

# (12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织  
国际局



(10) 国际公布号

WO 2018/233502 A1

(43) 国际公布日  
2018年12月27日 (27.12.2018)

- (51) 国际专利分类号:  
H04B 10/70 (2013.01)
- (21) 国际申请号: PCT/CN2018/090544
- (22) 国际申请日: 2018年6月11日 (11.06.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201710467962.1 2017年6月20日 (20.06.2017) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN).

- (72) 发明人: 李政宇 (LI, Zhengyu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 苏长征 (SU, Changzheng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陆亮亮 (LU, Liangliang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: DATA TRANSMISSION METHOD, DEVICE, AND SYSTEM

(54) 发明名称: 一种数据传输方法、装置及系统

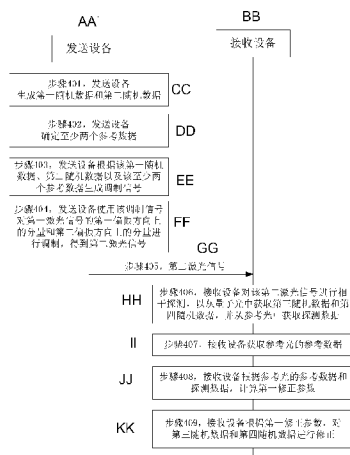


图 4

$$\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_1 & -X_1 & Y_1 & -Y_1 \\ X_1 & X_4 & Y_1 & Y_4 \\ X_1 & -X_1 & Y_1 & -Y_1 \end{pmatrix} \quad (1)$$

- AA Transmitting device
- BB Receiving device
- CC Step 401, the transmitting device generates first random data and second random data
- DD Step 402, the transmitting device determines at least two pieces of reference data
- EE Step 403, the transmitting device generates a modulating signal according to the first random data, the second random data, and the at least two pieces of reference data
- FF Step 404, the transmitting device modulates components of a first laser signal in a first polarization direction and in a second polarization direction using the modulating signal, to obtain a second laser signal
- GG Step 405, second laser signal
- HH Step 406, the receiving device performs coherent detection on the second laser signal so as to obtain third random data and fourth random data from quantum light and detection data from reference light
- JJ Step 408, the receiving device calculates a first correction parameter according to the reference data and detection data of the reference light
- KK Step 409, the receiving device corrects the third random data and fourth random data according to the first correction parameter

(57) Abstract: The application discloses a data transmission method, device, and system, relating to the technical field of communications, and can solve the problem of channel resource waste. The method comprises: a transmitting device generating first random data and second random data; determining at least two pieces of reference data; generating a modulating signal according to the first random data, the second random data, and the at least two pieces of reference data; the transmitting device modulating components of a first laser signal in a first



WO 2018/233502 A1

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,  
US, UZ, VC, VN, ZA, ZM, ZW。

- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

- 包括国际检索报告 (条约第21条(3))。

---

polarization direction and in a second polarization direction using the modulating signal, to obtain a second laser signal, the first polarization direction and the second polarization direction being perpendicular to each other, and the second laser signal comprising quantum light and reference light; the transmitting device transmitting the second laser signal; and the transmitting device determining at least two pieces of reference data, any two of the at least two pieces of reference data satisfying the following condition: one reference data  $(X_1, X_2, Y_1, Y_2)^T$  is different from another reference data  $(X_3, X_4, Y_3, Y_4)^T$ , and the matrix (I) formed by  $(X_1, X_2, Y_1, Y_2)^T$  and  $(X_3, X_4, Y_3, Y_4)^T$  is a full rank matrix.

(57) 摘要: 本申请公开了一种数据传输方法、装置及系统, 涉及通信技术领域, 能够解决信道资源浪费的问题。该方法包括: 发送设备生成第一随机数据和第二随机数据; 确定至少两个参考数据; 根据该第一随机数据、该第二随机数据以及该至少两个参考数据生成调制信号; 该发送设备使用该调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制, 得到第二激光信号, 该第一偏振方向和该第二偏振方向相互垂直, 该第二激光信号包括量子光和参考光; 该发送设备发送该第二激光信号; 该发送设备确定至少两个参考数据, 该至少两个参考数据中的任意两个参考数据满足以下条件: 一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同, 且  $(X_1, X_2, Y_1, Y_2)^T$  与  $(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵 (I) 满秩。

## 一种数据传输方法、装置及系统

5 本申请要求于 2017 年 06 月 20 日提交中国专利局、申请号为 201710467962.1、发明名称为“一种数据传输方法、装置及系统”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

### 技术领域

本申请涉及通信技术领域，尤其涉及一种数据传输方法、装置及系统。

### 10 背景技术

随着信息化程度的加快，通信的频率更加频繁，人们对通信的安全性的要求越来越高。量子保密通信是量子特性与传统密码结合的产物，它利用量子力学的基本原理和特性来确保通信的安全性。量子密钥分发 (Quantum key distribution, QKD) 技术是现阶段最接近实用的量子保密通信技术，QKD 技术是在已共享部分安全密钥的前提下，实现对称密钥的无条件安全分发。

15 目前，提出一种自参考连续变量量子密钥分发 (Self-Referenced Continuous-Variable Quantum Key Distribution, SR-CV-QKD) 的方案。其核心思想是：发送设备将待传输的量子密钥数据加载到量子光的一个偏振方向的分量上，然后在两个量子光之间引入一个光强较强的参考脉冲，用于接收设备检测发送的激光与接收设备产生的本振光的频偏与相差，并利用此信息修正密钥使得双方共享具有强相关的初始密钥。且接收设备在检测此信息之前，采用偏振控制器对发送设备发送的激光和接收设备产生的本振光进行稳频。由于基于参考光脉冲和相邻的量子光脉冲在时域上非常接近，且两者都经过了同一段信道传输。因此可以近似地认为参考光脉冲传输过程中变化的相位和相邻的量子光光脉冲一致，或者用前后两个参考光脉冲的平均相位来代替中间量子光信号光脉冲的相位。

20 然而，在上述方案中，发送设备只利用了一个偏振方向来编码量子密钥数据，另一个偏振方向是闲置的，没有充分利用信道资源，导致信道资源浪费。

### 发明内容

本申请提供了一种数据传输方法、装置及系统，能够解决信道资源浪费的问题。

30 第一方面，本申请提供了一种数据传输方法，该方法包括：发送设备生成第一随机数据和第二随机数据；该发送设备确定至少两个参考数据，该至少两个参考数据中的任意两个参考数据满足以下条件：该任意两个参考数据中的一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且  $(X_1, X_2, Y_1, Y_2)^T$  与

$(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩；该发送设备根据该第一随机数据、

该第二随机数据以及该至少两个参考数据生成调制信号；该发送设备使用该调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号，该第一偏振方向和该第二偏振方向相互垂直，该第二激光信号包括量子光和参考光；其中，该第二激光信号中的每一个计算周期包括一组量子光和两组参考光，该一组量子光在第一偏振方向上加载了该第一随机数据，该一组量子光在第二偏振方向上加载了该第二随机数据，该两组参考光中的第一组参考光在第一偏振方向上的  $x$  分量上加载了  $X_1$ ，该第一组参考光在第一偏振方向上的  $p$  分量上加载了  $X_2$ ，该第一组参考光在第二偏振方向上的  $x$  分量上加载了  $Y_1$ ，该第一组参考光在第二偏振方向上的  $p$  分量上加载了  $Y_2$ ，该两组参考光中的第二组参考光在第一偏振方向上的  $x$  分量上加载了  $X_3$ ，该第二组参考光在第一偏振方向上的  $p$  分量上加载了  $X_4$ ，该第二组参考光在第二偏振方向上的  $x$  分量上加载了  $Y_3$ ，该第二组参考光在第二偏振方向上的  $p$  分量上加载了  $Y_4$ ；该发送设备发送该第二激光信号。

采用本申请提供的数据传输方法，发送设备通过对第一激光信号的两个相互垂直的偏振方向上的分量进行调制，使得得到的第二激光信号在这两个偏振方向上，分别加载了两个相互独立的随机数据，由于这两个偏振方向相互垂直，相互之间无串扰，因此，在保证不影响系统安全性的情况下，充分利用了信道资源，将系统的成码率提高了一倍，从而解决了信道资源浪费的问题。

可选的，该发送设备使用该调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号之前，该方法还包括：该发送设备将该第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光。

可选的，该发送设备将该第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光，包括：该发送设备利用偏振分束器 PBS 或者分束器 BS，将该第一激光信号分为该第一偏振方向上的分量光和该第二偏振方向上的分量光。

采用上述两种可选的方式，发送设备可以先将第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光，以单独进行调制，从而提高了对第一激光信号在两个偏振方向上调制的精度。

可选的，该调制信号的个数为 2，该发送设备使用该调制信号对第一激光信号进行调制，得到第二激光信号，包括：该发送设备将该第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光；该发送设备采用两个调制信号中的第一个调制信号对该第一偏振方向上的分量光进行调制，采用该两个调制信号中的第二个调制信号对该第二偏振方向上的分量光进行调制；该发送设备将调制后的该第一偏振方向上的分量光进行  $90^\circ$  偏振旋转；该发送设备将调制后的该第二偏振方向上的分量光进行延时，使得调制后的该第一偏振方向上的分量光与调制后的该第二偏振方向上的分量光在时域上重合；该发送设备将经过  $90^\circ$  偏振旋转后的该第一偏振方向上的分量光，和经过延时后的该第二偏振方向上的分量光进行合束，得到该第二激光信号。

采用该可选的方式，发送设备通过分别为第一激光信号在两个偏振方向上的分量生成单独的调制信号，提高了对第一激光信号在两个偏振方向上调制的精度。

可选的，该发送设备根据该第一随机数据、该第二随机数据以及该至少两个参考数据生成调制信号，包括：该发送设备根据信道特性确定用于产生参考光的信号和用

于产生量子光的信号的组合模式，该信道特性为传输该第二激光信号的信道的特性；该发送设备按照该组合模式将该第一随机数据、该第二随机数据以及该至少两个参考数据进行排列组合，生成该调制信号。

