*}} - \sqrt{\eta_1}\, P_{a_{\mathrm{N1}}} \end{cases}, \tag{14}$$

$$\begin{cases} P_{a_{22}} = \sqrt{\eta_2}\, P_{a_{21}} + \sqrt{1-\eta_2}\, P_{a_{\mathrm{N2}}} \\ P_{a_{\mathrm{E2}}} = \sqrt{1-\eta_2}\, P_{a_{21}} - \sqrt{\eta_2}\, P_{a_{\mathrm{N2}}} \end{cases}, \tag{15}$$

式中：a_{E1} 和 a_{E2} 分别为敌方通过透射率为 η_1 和 η_2 的分光镜获取的光学模；$X_{a_{13}}$、$X_{a_{22}}$、$X_{a_{\mathrm{N1}}}$、$X_{a_{\mathrm{N2}}}$、$X_{a_{\mathrm{E1}}}$、$X_{a_{\mathrm{E2}}}$ 分别为光学模 a_{13}、a_{22}、a_{N1}、a_{N2}、a_{E1}、a_{E2} 的正交振幅分量；$P_{a_{13}}$、$P_{a_{22}}$、$P_{a_{\mathrm{N1}}}$、$P_{a_{\mathrm{N2}}}$、$P_{a_{\mathrm{E1}}}$、$P_{a_{\mathrm{E2}}}$ 分别为光学模 a_{13}、a_{22}、a_{N1}、a_{N2}、a_{E1}、a_{E2} 的正交相位分量。

敌方保留 a_{E1} 和 a_{E2}，将 a_{13} 和 a_{22} 发送给副台，然后对 a_{E1} 和 a_{E2} 进行增益放大，待主台公布编码基后，敌方可利用测量基对量子态进行测量。副台收到 a_{13} 和 a_{22} 后，发现噪声等于信道噪声，因此敌方的窃听行为不会被发现。则此时副台对 a_{13} 和 a_{22} 进行联合测量，在振幅分量上得到的主台信息为

$$X_{\mathrm{u2}} = \frac{1}{\sqrt{2}}\left(X_{a_{13}} - X_{a_{22}}\right) = \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1}\, X_{a_{12}^{*}} + \sqrt{1-\eta_1}\, X_{a_{\mathrm{N1}}} - \sqrt{\eta_2}\, X_{a_{21}} - \sqrt{1-\eta_2}\, X_{a_{\mathrm{N2}}}\right) = \frac{1}{\sqrt{2}}\left[\left(\sqrt{\eta_1}\, X_{a_{10}} - \sqrt{\eta_2}\, X_{a_{20}}\right)\cosh(r) + \left(\sqrt{\eta_1}\, X_{a_{20}} - \sqrt{\eta_2}\, X_{a_{10}}\right)\sinh(r) + \sqrt{1-\eta_1}\, X_{a_{\mathrm{N1}}} - \sqrt{1-\eta_2}\, X_{a_{\mathrm{N2}}} + \sqrt{\eta_1}\, X_{x_{\mathrm{A}}}\right], \tag{16}$$

式中：$\frac{1}{\sqrt{2}}\sqrt{\eta_1}\, X_{x_{\mathrm{A}}}$ 为传给副台的有效信息；x_{A} 为真空态，服从高斯分布 $x_{\mathrm{A}} \sim N\left(0, \frac{1}{4}\right)$。量子噪声也服从 $N\left(0, \frac{1}{4}\right)$，则主副台的互信息量为

$$I(\mathrm{Main}, \mathrm{Sec}) = \mathrm{lb}\left(1 + \frac{S_1}{N_1}\right) = \mathrm{lb}\left\{1 + \frac{8\eta_1 V_{x_{\mathrm{A}}}}{(\eta_1+\eta_2)\left[\cosh(2r)-1\right] - \sqrt{\eta_1\eta_2}\sinh(2r) + 2}\right\}, \tag{17}$$

式中：S_x 为主副台间信号功率；N_x 为主副台间噪声功率；$V_{x_{\mathrm{A}}}$ 为信号功率的方差。

敌方在窃听到正确的测量基后，对保留的a_{E1}和a_{E2}进行联合测量，得到

$$X_{uE}=\frac{1}{\sqrt{2}}\left(X_{a_{E1}}-X_{a_{E2}}\right)=\frac{1}{\sqrt{2}}\left(\sqrt{1-\eta_1}\,X_{a_{12}^{*}}-\sqrt{\eta_1}\,X_{a_{N1}}-\sqrt{1-\eta_2}\,X_{a_{21}}+\sqrt{\eta_2}\,X_{a_{N2}}\right)=$$
$$\frac{1}{\sqrt{2}}\left[\left(\sqrt{1-\eta_1}\,X_{a_{10}}-\sqrt{1-\eta_2}\,X_{a_{20}}\right)\cosh(r)+\left(\sqrt{1-\eta_1}\,X_{a_{20}}-\sqrt{1-\eta_2}\,X_{a_{10}}\right)\sinh(r)-\right.$$
$$\left.\sqrt{\eta_1}\,X_{a_{N1}}+\sqrt{\eta_2}\,X_{a_{N2}}-\sqrt{(1-\eta_1)}\,X_{A}\right]。\tag{18}$$

Eve在振幅和相位上测得的互信息量为

$$I(\text{Main, Eve})=\text{lb}\left(1+\frac{S_E}{N_E}\right)。\tag{19}$$

由于

$$S_E=\frac{1}{2}(1-\eta_1)V_{x_A},\tag{20}$$

故

$$I(\text{Main, Eve})=\text{lb}\left\{1+\frac{8(1-\eta_1)V_{x_A}}{\left[2-(\eta_1+\eta_2)\right]\cosh(2r)-\sqrt{(1-\eta_1)(1-\eta_2)}\sinh(2r)+\eta_1+\eta_2}\right\},\tag{21}$$

式中：S_E为主台与敌方间的信号功率；N_E为主台与敌方间的噪声功率。可得信息效率为$\Delta I=I(\text{Main, Sec})-I(\text{Main, Eve})$，为了使主副台间能安全传输，则需$\Delta I>0$。

为了便于分析，对于一般情况，令$r=1$，$V_{x_A}=0.25$，图5是不同η_2下ΔI随η_1的变化。

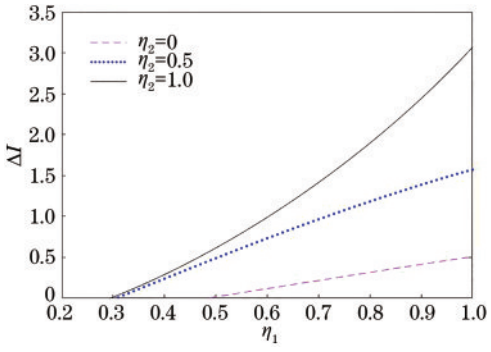

图5不同η_2下ΔI与η_1的关系

Fig. 5　Relationship between ΔI and η_1 under different η_2

由图5可以发现，ΔI与η_1和η_2均为正相关，这与实际相符，分光镜的透射率越高，则传输给副台的信号光越多，因此信息传输效率越高。对于敌方来说，需获取足够信息才能完成有效窃密，因此需要较低的透射率。当透射率过低时，$\Delta I<0$，副台接收不到信息，那么主副台将立即停止此次通信。