5 采用该可选的方式，发送设备根据信道特性确定参考光和量子光的组合模式，当接收设备根据参考光分析量子光所经历的信道特性变化时，能够提高分析精度。

可选的，该组合模式为时分模式，该时分模式包括该用于产生量子光的信号的数量和该用于产生参考光的信号的数量，以及该用于产生量子光的信号和该用于产生参考光的信号。

10 可选的，该组合模式包括频分模式，该频分模式包括该用于产生量子光的信号的数量和该用于产生参考光的信号的数量，以及该用于产生量子光的信号和该用于产生参考光的信号在频域上的分布方式。

可选的，该方法还包括：该发送设备接收接收设备发送的第一修正参数；该发送设备根据该第一修正参数，对该第一随机数据和该第二随机数据进行数据修正。

15 可选的，该方法还包括：该发送设备接收接收设备发送的第一修正参数；该发送设备获取第二修正参数；该发送设备根据该第二修正参数和该第一修正参数，对该第一随机数据和该第二随机数据进行数据修正。

可选的，该方法还包括：该发送设备获取第二修正参数；该发送设备根据该第二修正参数，对该第一随机数据和该第二随机数据进行数据修正。

20 采用上述三种可选方式，发送设备能够通过第一修正参数和/或第二修正参数对第一随机数据和第二随机数据进行修正，以使得发送设备和接收设备的随机数据具有最大关联。使得接收设备无需使用偏振控制器来调整光脉冲的偏振。

25 第二方面，本申请提供一种数据传输方法，该方法包括：接收设备接收第二激光信号，该第二激光信号包括量子光和参考光；该接收设备对该第二激光信号进行相干探测，以从该量子光中获取第三随机数据和第四随机数据，以及从该参考光中获取探测数据；该接收设备获取该参考光的参考数据，该参考数据为该发送设备在调制该参考光时使用的参考数据；该接收设备根据该参考光的参考数据和该探测数据，计算第一修正参数；其中，该第二激光信号中的每一组量子光和两组参考光为一个计算周期，该两组参考光中的第一组参考光的参考数据  $(X_1, X_2, Y_1, Y_2)^T$  和该两组参考光中的第

二组参考光的参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩， $X_1$  为

30 该第一组参考光在第一偏振方向上的 x 分量上加载的参考数据， $X_2$  为该第一组参考光在第一偏振方向上的 p 分量上加载的参考数据， $Y_1$  为该第一组参考光在第二偏振方向上的 x 分量上加载的参考数据， $Y_2$  为该第一组参考光在第二偏振方向上的 p 分量上加载的参考数据， $X_3$  为该第二组参考光在第一偏振方向上的 x 分量上加载的参考数据， $X_4$  为该第二组参考光在第一偏振方向上的 p 分量上加载的参考数据， $Y_3$  为该第二组参考光在第二偏振方向上的 x 分量上加载的参考数据， $Y_4$  为该第二组参考光在第二偏振方向上的 p 分量上加载的参考数据。

采用本申请提供的数据传输方法，由于发送设备在第二激光信号的两个相互垂直的偏振方向上，分别加载了两个相互独立的随机数据，因此，接收设备能够在第二激光信号中获取第三随机数据和第四随机数据。由于这两个偏振方向相互垂直，相互之间无串扰，因此，在保证不影响系统安全性的情况下，充分利用了信道资源，将系统的成码率提高了一倍，从而解决了信道资源浪费的问题。

5 可选的，该探测数据包括第一部分探测数据和第二部分探测数据，该接收设备对该第二激光信号进行相干探测，以从该量子光中获取第三随机数据和第四随机数据，以及从该参考光中获取探测数据，包括：该接收设备将该第二激光信号划分为第一光信号和第二光信号；该接收设备采用第一相干探测方式对该第一光信号进行相干探测，以从该第一光信号中的参考光中获取该第一部分探测数据，以及从该第一光信号中的量子光中获取该第三随机数据和该第四随机数据；该接收设备采用第二相干探测方式对该第二光信号进行相干探测，以该第二光信号中的参考光中获取该第二部分探测数据。

15 在这种可选的方式中，无需接收设备中的探测器能对微弱的光和较强的参考光都完成探测，通过将第二激光信号划分为第一光信号和第二光信号，从第二光信号中仅探测参考光，从而降低了探测区间。

可选的，该接收设备根据该参考光的参考数据和该探测数据，计算第一修正参数之后，该方法还包括：该接收设备向该发送设备发送该第一修正参数。

20 可选的，该接收设备根据该参考光的参考数据和该探测数据，计算第一修正参数之后，该方法还包括：该接收设备根据该第一修正参数对该第三随机数据和该第四随机数据进行数据修正。

可选的，该接收设备获取该第三随机数据和该第四随机数据之后，该方法还包括：该接收设备获取第二修正参数；该接收设备根据该第二修正参数对该第三随机数据和该第四随机数据进行数据修正。

25 可选的，该接收设备根据该参考光的参考数据和该探测数据，计算第一修正参数之后，该方法还包括：该接收设备获取第二修正参数；该接收设备根据该第一修正参数和该第二修正参数，对该第三随机数据和该第四随机数据进行数据修正。

30 采用上述三种可选方式，接收设备无需使用偏振控制器来调整光脉冲的偏振，可以直接通过探测到的探测数据以及参考光的参考数据来计算第一修正参数，第一修正参数表现了光在信道以及接收设备中传输时发生的偏振方向、相位等的影响。然后通过第一修正参数和/或第二修正参数来对第三随机数据和第四随机数据进行修正，以使得发送设备和接收设备的随机数据具有最大关联。

35 第三方面，本申请还提供了一种发送设备，所述发送设备可以包括用于执行前述第一方面及第一方面的各种实现方式中方法步骤的生成单元、调制单元、发送单元、接收单元、修正单元、获取单元、分束单元等单元模块。

本申请提供的发送设备的技术效果可以参见上述第一方面或第一方面的各个实现方式的技术效果，此处不再赘述。

第四方面，本申请还提供了一种接收设备，所述接收设备用于执行前述第二方面及第二方面的各种实现方式中方法步骤的接收单元、探测单元、获取单元、计算单元、

修正单元、分束单元等单元模块。

本申请提供的接收设备的技术效果可以参见上述第二方面或第二方面的各个实现方式的技术效果，此处不再赘述。

5 第五方面，本申请还提供了一种发送设备，包括：处理器、调制器、随机数据源以及光源；所述光源用于发射第一激光信号，所述随机数据源用于生成第一随机数据和第二随机数据，所述处理器用于确定至少两个参考数据，根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号，其中，所述至少两个参考数据中的任意两个参考数据满足以下条件：所述任意两个参考数据中的一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且  $(X_1, X_2, Y_1, Y_2)^T$  与

10  $(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩；所述调制器用于使用所述调制信

号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号，并发送所述第二激光信号，其中，所述第二激光信号中的每一个计算周期包括一组量子光和两组参考光，所述一组量子光在第一偏振方向上加载了所述第一随机数据，所述一组量子光在第二偏振方向上加载了所述第二随机数据，所述两组参考光中的第一组参考光在第一偏振方向上的 x 分量上加载了  $X_1$ ，所述第一组参考光在第一偏振方向上的 p 分量上加载了  $X_2$ ，所述第一组参考光在第二偏振方向上的 x 分量上加载了  $Y_1$ ，所述第一组参考光在第二偏振方向上的 p 分量上加载了  $Y_2$ ，所述两组参考光中的第二组参考光在第一偏振方向上的 x 分量上加载了  $X_3$ ，所述第二组参考光在第一偏振方向上的 p 分量上加载了  $X_4$ ，所述第二组参考光在第二偏振方向上的 x 分量上加载了  $Y_3$ ，所述第二组参考光在第二偏振方向上的 p 分量上加载了  $Y_4$ ；所述发送设备发送所述第二激光信号。

20 本申请提供的发送设备的技术效果可以参见上述第一方面或第一方面的各个实现方式的技术效果，此处不再赘述。

25 第六方面，本申请还提供了一种接收设备，包括：处理器、探测器及本地本振光源等；所述探测器用于接收第二激光信号，所述第二激光信号包括量子光和参考光；所述本地本振光源用于发射 LL0，所述探测器还用于使用所述 LL0 对所述第二激光信号进行相干探测，以从所述量子光中获取第三随机数据和第四随机数据，以及从所述参考光中获取探测数据；所述处理器用于获取所述参考光的参考数据，并根据所述参考光的参考数据和所述探测数据，计算第一修正参数；其中，所述参考数据为所述发送设备在调制所述参考光时使用的参考数据；所述第二激光信号中的每一组量子光和两组参考光为一个计算周期，所述两组参考光中的第一组参考光的参考数据  $(X_1, X_2, Y_1, Y_2)^T$  和所述两组参考光中的第二组参考光的参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，

且矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩,  $X_1$  为所述第一组参考光在第一偏振方向上的 x 分量

5 上加载的参考数据,  $X_2$  为所述第一组参考光在第一偏振方向上的 p 分量上加载的参考数据,  $Y_1$  为所述第一组参考光在第二偏振方向上的 x 分量上加载的参考数据,  $Y_2$  为所述第一组参考光在第二偏振方向上的 p 分量上加载的参考数据,  $X_3$  为所述第二组参考光在第一偏振方向上的 x 分量上加载的参考数据,  $X_4$  为所述第二组参考光在第一偏振方向上的 p 分量上加载的参考数据,  $Y_3$  为所述第二组参考光在第二偏振方向上的 x 分量上加载的参考数据,  $Y_4$  为所述第二组参考光在第二偏振方向上的 p 分量上加载的参考数据。

10 从而实现以第二方面各种实现方式所述数据传输方法, 所述探测器用于使用所述本地本振光源输出的本振光, 对接收到的第二激光信号进行探测。

本申请提供的接收设备的技术效果可以参见上述第二方面或第二方面的各个实现方式的技术效果, 此处不再赘述。

第七方面, 本申请还提供了一种存储介质, 该计算机存储介质可存储有程序, 该程序执行时可实现包括本申请提供的数据传输方法各实施例中的部分或全部步骤。

15 第八方面, 本申请还提供一种通信系统, 包括如第三方面或第三方面的任一实现方式所述的发送设备, 和第四方面或第四方面的任一实现方式所述的接收设备; 或者, 包括如第五方面所述的发送设备, 和第六方面所述的接收设备。