在$\eta_1=\eta_2=\eta$，$V_{x_A}=0.25$的条件下，传输效率在不同压缩度下随η的变化如图6所示。

从图6中可以发现，当$r=0$时，$\Delta I<0$，此时信息效率小于0，没有实际意义，信息无法进行传输；

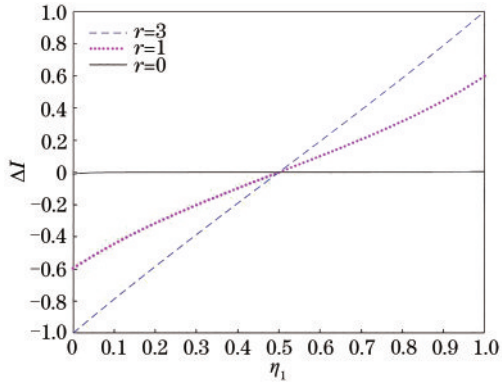

图6　不同r下ΔI与η的关系

Fig. 6　Relationship between ΔI and η under different r

当$r=1$或$r=3$时，$\Delta I>0$，信息效率大于0，信息可以有效传输。压缩率r越大，斜率越大，说明$\Delta I/\eta$变化更明显。当有敌方窃听，即η减小时，压缩率越大的纠缠态越容易被发现，所以在相位码传输的过程中，我们应该选用压缩率较高的压缩态。在压缩率相同的条件下，η_1越小，也就是敌方获得的信号越强时，信息传输的效率ΔI越低，因此在相位码传输过程中，传输效率显著降低说明传输受到了干扰，此时应停止此次通信。

5　结　　论

提出了基于EPR态的罗兰C台识别码传输方案，实现了主副台间相位码的识别与保密传输。罗兰C主台通过平移算符操作，可将台识别码编码到一个纠缠光学模上，任意一个副台通过经典信道得到Bell基测量结果，并参照统一的编码规则，识别

出主台的台识别码。该方案通过引入诱骗态，能有效抵抗纠缠测量攻击。在分光镜攻击下，分析了信息传输速率随压缩参数和分光镜透射系数的变化。安全性分析结果显示，所提方案能实现罗兰C台识别码的安全传输。

参 考 文 献

[1] Chen C, Wu D W, Yang C Y, et al. Research on enhancing synchronization precision between Roland C stations based on cavity electro-opto-mechanical system [J]. Acta Optica Sinica, 2019, 39(8): 0827001.
陈超, 吴德伟, 杨春燕, 等. 基于腔电光力系统增强罗兰C台间同步精度问题研究[J]. 光学学报, 2019, 39(8): 0827001.

[2] Gao W M. Research status and progress on E-Loran system[J]. Information & Communications, 2019, 32(7): 166-170.
高万明. E罗兰系统研究现状和进展[J]. 信息通信, 2019, 32(7): 166-170.

[3] Chen C, Wu D W, Yang C Y, et al. Method for improving Roland C inter-station synchronization precision using continuous-variable entanglement signals [J]. Laser & Optoelectronics Progress, 2019, 56(4): 042702.
陈超, 吴德伟, 杨春燕, 等. 利用连续变量纠缠信号提高罗兰C台间同步精度的方法[J]. 激光与光电子学进展, 2019, 56(4): 042702.

[4] Lin H W, Zhou H Q, Liu F T, et al. Research on phase coding identification of Loran-C signal under the background of strong CWI[J]. Journal of Test and Measurement Technology, 2012, 26(3): 252-255.
林洪文, 周洪庆, 刘福太, 等. 强载波干扰条件下的罗兰-C相位编码识别研究[J]. 测试技术学报, 2012, 26(3): 252-255.

[5] Lin H W, Zhang Q S, Yang D K, et al. Phase coding identification of Loran-C signal based on apFFT[J]. Journal of Tianjin University, 2011, 44(3): 257-260.
林洪文, 张其善, 杨东凯, 等. 基于apFFT的罗兰-C信号相位编码识别[J]. 天津大学学报, 2011, 44(3): 257-260.

[6] Wang Y Q, Li J. Neural network based Loran-C ASF correction method [J]. Modern Navigation, 2020, 11(2): 114-116.
王宇琦, 李江. 一种基于神经网络的罗兰C ASF修正方法[J]. 现代导航, 2020, 11(2): 114-116.