**附图说明**

- 图 1 为本申请提供的通信系统的结构示意图;
- 20 图 2 为本申请提供了一种发送设备的结构示意图一;
- 图 3 为本申请提供了一种接收设备的结构示意图一;
- 图 4 为本申请提供了一种数据传输方法的一个实施例的流程图一;
- 图 5A 为本申请提供了一种时分模式下的光脉冲示意图;
- 图 5B 为本申请提供了一种频分模式下的光脉冲示意图;
- 25 图 6A 为本申请提供了一种发送设备的结构示意图二;
- 图 6B 为本申请提供了一种发送设备的结构示意图三;
- 图 6C 为本申请提供了一种发送设备的结构示意图四;
- 图 6D 为本申请提供了一种发送设备的结构示意图五;
- 图 6E 为本申请提供了一种发送设备的结构示意图六;
- 30 图 7A 为本申请提供了一种接收设备的结构示意图二;
- 图 7B 为本申请提供了一种接收设备的结构示意图三;
- 图 7C 为本申请提供了一种接收设备的结构示意图四;
- 图 8 为本申请提供了一种数据传输方法的一个实施例的流程图二;
- 图 9 为本申请提供了一种数据传输方法的一个实施例的流程图三;
- 35 图 10 为本申请提供了一种数据传输方法的一个实施例的流程图四;

图 11A 为本申请提供的一种发送设备的结构示意图七；  
图 11B 为本申请提供的一种发送设备的结构示意图八；  
图 11C 为本申请提供的一种发送设备的结构示意图九；  
图 11D 为本申请提供的一种发送设备的结构示意图十；  
5 图 11E 为本申请提供的一种发送设备的结构示意图十一；  
图 12A 为本申请提供的一种接收设备的结构示意图七；  
图 12B 为本申请提供的一种接收设备的结构示意图八；  
图 12C 为本申请提供的一种接收设备的结构示意图九；  
图 12D 为本申请提供的一种接收设备的结构示意图十。

## 10 具体实施方式

首先，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中字符“/”，一般表示前后关联对象是一种“或”的关系。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。

15 此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

20 其次，本申请提供的数据传输方法可以适用于量子通信系统中，如图 1 所示，为本申请提供的一种通信系统框图，包括至少一个发送设备和至少一个接收设备。其中，发送单元可以是具有量子保密通信功能的量子发送设备。接收设备可以是具有量子保密通信功能的量子接收设备。

示例性的，如图 2 所示，为本申请提供的一种发送设备的结构示意图，可以包括光源、处理器、存储器、调制模块以及随机信号源等。

25 其中，处理器用于解密接收到的命令，根据解密的命令执行计算或数据处理，以及将处理后的数据发送至其他设备，以控制其他设备执行相应的操作。处理器可以是中央处理器 (Central Processing Unit, CPU)，通用处理器，数字信号处理器 (Digital Signal Processor, DSP)，专用集成电路 (Application-Specific Integrated Circuit, ASIC)，现场可编程门阵列 (Field Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。

30 存储器包括程序模块以及数据模块等。程序模块可以由软件、固件、硬件或其中的至少两种组成，用于存储应用程序以及操作系统。所述存储器可以包括易失性存储器 (volatile memory)，例如随机存取内存 (random access memory，简称 RAM)；还可以包括非易失性存储器 (non-volatile memory)，例如快闪存储器 (flash memory)，硬盘 (hard disk drive，简称 HDD) 或固态硬盘 (solid-state drive，简称 SSD)；存储器还可以包括上述种类的存储器的组合。

光源用于产生激光信号。调制模块可以在处理器的控制下，利用随机信号源产生

的生成随机数据，对激光信号进行调制，得到加载了随机数据的激光信号，并将激光信号发出。其中，调制模块可以包括强度调制器、相位调制器以及驱动器，还可以包括偏振分束器、分束器、环形器、90° 偏振旋转器、延时器、四相移相键控 (Quadrature phase-shift keying, QPSK) 调制器，双极化四相移相键控 (Dual polarization quadrature phase-shift keying, DPQPSK) 调制器等器件。

此外，本申请提供的发送设备还可以包括通信接口，用于在处理器的控制下与系统中的其他网元设备进行数据通信。

如图 3 所示，为本申请提供的一种接收设备的结构示意图，可以包括处理器、存储器、探测模块、以及本地本振光源等。

其中，处理器用于解密接收到的命令，根据解密的命令执行计算或数据处理，以及将处理后的数据发送至其他设备，以控制其他设备执行相应的操作。处理器可以为 CPU，通用处理器，DSP，ASIC，FPGA 或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。

存储器包括程序模块以及数据模块等。程序模块可以由软件、固件、硬件或其中的至少两种组成，用于存储应用程序以及操作系统。所述存储器可以包括易失性存储器，例如 RAM；还可以包括非易失性存储器，例如快闪存储器，HDD 或者 SSD；存储器还可以包括上述种类的存储器的组合。

本地本振光源用于产生本振光。探测模块用于接收激光信号，并利用本振光对接收到的激光信号进行相干探测，获取探测数据。其中，探测模块可以包括外差探测器 (Heterodyne Detector, HD)、平衡零差探测器 (Balanced Homodyne Detector, BHD) 以及模数转换器 (Analog-to-digital converter, ADC) 等器件。

此外，本申请提供的接收设备还可以包括通信接口，用于在处理器的控制下与系统中的其他网元设备进行数据通信。

基于图 1，参见图 4，为本申请提供的一种数据传输方法的一个实施例的流程图，该方法包括如下步骤：

步骤 401，发送设备生成第一随机数据和第二随机数据。

在本申请中，发送设备可以根据预设的调制协议生成两个相互独立的第一随机数据和第二随机数据。其中，调制制式可以为四相移相键控 (Quadrature phase-shift keying, QPSK) 调制协议、双极化四相移相键控 (Dual polarization quadrature phase-shift keying, DPQPSK) 调制协议、高斯调制协议等。

在一个示例中，发送设备可以通过两个相互独立的随机信号源生成第一随机数据和第二随机数据。例如，真随机数发生器 (True Random Number Generator, TRNG)，量子随机数发生器 (Quantum Random Number Generator, QRNG) 等。

示例性的，当预设的调制协议是高斯调制协议时，发送设备可以将 TRNG1 生成的离散化高斯随机数作为第一随机数据，通过将 TRNG2 生成的离散化高斯随机数作为第二随机数据。

步骤 402，发送设备确定至少两个参考数据。

在本申请中，该至少两个参考数据中的任意两个参考数据需要满足以下条件：

该任意两个参考数据中的一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且  $(X_1, X_2, Y_1)^T$  与  $(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵

$$\begin{pmatrix} X_1 & X_2 & Y_1 \\ X_2 & -X_1 & Y_2 \\ X_3 & X_4 & Y_3 \\ X_4 & -X_3 & Y_4 \end{pmatrix} \text{ 满秩。}$$

5 需要说明的是，在本申请中，一个参考数据可以分为两个序列，分别用于调制一个激光信号在不同偏振方向上的分量。例如，参考数据  $(X_1, X_2, Y_1, Y_2)^T$  包括序列  $(X_1, X_2)$  和序列  $(Y_1, Y_2)$ 。其中，序列  $(X_1, X_2)$  用于调制该激光信号在第一偏振方向上的正则分量（包括 x 分量和 p 分量），序列  $(Y_1, Y_2)$  用于调制该激光信号在第二偏振方向上的正则分量。

10 步骤 403，发送设备根据该第一随机数据、第二随机数据以及该至少两个参考数据生成调制信号。

步骤 404，发送设备使用该调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号。

15 在本申请中，当发送设备需要发送第一随机数据和第二随机数据时，发送设备即可通过光源产生第一激光信号，该第一激光信号可以是连续激光也可以是脉冲激光。下面以脉冲激光为例进行示例性的说明。

20 示例性的，发送设备中的光源可以包括激光器和脉冲产生模块，由激光器产生连续波（Continuous Wave, CW），然后由脉冲产生模块通过斩波的方式将该连续波转换成光脉冲，从而得到第一激光信号。其中，该连续波可以是具有线偏振、窄线宽的连续波。通过斩波方式得到的光脉冲，可以是具有高消光比的光脉冲。

在一个示例中，第一激光信号中光脉冲的占空比可以在 1%~99% 之间。例如，以 100MHz 的系统重复频率为例，如果发送设备按照 50% 的占空比来生成光脉冲，那么经过斩波后可以生成包络为 5ns 宽方波的线偏振光脉冲。

25 当生成第一激光信号后，发送设备可以通过对第一激光信号的调制，将需要发送的第一随机数据和第二随机数据，以及用于接收设备分析信道特性变化情况的至少两个参考数据加载到第一激光信号上，得到第二激光信号。

30 在本申请中，第二激光信号中加载了第一随机数据和第二随机数据的光脉冲称为量子光，发送设备通过量子光传输第一随机数据和第二随机数据；第二激光信号中加载了至少两个参考数据中的任一个参考数据的光脉冲称为参考光，接收设备可以通过参考光分析信道特性变化情况（例如，时延不稳定、相位发生偏差以及偏振方向旋转等情况），以计算修正参数，来对获得的随机数据进行修正。

需要说明的是，接收设备在每次分析一组量子光（包括至少一个量子光）所经历的信道特性变化情况时，都需要通过对至少两组参考光（每一组参考光可以包括至少一个参考光）进行探测分析来获得。因此，在本申请中，第二激光信号中的每一组量子光和两组参考光为一个计算周期。其中，这一组量子光在第一偏振方向上加载了第

一随机数据，在第二偏振方向上加载了第二随机数据。这两组参考光中的第一组参考光中的每个参考光上加载的参考数据都相同，第二组参考光中的每个参考光上加载的参考数据也都相同。其中，第一组参考光在第一偏振方向上的分量上的 x 分量上加载了  $X_1$ ，该第一组参考光在第一偏振方向上的分量上的 p 分量上加载了  $X_2$ ，该第一组参考光在第二偏振方向上的分量上的 x 分量上加载了  $Y_1$ ，该第一组参考光在第二偏振方向上的分量上的 p 分量上加载了  $Y_2$ ，该两组参考光中的第二组参考光在第一偏振方向上的分量上的 x 分量上加载了  $X_3$ ，该第二组参考光在第一偏振方向上的分量上的 p 分量上加载了  $X_4$ ，该第二组参考光在第二偏振方向上的分量上的 x 分量上加载了  $Y_3$ ，该第二组参考光在第二偏振方向上的分量上的 p 分量上加载了  $Y_4$ 。

10 示例性的，以量子光的第一偏振方向上的调制为例，假设第一随机数据包括多对数据，其中一对数据为  $a_1$  (x 分量) 和  $a_2$  (p 分量)。即数据  $a_1$  和  $a_2$  为根据预设的调制协议的调制制式获得的一对随机数据。比如对于高斯调制协议， $a_1$  和  $a_2$  就是服从某个方差和均值的高斯随机数；对于 QPSK 调制， $a_1$  和  $a_2$  就是服从某个特定取值的两点分布。

15 假设在调制得到量子光时，生成的第一偏振方向上的相干态为  $|\alpha\rangle$ ，其中  $\alpha = f_1(a_1) + if_2(a_2)$ ， $f_1$  表示将  $a_1$  加载到量子光在第一偏振方向上的 x 分量上时经历的函数变换， $f_2$  表示将  $a_2$  加载到量子光在第一偏振方向上的 p 分量上时经历的函数变换。在一个示例中， $f_1(a_1) = a_1$ ， $f_2(a_2) = a_2$ 。若  $\mu$  代表该相干态的平均光子数，则  $\mu = |\alpha|^2 = a_1^2 + a_2^2$ 。

20 那么，在本申请中，量子光在第一偏振方向上加载了第一随机数据，即为经过调制得到的量子光在第一偏振方向上的 x 分量为  $f_1(a_1)$ ，在第一偏振方向上的 p 分量为  $f_2(a_2)$ 。

同理，以参考光的第一偏振方向上的调制为例，如果参考数据分别为  $X_1$  (x 分量) 和  $X_2$  (p 分量)，假设在调制得到参考光时，生成的第一偏振方向上的相干态为  $|\beta\rangle$ ，那么， $\beta = f_3(X_1) + if_4(X_2)$ ， $f_3$  表示将  $X_1$  加载到参考光在第一偏振方向上的 x 分量上时经历的函数变换， $f_4$  表示将  $X_2$  加载到参考光在第一偏振方向上的 p 分量上时经历的函数变换。在一个示例中， $f_3(X_1) = X_1$ ， $f_4(X_2) = X_2$ 。若  $\nu$  代表该相干态的平均光子数，则  $\nu = |\beta|^2 = X_1^2 + X_2^2$ 。而参考数据  $X_1$  和  $X_2$  为根据协议所选调制制式而决定的随机数。比如对于高斯调制协议， $X_1$  (和  $X_2$ ) 就是服从某个方差和均值的高斯随机数；对于 QPSK 调制， $X_1$  (和  $X_2$ ) 就是服从某个特定取值的两点分布。

30 可以理解的是，在本申请中，参考光在第一偏振方向上的分量上的 x 分量上加载了  $X_1$ ，即为经过调制得到的参考光在第一偏振方向上的 x 分量为  $f_3(X_1)$ ，第一组参考光在第一偏振方向上的分量上的 p 分量上加载了  $X_2$ ，即为经过调制得到的参考光在第一偏振方向上的 p 分量为  $f_4(X_2)$ 。

35 需要说明的是，第一随机数据和第二随机数据是发送设备通过随机数据源生成的，该至少两个参考数据是发送设备从该发送设备的存储器中获取的，或者是通过参考数据输出模块生成的。而在对第一激光信号进行调制的过程中，第一随机数据、第二随机数据以及该至少两个参考数据是按照排列组合方式加载在该第一激光信号上的。因此，对第一激光信号进行调制之前，发送设备可以先通过数据合并器，按照预设的组

合模式，将第一随机数据、第二随机数据以及该至少两个参考数据进行排列组合，得到与量子光和参考光的排列顺序相对应的数据序列。且由于发送设备使用调制器调制第一激光信号时，使用的是其他类型的信号，例如电压信号。因此，发送设备还可以通过数据转换器将该数据序列转换为对应的电压信号，从而得到最终使用的调制信号。

5 在一个示例中，发送设备可以先根据信道特性确定用于产生量子光的信号（以下简称量子信号）和用于产生参考光的信号（以下简称参考信号）的组合模式，然后按照该组合模式将该第一随机数据、该第二随机数据以及该至少两个参考数据进行排列组合，生成该调制信号。其中，量子信号和参考信号的组合模式，决定了通过该调制信号调制所得的第二激光信号中量子光和参考光的组合模式。

10 例如，如果传输第二激光信号的信道特性变化十分缓慢，或系统工作重复频率极高。那么，通过该调制信号调制所得第二激光信号在一个计算周期内，可以包括若干个量子光和两个参考光。这两个参考光可以分别位于该若干个量子光的两端，也可以夹杂在该若干个量子光之间。如果信道特性变化较快，那么，通过该调制信号调制所得第二激光信号在一个计算周期内，可以增加参考光的数量，即包括若干个量子光和  
15 两组若干个参考光。如果信道特性变化非常快，那么，在一个计算周期内，可以包括一个量子光和分别位于该量子光两端的两组若干个参考光。

在一个示例中，量子信号和参考信号的组合模式可以是时分模式，也可以是频分模式。其中，时分模式包括量子信号的数量、参考信号的数量，以及量子信号和参考信号在时域上的分布方式。频分模式包括量子信号的数量、参考信号的数量，以及量子信号和参考信号在频域上的分布方式。  
20

可以理解的是，通过时分模式生成的调制信号，调制所得的第二激光信号中的量子光和参考光也是按照对应该时分模式进行划分，且该第二激光信号中量子光和参考光的数量以及在时域上的分布，与量子信号和参考信号在时域上的分布方式相同。

25 例如，以脉冲光为例，时分模式是指不同延时位置的光脉冲代表不同类型的光（量子光或者参考光）。示例性的，如图 5A 所示，第二激光信号包括 9 个光脉冲，第 1、3、4、6、7、9 个光脉冲为参考光，第 2、5、8 个光脉冲为量子光。第 1、3 个参考光用于分析第 2 个量子光所经历的信道特性变化情况；第 4、6 个参考光用于分析第 5 个量子光所经历的信道特性变化情况；第 7、9 个参考光用于分析第 8 个量子光所经历的信道特性变化情况。

30 同理，通过频分模式生成的调制信号，调制所得的第二激光信号中的量子光和参考光也是按照对应该频分模式进行划分，且该第二激光信号中量子光和参考光的数量以及在频域上的分布，与量子信号和参考信号在频域上的分布方式相同。即通过频分模式可以使得得到的第二激光信号中量子光和参考光的频率不同，但在时间上可以是重合的。例如，如图 5B 所示，第二激光信号中的一个光脉冲在频率 1 和频率 2 为参考光，在频率 3 为两量子光。一个光脉冲中的两个参考光用于分析该光脉冲中量子光所  
35 经历的信道特性变化情况。

在本申请中，发送设备可以生成一个调制信号，来对第一激光信号的两个偏振方向进行调制。发送设备也可以生成两个调制信号，分别对第一激光信号的两个偏振方向进行单的调制。

发送设备可以直接对第一激光信号进行双偏振调制。也可以在对第一激光信号进行双偏振调制之前,可以先将第一激光信号从第一偏振方向和第二偏振方向进行分束,得到第一偏振方向上的分量光和第二偏振方向分量光。然后分别对第一路偏振光和第二路偏振光进行调制。最后将调制后的第一路偏振光和第二路偏振光合束成一路激光,得到第二激光信号。

在本申请中,发送设备可以利用偏振分束器或者这分束器对第一激光信号进行分束。

下面将结合如下三示例,对发送设备使用调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制的方式进行示例性的说明。

10 当发送设备生成一个调制信号,且采用时分模式时,发送设备的结构可以如图 6A 所示,包括光源 1,调制信号生成模块 2 以及双偏振方向调制模块 3。

光源 1 包括激光器 11 和脉冲模块 12,由激光器 11 生成连续波,再由脉冲模块 12 将该连续波转换成光脉冲,得到第一激光信号。

15 调制信号生成模块 2 可以包括随机信号源 21、随机信号源 22、参考数据输出模块 23、数据合并器 24、数据转换器 25。随机信号源 21 生成并输出第一随机数据,随机信号源 22 生成并输出第二随机数据,参考数据输出模块 23 输出至少两个参考数据。数据合并器 24 将输入的第一随机数据、第二随机数据以及至少两个参考数据,按照发送设备确定的时分模式进行排列组合,得到数据序列。数据合并器 24 得到数据序列后,即可将数据序列输出,发送至数据转换器 25,由数据转换器 25 将该数据序列转换为调制信号。

20 例 1,结合上述图 5A,假设随机信号源 21 的第一随机数据包括 3 对数据,为  $\{(a_1, a_2), (a_3, a_4), (a_5, a_6)\}$ ,随机信号源 22 第二随机数据包括 3 对数据,为  $\{(b_1, b_2), (b_3, b_4), (b_5, b_6)\}$ 。参考数据输出模块 23 输出了两个参考数据为  $(X_1, X_2, Y_1, Y_2)^T$  和  $(X_3, X_4, Y_3, Y_4)^T$ 。预设的时分模式为:在每一个偏振方向上包括 6 个参考信号和 3 个量子信号,按照光脉冲的时间顺序,在时域上的分布情况是为先排列用于调制第一偏振方向上的分量的各个信号,再排列用于调制第二偏振方向上的分量的各个信号,每一个偏振方向对应的 6 个参考信号和 3 个量子信号,按照 2 个参考信号和 1 个量子信号为一组进行划分,得到 3 组信号依次排列,每一组中按照“参考信号,量子信号,参考信号”的顺序排列。

30 那么,数据合并器 24 根据该预设的时分模式,先对第一随机数据、第二随机数据以及两个参考数据进行排列,得到的数据序列为  $\{(X_1, X_2), (a_1, a_2), (X_3, X_4), (X_1, X_2), (a_3, a_4), (X_3, X_4), (X_1, X_2), (a_5, a_6), (X_3, X_4), (Y_1, Y_2), (b_1, b_2), (Y_3, Y_4), (Y_1, Y_2), (b_3, b_4), (Y_3, Y_4), (Y_1, Y_2), (b_5, b_6), (Y_3, Y_4)\}$ 。其中,  $\{(X_1, X_2), (a_1, a_2), (X_3, X_4), (X_1, X_2), (a_3, a_4), (X_3, X_4), (X_1, X_2), (a_5, a_6), (X_3, X_4)\}$  为与第一偏振方向对应的数据子序列 1,  $\{(Y_1, Y_2), (b_1, b_2), (Y_3, Y_4), (Y_1, Y_2), (b_3, b_4), (Y_3, Y_4), (Y_1, Y_2), (b_5, b_6), (Y_3, Y_4)\}$  为与第二偏振方向对应的数据子序列 2。数据合并器 24 将该数据序列发送至数据转换器 25 后,即可由数据转换器 25 将该数据序列转换为对应的电压序列,得到调制信号。