[7] Han D, Li Z H, Gao F F, et al. Comparison and analysis of several kinds of quantum key distribution protocols[J]. Journal of Quantum Optics, 2019, 25(4): 380-386.
韩朵, 李志慧, 高菲菲, 等. 几类量子密钥分发协议的比较与分析[J]. 量子光学学报, 2019, 25(4): 380-386.

[8] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 94(23): 230503.

[9] Fossier S, Diamanti E, Debuisschert T, et al. Field test of a continuous-variable quantum key distribution prototype [EB/OL]. (2008-12-17) [2020-06-21]. https://arxiv.org/abs/0812.3292.

[10] Guo Y, Liao Q, Wang Y J, et al. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction [J]. Physical Review A, 2017, 95(3): 032304.

[11] Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states[J]. Physical Review Letters, 2015, 114(7): 070501.

[12] Fang S H, Peng J Y, Huang P, et al. The synchronization scheme and implementation of continuous variable quantum key distribution system[J]. Journal of Quantum Optics, 2016, 22(1): 43-49.
方双红, 彭进业, 黄鹏, 等. 连续变量量子密钥分发系统同步方案及实现[J]. 量子光学学报, 2016, 22(1): 43-49.

[13] Li Y M, Zhang K S, Xie C D, et al. Quantum cryptography of continuous variable with quadrature squeezed state light [J]. Acta Sinica Quantum Optica, 2002, 8(2): 71-75.
李永民, 张宽收, 谢常德, 等. 利用正交压缩态光场实现连续变量的量子密码术[J]. 量子光学学报, 2002, 8(2): 71-75.

[14] He G Q, Yi Z, Zhu J, et al. Quantum key distribution using two-mode squeezd states[J]. Acta Physica Sinica, 2007, 56(11): 6427-6433.
何广强, 易智, 朱俊, 等. 基于双模压缩态的量子密钥分发方案[J]. 物理学报, 2007, 56(11): 6427-6433.

[15] Yi Z, He G Q, Zeng G H, et al. Quantum voting protocol using two-mode squeezed states[J]. Acta Physica Sinica, 2009, 58(5): 3166-3172.
易智, 何广强, 曾贵华, 等. 基于双模压缩态的量子投票协议[J]. 物理学报, 2009, 58(5): 3166-3172.

[16] Dong Y D, Peng X T, Song Y, et al. Multi-user quantum identify authentication protocol based on

orbital angular momentum technology[J]. Journal of Quantum Optics, 2019, 25(2): 152-157.
董颖娣, 彭晓天, 宋扬, 等. 基于轨道角动量的多用户量子身份认证协议[J]. 量子光学学报, 2019, 25(2): 152-157.

[17] Song H C, Gong L H, Zhou N R, et al. Continuous-variable quantum deterministic key distribution protocol based on quantum teleportation [J]. Acta Physica Sinica, 2012, 61(15): 154206.
宋汉冲, 龚黎华, 周南润, 等. 基于量子远程通信的连续变量量子确定性密钥分配协议[J]. 物理学报, 2012, 61(15): 154206.

[18] Zhang S L. Design and analysis of continuous variable quantum cryptography protocol[D]. Changsha: National University of Defense Technology, 2009: 47-59.
张守林. 连续变量量子密码协议设计与分析[D]. 长沙: 国防科学技术大学, 2009: 47-59.

[19] Yu Z B. Study on continuous variable quantum dialogue protocols based on two-mode squeezed states and GHZ states[D]. Nanchang: Nanchang University, 2016: 47-59.
余镇波. 基于双模压缩态和GHZ态的连续变量量子对话协议研究[D]. 南昌: 南昌大学, 2016: 47-59.

[20] Zhou F. Security analysis of continuous-vairable quantum cryptogram communication protocols based on beam splitter [D]. Jishou: Jishou University, 2012: 89-105.
周方. 基于分束器的连续变量量子保密通信协议安全性分析[D]. 吉首: 吉首大学, 2012: 89-105.