双偏振方向调制模块 3 可以包括环形器 31、偏振分束器 32、强度调制器 33、相位调制器 34、驱动器 35 以及  $90^\circ$  偏振旋转器 35。脉冲模块 12 输出的第一激光信号从环形器 31 的 311' 端进入环形器 31 后,从环形器的 312' 端输出,并从偏振分束器 32 的 321 端进入偏振分束器 32。偏振分束器 32 将第一激光信号一分为二,得到该第一激光信号在第一偏振方向上的分量光(以下称为第一路偏振光)和在第二偏振方向上的分量光(以下称为第二路偏振光)。

第一路偏振光从偏振分束器 32 的 322 端输出,按照如图 6A 所示的逆时针方向,延保偏光纤传输。当经过强度调制器 33 和相位调制器 34 时,驱动器 35 根据调制信号对强度调制器 33 和相位调制器 34 进行驱动,以使得强度调制器 33 和相位调制器 34 按照调制信号中的电压序列对经过的第一路偏振光进行调制,以将数据子序列 1 加载在第一路偏振光上。第一路偏振光经过强度调制器 33 和相位调制器 34 的调制后,经过  $90^\circ$  偏振旋转器 35 旋转  $90^\circ$ ,继续沿着保偏光纤传输,从偏振分束器 32 的 323 端进入偏振分束器 32。

第二路偏振光从偏振分束器 32 的 323 端输出,按照如图 6A 所示的顺时针方向沿着保偏光纤传输,先经过  $90^\circ$  偏振旋转器 35 旋转  $90^\circ$ ,以使得第一路偏振光和第二路偏振光的偏振方向保持相互垂直。然后经过相位调制器 34 和强度调制器 33。通过相位调制器 34 和强度调制器 33 的调制,以将数据子序列 2 加载在第二路偏振光上。第二路偏振光经过相位调制器 34 和强度调制器 33 的调制后,继续沿着保偏光纤传输,从偏振分束器 32 的 322 端进入偏振分束器 32。

结合上述例 1 可知,双偏振方向调制模块 3 采用上述调制信号对第一激光信号中的 9 个光脉冲进行调制后,即可如图 5A 所示的第二激光信号中,其中,光脉冲 1、4、7 在第一偏振方向上的 x 分量加载了  $X_1$ ,在第一偏振方向上的 p 分量加载了  $X_2$ ,在第二偏振方向上的 x 分量加载了  $Y_1$ ,在第一偏振方向上的 p 分量加载了  $Y_2$ ;光脉冲 3、6、9 在第一偏振方向上的 x 分量加载了  $X_3$ ,在第一偏振方向上的 p 分量加载了  $X_4$ ,在第二偏振方向上的 x 分量加载了  $Y_3$ ,在第一偏振方向上的 p 分量加载了  $Y_4$ ;光脉冲 2 在第一偏振方向上的 x 分量加载了  $a_1$ ,在第一偏振方向上的 p 分量加载了  $a_2$ ,在第二偏振方向上的 x 分量加载了  $b_1$ ,在第二偏振方向上的 p 分量加载了  $b_2$ ;光脉冲 5 在第一偏振方向上的 x 分量加载了  $a_3$ ,在第一偏振方向上的 p 分量加载了  $a_4$ ,在第二偏振方向上的 x 分量加载了  $b_3$ ,在第二偏振方向上的 p 分量加载了  $b_4$ ;光脉冲 8 在第一偏振方向上的 x 分量加载了  $a_5$ ,在第一偏振方向上的 p 分量加载了  $a_6$ ,在第二偏振方向上的 x 分量加载了  $b_5$ ,在第二偏振方向上的 p 分量加载了  $b_6$ 。

值得说明的是,由于第一路偏振光和第二路偏振光到达相位调制器 34 和强度调制器 33 的时刻是有差异的,即相位调制器 34 和强度调制器 33 对第一路偏振光和第二路偏振光的调制在时域上是分离的,因此使用一组调制器能够实现对两个偏振方向分别调制独立的数据。

由于第一路偏振光和第二路偏振光同时从偏振分束器 32 的 323 端和 322 端输出,又经过相同的路径,因此第一路偏振光和第二路偏振光可以同时回到偏振分束器 32 中。进而,偏振分束器 32 可以对第一路偏振光和第二路偏振光进行合束,得到第二激光信号。

第二激光信号从偏振分束器 32 的 321 端输出，从环形器 31 的 312' 端输入，然后从环形器的 323 端输出，经过信道传输至接收设备。

5 可选的，结合图 6A，如图 6B 所示，为了得到不同强度的参考光（光强较强）和量子光（光强较弱），可以在偏振分束器 32 的 323 端与 90° 偏振旋转器 35 之间增加驱动器 36 和强度调制器 37。从而驱动器 36 可以根据预设的强度比例，对强度调制器 37 进行驱动，以使得强度调制器 37 能够将经过的第一偏振光和第二偏振光中参考光的光强，和量子光的光强调制为预设的强度比例。

当发送设备生成两个调制信号，且采用时分模式时，发送设备的结构可以如图 6C 所示，包括光源 1，调制信号生成模块 2 以及调制模块 3。

10 与图 6A 所示的发送设备的结构相比，调制信号生成模块 2 包括随机信号源 21、随机信号源 22、参考数据输出模块 23、参考数据输出模块 26、数据合并器 24、数据合并器 27、数据转换器 25 以及数据转换器 28。

15 其中，随机信号源 21 生成并输出第一随机数据，参考数据输出模块 23 输出该至少两个参考数据中用于调制第一偏振方向上的分量的序列。数据合并器 24 将第一随机数据和该至少两个参考数据中用于调制第一偏振方向上的分量的序列，按照预设的时分模式进行排列，得到数据子序列 1。然后数据转换器 25 将数据子序列 1 转化为调制信号 1。

20 同理，随机信号源 22 生成并输出第二随机数据，参考数据输出模块 26 输出该至少两个参考数据中用于调制第二偏振方向上的分量的序列。数据合并器 27 将第二随机数据和该至少两个参考数据中用于调制第二偏振方向上的分量的序列，也按照该时分模式进行排列，得到数据子序列 2。然后数据合并器 28 将该数据子序列 2 转换为调制信号 2。

25 例 2，结合上述图 5A，假设随机信号源 21 的第一随机数据包括 3 对数据，为  $\{(a_1, a_2), (a_3, a_4), (a_5, a_6)\}$ ，随机信号源 22 第二随机数据包括 3 对数据，为  $\{(b_1, b_2), (b_3, b_4), (b_5, b_6)\}$ 。参考数据输出模块 23 输出了两个用于调制第一偏振方向上的分量的序列  $(X_1, X_2)^T$ ，和  $(X_3, X_4)^T$ 。参考数据输出模块 26 输出了两个用于调制第二偏振方向上的分量的序列  $(Y_1, Y_2)^T$ ，和  $(Y_3, Y_4)^T$ 。

30 预设的时分模式为：包括 6 个参考信号和 3 个量子信号，按照光脉冲的时间顺序，在时域上的分布情况是按照 2 个参考信号和 1 个量子信号为一组，将 6 个参考信号和 3 个量子信号划分为 3 组信号，将该 3 组信号依次排列，每一组中按照“参考信号，量子信号，参考信号”的顺序排列。

35 那么，数据合并器 24 根据该预设的时分模式，先对第一随机数据和两个用于调制第一偏振方向上的分量的序列进行排列，得到的数据子序列 1 为  $\{(X_1, X_2), (a_1, a_2), (X_3, X_4), (X_1, X_2), (a_3, a_4), (X_3, X_4), (X_1, X_2), (a_5, a_6), (X_3, X_4)\}$ ，然后数据转换器 25 将数据子序列 1 转换为对应的电压序列，得到调制信号 1。

那么，数据合并器 27 也根据该预设的时分模式，先对第二随机数据和两个用于调制第二偏振方向上的分量的序列进行排列，得到的数据子序列 2 为  $\{(Y_1, Y_2), (b_1, b_2), (Y_3, Y_4), (Y_1, Y_2), (b_3, b_4), (Y_3, Y_4), (Y_1, Y_2), (b_5, b_6), (Y_3, Y_4)\}$ 。然后数据合并器 28

将该数据子序列 2 转换对应的电压序列，得到调制信号 2。

双偏振方向调制模块 3 包括偏振分束器 32、强度调制器 33、相位调制器 34、驱动器 35、强度调制器 38、相位调制器 39、驱动器 310、延时器 311、90° 偏振旋转器 35 以及偏振分束器 312。

5 其中，脉冲模块 12 输出的第一激光信号从偏振分束器 32 的 321 端进入偏振分束器 32。偏振分束器 32 将第一激光信号一分为二，得到第一路偏振光和第二路偏振光。第一路偏振光从偏振分束器 32 的 322 端输出，延保偏光纤传输。当经过强度调制器 33 和相位调制器 34 时，驱动器 35 根据调制信号 1 对强度调制器 33 和相位调制器 34 进行驱动，以使得强度调制器 33 和相位调制器 34 按照调制信号 1 中的电压序列对经  
10 过的第一路偏振光进行调制，以将数据子序列 1 加载在第一路偏振光上。第一路偏振光经过强度调制器 33 和相位调制器 34 的调制后，经过延时器 311，由延时器 311 对第一路偏振光到达偏振分束器 312 的时间进行控制，以使得第一路偏振光和第二路偏振光同时到达偏振分束器 312。第一路偏振光延时器 11 后，继续沿着保偏光纤传输，从偏振分束器 312 的 3121 端进入偏振分束器 312。

15 第二路偏振光从偏振分束器 32 的 323 端输出，沿着保偏光纤传输，当经过强度调制器 38 和相位调制器 39 时，驱动器 310 根据调制信号 2 对强度调制器 38 和相位调制器 39 进行驱动，以使得强度调制器 38 和相位调制器 39 按照调制信号 2 中的电压序列对经过的第二路偏振光进行调制，以将数据子序列 2 加载在第二路偏振光上。第二路偏振光经过强度调制器 38 和相位调制器 39 的调制后，经过 90° 偏振旋转器 35 旋转  
20 90°，以使得第二路偏振光和第一路偏振光保持相互垂直。第二路偏振光经过 90° 偏振旋转器 35 后，从偏振分束器 312 的 3122 端进入偏振分束器 312。之后，偏振分束器 312 对第一路偏振光和第二路偏振光进行合束，得到第二激光信号，并通过偏振分束器 312 的 3123 端输出至信道。

25 可选的，结合图 6C，如图 6D 所示，为了得到不同强度的参考光和量子光，还可以在过偏振分束器 312 的 3123 端增加驱动器 36 和强度调制器 37。驱动器 36 根据预设的强度比例，对强度调制器 37 进行驱动，以使得强度调制器 37 能够将经过的第二激光信号中参考光的光强，和量子光的光强调制为预设的强度比例。

当发送设备生成二个调制信号，且采用频分模式时，发送设备的结构可以如图 6E 所示，包括光源 1，调制信号生成模块 2 以及双偏振方向调制模块 3。

30 与如图 6C 所示的发送设备的结构相比，调制信号生成模块 2 中数据合并器 24 将第一随机数据和该至少两个参考数据中用于调制第一偏振方向上的分量的序列，按照“一个光脉冲中频率为  $\omega_{r1}, \omega_{r2}$  的两个光为参考光，频率为  $\omega_s$  的光为量子光”的组合模式进行排列，得到数据子序列 3。并由数据转换器 25 将数据子序列 3 转化为调制信号 1。数据合并器 27 将第二随机数据和该至少两个参考数据中用于调制第二偏振方向上的分量的序列，也按照“一个光脉冲中频率为  $\omega_{r1}, \omega_{r2}$  的两个光为参考光，频率为  $\omega_s$  的光为量子光”的组合模式进行排列，得到数据子序列 4。并由数据合并器 28 将该数据子序列 4 转换为调制信号 2。

例 3，结合上述图 5B，假设随机信号源 21 的第一随机数据包括 1 对数据，为  $(a_1, a_2)$ ，随机信号源 22 第二随机数据包括 1 对数据，为  $(b_1, b_2)$ 。参考数据输出模块 23 输出了

两个用于调制第一偏振方向上的分量的序列  $(X_1, X_2)^T$ ，和  $(X_3, X_4)^T$ 。参考数据输出模块 26 输出了两个用于调制第二偏振方向上的分量的序列  $(Y_1, Y_2)^T$ ，和  $(Y_3, Y_4)^T$ 。

5 预设的频分模式为：包括 2 个参考信号和 1 个量子信号，按照一个光脉冲的频域划分  $(\omega_{r1}, \omega_{r2}, \omega_{r3})$ ，在频域上的分布情况是按照“第一个参考信号，第二个参考信号，量子信号”的顺序排列。即第一个参考信号调制频率为  $\omega_{r1}$  的光，第二个参考信号调制频率为  $\omega_{r2}$  光，量子信号调制频率为  $\omega_{r3}$  光。

10 那么，数据合并器 24 根据该预设的频分模式，先对第一随机数据和两个用于调制第一偏振方向上的分量的序列进行排列，得到的数据子序列 3 为  $\{(X_1, X_2), (X_3, X_4), (a_1, a_2)\}$ 。然后数据转换器 25 将数据子序列 3 转换为对应的电压序列，得到调制信号 3。

数据合并器 27 也根据该预设的频分模式，先对第二随机数据和两个用于调制第二偏振方向上的分量的序列进行排列，得到的数据子序列 4 为  $\{(Y_1, Y_2), (Y_3, Y_4), (b_1, b_2)\}$ 。然后数据合并器 28 将该数据子序列 4 转换为对应的电压序列，得到调制信号 4。

15 双偏振方向调制模块 3 包括驱动器 35、驱动器 310、DPQPSK 调制器 313。其中，DPQPSK 调制器有两组输入，驱动器 35 通过调制信号 3，驱动 DPQPSK 调制器 313，以使得 DPQPSK 调制器 313 将数据子序列 3 加载在第一偏振方向的光上。驱动器 310 通过调制信号 4，驱动 DPQPSK 调制器 313，以使得 DPQPSK 调制器 313 将数据子序列 4 加载在第二偏振方向的光上。

20 结合上述例 3，可知，双偏振方向调制模块 3 采用调制信号 3 和调制信号 4 对第一激光信号中的 1 个光脉冲进行调制后，即可如图 5B 所示的第二激光信号中。其中，第二激光信号中的光脉冲中频率为  $\omega_{r1}$  的光为第一个参考光，第一个参考光在第一偏振方向上的 x 分量加载了  $X_1$ ，在第一偏振方向上的 p 分量加载了  $X_2$ ，在第二偏振方向上的 x 分量加载了  $Y_1$ ，在第一偏振方向上的 p 分量加载了  $Y_2$ ；该光脉冲中频率为  $\omega_{r2}$  的光为第二个参考光，第二个参考光在第一偏振方向上的 x 分量加载了  $X_3$ ，在第一偏振方向上的 p 分量加载了  $X_4$ ，在第二偏振方向上的 x 分量加载了  $Y_3$ ，在第一偏振方向上的 p 分量加载了  $Y_4$ ；该光脉冲中频率为  $\omega_{r3}$  的光为量子光，该量子光在第一偏振方向上的 x 分量加载了  $a_1$ ，在第一偏振方向上的 p 分量加载了  $a_2$ ，在第二偏振方向上的 x 分量加载了  $b_1$ ，在第二偏振方向上的 p 分量加载了  $b_2$ 。

30 可以看出，通过频分模式，使得每个光脉冲都可以传递 2 个随机数据，因此使得量子信号率达到了 2 信号/脉冲。

步骤 405，发送设备发送该第二激光信号。

发送设备通过将第二激光信号发送至光纤信道中，传输至接收设备。

35 步骤 406，接收设备对该第二激光信号进行相干探测，以从量子光中获取第三随机数据和第四随机数据，并从参考光中获取探测数据。

在本申请中，接收设备可以将第二激光信号一分为二，得到该第二激光信号在第一偏振方向上的光和在第二偏振方向上的光。然后接收设备可以通过本地本振光 (Locally Local Oscillator, LLO) 分别对该第二激光信号在两个偏振方向上的光进

行干涉，以获取第三随机数据、第四随机数据和探测数据。

示例性的，如图 7A 所示，为接收设备的一种可能的结构示意图，包括偏振分束器 4、光源 5、延时器 6 和延时器 7 和相干探测模块 8。

5 接收设备从信道接收到第二激光信号后，通过偏振分束器 4 将第二激光信号一分为二，得到该第二激光信号在第一偏振方向上的光（以下简称第一偏振光）和在第二偏振方向上的光（以下简称第二偏振光）。

光源 5 包括激光源 51、脉冲模块 52 以及分束器 53。其中，激光源 51 生成连续波，然后由脉冲模块将该连续波转换成光脉冲，得到 LL0。在本示例中，分束器 53 是偏振分束器，用于将得到的 LL0 进行分束，得到两个偏振方向上的 LL0（以下简称为第一 LL0 和第二 LL0）。

需要说明的是，接收设备使用的 LL0 可以是连续光，也可以是脉冲光，在本示例中，以脉冲光为例进行说明。

延时器 6 用于控制减小第一 LL0 与第一偏振光到达相干探测模块 8 的相位差，以使得第一 LL0 能够对第一偏振光进行干涉。

15 延时器 7 用于控制第二 LL0 与第二偏振光同时到达相干探测模块 8，以使得第二 LL0 能够对第二偏振光进行干涉。

相干探测模块 8 包括外差探测器（Heterodyne Detector, HD）81、HD82、模数转换器（Analog-to-digital converter, ADC）83。其中，HD81 与分束器 53 和延时器 6 之间通过保偏光纤连接，第一 LL0 和第一偏振光通过保偏光纤输入 HD81。其中，保偏光纤能够保持第一 LL0 和第一偏振光偏振方向不发生旋转。

20 第一 LL0 和第一偏振光进入 HD81 后，HD81 控制第一 LL0 与第一偏振光发生干涉，以探测第一偏振光上加载的数据。然后由 ADC83 对 HD81 的探测结果进行采集，获取在第一偏振方向上，从量子光上探测到的第三随机数据，和从参考光上探测到的探测数据。

25 同理，HD82 与分束器 53 和延时器 7 之间有也通过保偏光纤连接，第二 LL0 和第二偏振光通过保偏光纤输入 HD82。HD82 控制第二 LL0 与第二偏振光发生干涉，以探测第二偏振光上加载的数据。然后由 ADC83 对 HD82 的探测结果进行采集，获取在第二偏振方向上，从量子光上探测到的第三随机数据，和在参考光上探测到的探测数据。

30 可选的，如图 7B 所示，为接收设备的另一种可能的结构示意图。与如图 7A 所示结构相比，是将图 7A 所示的结构中使用的 HD81 和 HD82，替换为平衡零差探测器（Balanced Homodyne Detector, BHD）84 和 BHD85。并增加随机信号源 86 和随机信号源 87。

35 可选的，接收设备也可以先将第二激光信号划分为第一光信号和第二光信号。然后通过不同的相干探测方式对第一光信号和第二光信号分别进行相干探测。例如，接收设备采用第一相干探测方式（例如，调制 LL0 强度的探测方式），对第一光信号进行相干探测，以该第一光信号中的参考光中获取探测数据（以下称为第一部分探测数据），以及从该第一光信号中的量子光中获取该第三随机数据和该第四随机数据。采用第二相干探测方式（例如，高带宽、低增益的探测方式），对第二光信号进行相干探测，仅探测第二光信号中的参考光，以该第二光信号中的参考光中获取探测数据（以下称为

第二部分探测数据)。

示例性的,接收设备的结构可以如图 7C 所示,包括分束器 9、偏振分束器 4、偏振分束器 10、偏振分束器 11、偏振分束器 12、光源 5、延时器 6、延时器 7、延时器 13、延时器 14 和相干探测模块 8。

5 其中,分束器 9 可以是非平衡的分束器,例如,分束器 9 是透过率较高的分束器,能够将输入的光,划分为 90%的光和 10%的光,并输出。假设,经过信道传输的第二激光信号从分束器 9 的 B 端进入分束器 9,90%的光作为第一光信号从分束器 9 的 B1 端输出,10%的光作为第二光信号从分束器 9 的 B2 端输出。

10 接收设备通过偏振分束器 4 将第一光信号一分为二,得到第一光信号在第一偏振方向上的光(以下简称第一偏振光 1)和在第二偏振方向上的光(以下简称第二偏振光 1)。

接收设备通过偏振分束器 10 将第二光信号一分为二,得到第二光信号在第一偏振方向上的光(以下简称第一偏振光 2)和在第二偏振方向上的光(以下简称第二偏振光 2)。

15 光源 5 包括激光源 51、脉冲模块 52 以及分束器 53。其中,激光源 51 生成连续波,然后由脉冲模块将该连续波转换成光脉冲,得到 LL0。在本示例中,分束器 53 可以是非平衡的分束器,用于对 LL0 进行分束,得到两路 LL0(以下简称为第一路 LL0 和第二路 LL0)。

20 接收设备通过偏振分束器 11 将第一路 LL0 一分为二,得到第一路 LL0 在第一偏振方向上的光(以下简称第一 LL01)和在第二偏振方向上的光(以下简称第二 LL01)。

接收设备通过偏振分束器 12 将第二路 LL0 一分为二,得到第二路 LL0 在第一偏振方向上的光(以下简称第一 LL02)和在第二偏振方向上的光(以下简称第二 LL02)。

延时器 6 用于控制减小第一 LL01 与第一偏振光 1 到达相干探测模块 8 的相位差。

延时器 7 用于控制减小第二 LL01 与第二偏振光 1 到达相干探测模块 8 的相位差。

25 延时器 13 用于控制减小第一 LL02 与第一偏振光 2 到达相干探测模块 8 的相位差。

延时器 14 用于控制减小第二 LL02 与第二偏振光 2 到达相干探测模块 8 的相位差。

30 相干探测模块 8 包括 HD81、HD82、ADC83、HD88、HD89。HD81、HD82 为能够测量量子光的高增益的探测器。第一 LL01 和第一偏振光 1 进入 HD81 后,HD81 控制第一 LL01 与第一偏振光 1 发生干涉,以探测第一偏振光 1 上加载的数据。然后由 ADC83 对 HD81 的探测结果进行采集,以获取第一光信号中量子光在第一偏振方向上的第三随机数据,以及第一光信号中的参考光在第一偏振方向上的探测数据。

35 第二 LL01 和第二偏振光 1 进入 HD82。HD82 控制第二 LL01 与第二偏振光 1 发生干涉,以探测第二偏振光 1 上加载的数据。然后由 ADC83 对 HD82 的探测结果进行采集,以获取第一光信号中量子光在第二偏振方向上的第四随机数据,以及第一光信号中的参考光在第二偏振方向上的探测数据。可以理解的是,第一光信号中的参考光在第一偏振方向上的探测数据和第一光信号中的参考光在第二偏振方向上的探测数据,为第一光信号中参考光上的第一探测数据。

HD88、HD89 为能够对光强较强的参考光进行探测的低增益的探测器。HD88 和 HD89 仅对第二光信号中的参考光进行探测。由于 HD88 和 HD89 的增益低,因此在探测过程

中不易出现饱和现象，从而能够提高对参考光的探测精度。

第一 LL02 和第一偏振光 2 进入 HD88 后，HD88 控制第一 LL02 与第一偏振光 2 发生干涉，以探测第一偏振光 2 中参考光上加载的数据。然后由 ADC83 对 HD88 的探测结果进行采集，以获取第二光信号中参考光在第一偏振方向上的探测数据。

5 第二 LL02 和第二偏振光 2 进入 HD89。HD89 控制第二 LL02 与第二偏振光 2 发生干涉，以探测第二偏振光 2 中参考光上加载的数据。然后由 ADC83 对 HD89 的探测结果进行采集，以获取第二光信号中参考光在第二偏振方向上的探测数据。可以理解的是，第二光信号中的参考光在第一偏振方向上的探测数据和第二光信号中的参考光在第二偏振方向上的探测数据，为第二光信号中参考光上的第二探测数据。

10 步骤 407，接收设备获取参考光的参考数据。

其中，参考光的参考数据为发送设备在调制每一个参考光时使用的参考数据。需要说明的是，接收设备和发送设备都可以预先保存相同的至少两个参考数据，从而当接收设备需要计算第一修正参数时，接收设备即可从该接收设备的存储器中获取每一个参考光的参考数据。

15 可选的，接收设备也可以通过接收发送设备发送的参考数据来获取。

步骤 408，接收设备根据参考光的参考数据和探测数据，计算第一修正参数。

需要说明的是，接收设备在每个计算周期内都会计算一个对应的第一修正参数。即在一个计算周期内，接收设备可以根据该计算周期内的两组参考光的参考数据和探测数据，计算与在该计算周期内信道的变化情况对应第一修正参数。

20 在说明计算第一修正参数的具体实施方式之前，首先简述信道对入射光偏振的旋转效应。一段长光纤可以等价于许多段双折光纤元的级联，每一段的慢轴方向是任意的（参考自书籍《PHOTONICS: Optical Electronics in Modern Communications, Sixth Edition》Amnon Yariv等著），其总的琼斯矩阵可以表示为：

$$J_{\text{fibre}} = \begin{bmatrix} a & b \\ -b^* & a^* \end{bmatrix}$$

25 其中， $a = a_0 e^{i\varphi_a}$ ,  $b = b_0 e^{i\varphi_b}$ ，为两个复系数，且满足  $|a|^2 + |b|^2 = 1$ 。其中， $a_0$ 、 $b_0$  和  $i$  均为信道参数。假设发送设备调制时，入射光在第一偏振方向上的正则分量记为  $(\hat{x}_{b1}, \hat{p}_{b1})$ ，而在第二偏振方向上的正则分量记为  $(\hat{x}_{b2}, \hat{p}_{b2})$ 。经过光纤信道的传输后，输出光在第一偏振方向上（假设为光场模式 c）的正则分量记为  $(\hat{x}_c, \hat{p}_c)$ ，在第二偏振方向上（假设为光场模式 d）的正则分量记为  $(\hat{x}_d, \hat{p}_d)$ ，矩阵 S 表示偏转参数，则输出光和入射光的正则  
30 分量之间存在如下辛变换关系：

$$\begin{pmatrix} \hat{x}_c \\ \hat{p}_c \\ \hat{x}_d \\ \hat{p}_d \end{pmatrix} = S \begin{pmatrix} \hat{x}_{b1} \\ \hat{p}_{b1} \\ \hat{x}_{b2} \\ \hat{p}_{b2} \end{pmatrix} = \begin{pmatrix} a_0 \cos \varphi_a & -a_0 \sin \varphi_a & b_0 \cos \varphi_b & -b_0 \sin \varphi_b \\ a_0 \sin \varphi_a & a_0 \cos \varphi_a & b_0 \sin \varphi_b & b_0 \cos \varphi_b \\ -b_0 \cos \varphi_b & -b_0 \sin \varphi_b & a_0 \cos \varphi_a & a_0 \sin \varphi_a \\ b_0 \sin \varphi_b & -b_0 \cos \varphi_b & -a_0 \sin \varphi_a & a_0 \cos \varphi_a \end{pmatrix} \begin{pmatrix} \hat{x}_{b1} \\ \hat{p}_{b1} \\ \hat{x}_{b2} \\ \hat{p}_{b2} \end{pmatrix}$$

若记矩阵  $R$  为

$$R(\theta) = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$$

则矩阵  $S$  可以简记为

$$5 \quad S(a, b) = \begin{pmatrix} a_0 R(-\varphi_a) & b_0 R(-\varphi_b) \\ b_0 R(\varphi_b) & a_0 R(\varphi_a) \end{pmatrix}$$

第二激光信号经过光纤信道到达接收设备的过程中，除了会发生上述偏振旋转效应，量子光和参考光到达接收设备时，与 LL0 之间还会存在一个未知相位差的。示例性的，若结合如图 7A 或 7B 所示，第二激光信号由偏振分束器 4 分束后得到的第一偏振光和第二偏振光，将经过不同路径与各自 LL0 进行干涉。延时器 6、7 是用来匹配第一偏振光和第二偏振光 10 和各自的 LL0 之间相位差的。但普遍来讲，相位差无法实现完全匹配，因此，假设光场模式  $c$  和光场模式  $d$  与各自 LL0 之间的额外相差为  $\theta_c$  和  $\theta_d$ 。则最终进入相干探测模块 8 的两光场模式  $c'$  和光场模式  $d'$  的正则分量，与光场模式  $c$  和光场模式  $d$  的正则分量之间的关系为（本实施例中暂假设存在发端激光器和收端激光器之间没有频偏）：

$$(\hat{x}_{c'}, \hat{p}_{c'}, \hat{x}_{d'}, \hat{p}_{d'})^T = R(\theta_c, \theta_d) (\hat{x}_c, \hat{p}_c, \hat{x}_d, \hat{p}_d)^T$$

15 其中，

$$R(\theta_c, \theta_d) = \begin{pmatrix} R(\theta_c) & 0 \\ 0 & R(\theta_d) \end{pmatrix}.$$

若发送设备采用如图 6C 或 6D 所示的结构，第一路偏振光和第二路偏振光在通过偏振分束器 312 合束之前，延时器 311 也很难完全补偿第一路偏振光和第二路偏振光的相位差。那么，可以假设第一路偏振光和第二路偏振光在通过偏振分束器 312 合束时的实际相位，相 20 对于调制信号的参考点的差异分别为  $(\theta_a, \theta_b)$  和  $(\theta_c, \theta_d)$ ，则可得到

$$(\hat{x}_{c'}, \hat{p}_{c'}, \hat{x}_{d'}, \hat{p}_{d'})^T = R(\theta_c, \theta_d) \cdot S(a, b) \cdot R(\theta_a, \theta_b) (\hat{x}_{b1}, \hat{p}_{b1}, \hat{x}_{b2}, \hat{p}_{b2})^T$$

综上所述，接收设备最终探测到的量子光上加载的正则分量和发送设备通过调制加载在量子光上的正则分量之间满足的变换关系为：

$$\begin{aligned}
S' &= R(\theta_c, \theta_d) \cdot S(a, b) \cdot R(\theta_a, \theta_b) \\
&= \begin{pmatrix} R(\theta_c) & 0 \\ 0 & R(\theta_d) \end{pmatrix} \begin{pmatrix} a_0 R(-\varphi_a) & b_0 R(-\varphi_b) \\ b_0 R(\varphi_b) & a_0 R(\varphi_a) \end{pmatrix} \begin{pmatrix} R(\theta_a) & 0 \\ 0 & R(\theta_b) \end{pmatrix} \\
&= \begin{pmatrix} a_0 R(-\varphi_a + \theta_c + \theta_a) & b_0 R(-\varphi_b + \theta_c + \theta_b) \\ b_0 R(\varphi_b + \theta_d + \theta_a) & a_0 R(\varphi_a + \theta_d + \theta_b) \end{pmatrix} \\
&= \begin{pmatrix} a_0 R(-\varphi_{a'} + \theta_0) & b_0 R(-\varphi_{b'} + \theta_0) \\ b_0 R(\varphi_{b'} + \theta_0) & a_0 R(\varphi_{a'} + \theta_0) \end{pmatrix} \\
&= R(\theta_0, \theta_0) \cdot S(a', b')
\end{aligned}$$

$$\text{其中, } \varphi_{a'} = \varphi_a - \frac{\theta_c - \theta_d}{2} - \frac{\theta_a - \theta_b}{2}, \quad \varphi_{b'} = \varphi_b - \frac{\theta_c - \theta_d}{2} + \frac{\theta_a - \theta_b}{2}, \quad \theta_0 = \frac{\theta_a + \theta_b + \theta_c + \theta_d}{2},$$

$a' = a_0 e^{i\varphi_{a'}}$ ,  $b' = b_0 e^{i\varphi_{b'}}$ 。  $S'$  代表最终的辛变换矩阵, 即第一修正参数。

5 那么, 接收设备需要根据参考光的探测数据和参考数据计算上述矩阵  $S'$  的各个元素, 或等效的各个未知变量  $a_0, b_0, \varphi_{a'}, \varphi_{b'}, \theta_0$ 。

下面将以一个计算周期为例, 对接收设备根据参考光的参考数据和探测数据, 计算第一修正参数的方式进行示例性的说明。

10 假设, 在一个计算周期内, 两组参考光中第一组参考光的参考数据为  $(x_1, 0, 0, 0)^T$ , 探测数据为  $(M_{c,1}^x, M_{c,1}^p, M_{d,1}^x, M_{d,1}^p)^T$ 。其中,  $(M_{c,1}^x, M_{c,1}^p)^T$  为探测到的第一组参考光在第一偏振方向上的正则分量的平均值,  $(M_{d,1}^x, M_{d,1}^p)^T$  为探测到的第一组参考光在第二偏振方向上的正则分量的平均值。第二组参考光的参考数据为  $(0, 0, x_2, 0)^T$ , 探测数据为  $(M_{c,2}^x, M_{c,2}^p, M_{d,2}^x, M_{d,2}^p)^T$ 。其中,  $(M_{c,2}^x, M_{c,2}^p)^T$  为探测到的第二组参考光在第一偏振方向上的正则分量的平均值,  $(M_{d,2}^x, M_{d,2}^p)^T$  为探测到的第二组参考光在第二偏振方向上的正则分量的平均值。

15 假设信道的衰减在各个方向是均匀的, 综合透过率 (包括信道的衰减率和接收设备内所有仪器设备的衰减率之和) 为  $\eta$ , 且忽略真空噪声的影响。那么, 两组参考光的参考数据和探测数据满足以下方程组:

$$\begin{cases} M_{c,1}^x = \eta a_0 \cos(\varphi_{a'} - \theta_0) x_1 \\ M_{c,1}^p = \eta a_0 \sin(\varphi_{a'} - \theta_0) x_1 \\ M_{d,1}^x = -\eta b_0 \cos(\varphi_{b'} + \theta_0) x_1 \\ M_{d,1}^p = \eta b_0 \sin(\varphi_{b'} + \theta_0) x_1 \end{cases}, \quad \begin{cases} M_{c,2}^x = \eta b_0 \cos(\varphi_{b'} - \theta_0) x_2 \\ M_{c,2}^p = \eta b_0 \sin(\varphi_{b'} - \theta_0) x_2 \\ M_{d,2}^x = \eta a_0 \cos(\varphi_{a'} + \theta_0) x_2 \\ M_{d,2}^p = -\eta a_0 \sin(\varphi_{a'} + \theta_0) x_2 \end{cases}$$

通过对上述方程组进行分析，可以得到：

$$W_1 = (M_{c,1}^x)^2 + (M_{c,1}^p)^2 + (M_{d,1}^x)^2 + (M_{d,1}^p)^2 = (\eta x_1)^2,$$

$$W_2 = (M_{c,2}^x)^2 + (M_{c,2}^p)^2 + (M_{d,2}^x)^2 + (M_{d,2}^p)^2 = (\eta x_2)^2$$

那么通过计算可以得到第一修正参数  $S'$  矩阵为：

$$S' = \begin{pmatrix} M_{c,1}^x/\sqrt{W_1} & -M_{c,1}^p/\sqrt{W_1} & M_{c,2}^x/\sqrt{W_2} & -M_{c,2}^p/\sqrt{W_2} \\ M_{c,1}^p/\sqrt{W_1} & M_{c,1}^x/\sqrt{W_1} & M_{c,2}^p/\sqrt{W_2} & M_{c,2}^x/\sqrt{W_2} \\ M_{d,1}^x/\sqrt{W_1} & -M_{d,1}^p/\sqrt{W_1} & M_{d,2}^x/\sqrt{W_2} & -M_{d,2}^p/\sqrt{W_2} \\ M_{d,1}^p/\sqrt{W_1} & M_{d,1}^x/\sqrt{W_1} & M_{d,2}^p/\sqrt{W_2} & M_{d,2}^x/\sqrt{W_2} \end{pmatrix}$$

5 进一步的，假设将矩阵  $S'$  的第一行和第三行的元素分别依次表示为  $z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8$ ，那么得到的矩阵  $S'$  即为：

$$S' = \begin{pmatrix} z_1 & z_2 & z_3 & z_4 \\ -z_2 & z_1 & -z_4 & z_3 \\ z_5 & z_6 & z_7 & z_8 \\ -z_6 & z_5 & -z_8 & z_7 \end{pmatrix}$$

可以理解的是，当对于任意两组参考光，例如，第一组参考光的参考数据为  $(X_1, X_2, Y_1, Y_2)^T$ ，探测数据为  $(M_{c,1}^x, M_{c,1}^p, M_{d,1}^x, M_{d,1}^p)^T$ ，第二组参考光的参考数据为  $(X_3, X_4, Y_3, Y_4)^T$ ，探测数据为  $(M_{c,2}^x, M_{c,2}^p, M_{d,2}^x, M_{d,2}^p)^T$ 。带入如下方程组，即可求解出第一修正参数  $S'$  中的各个元素：

$$\begin{cases} M_{c,1}^x = \eta(X_1 z_1 + X_2 z_2 + Y_1 z_3 + Y_2 z_4) \\ M_{c,1}^p = \eta(-X_1 z_2 + X_2 z_1 - Y_1 z_4 + Y_2 z_3) \\ M_{d,1}^x = \eta(X_1 z_5 + X_2 z_6 + Y_1 z_7 + Y_2 z_8) \\ M_{d,1}^p = \eta(-X_1 z_6 + X_2 z_5 - Y_1 z_8 + Y_2 z_7) \end{cases}, \begin{cases} M_{c,2}^x = \eta(X_3 z_1 + X_4 z_2 + Y_3 z_3 + Y_4 z_4) \\ M_{c,2}^p = \eta(-X_3 z_2 + X_4 z_1 - Y_3 z_4 + Y_4 z_3) \\ M_{d,2}^x = \eta(X_3 z_5 + X_4 z_6 + Y_3 z_7 + Y_4 z_8) \\ M_{d,2}^p = \eta(-X_3 z_6 + X_4 z_5 - Y_3 z_8 + Y_4 z_7) \end{cases}$$

值得说明的是，由于一个计算周期内的这两组参考光的参考数据  $(X_1, X_2, Y_1, Y_2)^T$  和

$(X_3, X_4, Y_3, Y_4)^T$  组成的矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  是满秩的。因此通过这两组参考光的参考

15 数据和探测数据求解出的  $z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8$  均是唯一的。从而即可与该计算周期对应的第一修正参数  $S'$  矩阵。

可选的，当接收设备的结构如图7C所示时，一方面，第二激光信号中的光脉冲从如图7C所示的A点进入信道，至进入接收设备的HD81（如图7C所示的C1点）和HD82（如图7C所示的C2点），光脉冲在两个偏振方向上的正则分量经历的旋转变化可分为两部分：第一部

分是从A点进入信道，至分束器9的输入端，即如图7C所示的B点（在本示例中分束器9的输出端B1、B2点和B点的状态相同），信道对第二激光信号的偏振旋转效应；第二部分是从分束器9的B1端口出来，至C1点和C2点，第一偏振光1和第二偏振光1的不同的相位差 $\theta_{C1}, \theta_{C2}$ 。

5 那么，当光脉冲在C1点和C2点的正则分量（即第一光信号到达HD81和HD82时，在第一偏振方向上和第二偏振方向上），与在A点时光脉冲在第一偏振方向和第二偏振方向上的正则分量之间的关系，可以表示为如下：

$$(\hat{x}_{C1}, \hat{p}_{C1}, \hat{x}_{C2}, \hat{p}_{C2})^T = R_C S (\hat{x}_{A1}, \hat{p}_{A1}, \hat{x}_{A2}, \hat{p}_{A2})^T$$

其中，

$$S = \begin{pmatrix} a_0 R(-\varphi_a) & b_0 R(-\varphi_b) \\ -b_0 R(\varphi_b) & a_0 R(\varphi_a) \end{pmatrix}, R_C = \begin{pmatrix} R(\theta_{C1}) & 0 \\ 0 & R(\theta_{C2}) \end{pmatrix}.$$

10 另一方面，光脉冲从A点进入信道，到进入接收设备HD88（如图7C所示的D1点）和HD89（如图7C所示的D2点），光脉冲在两个偏振方向上的正则分量经历的旋转变化也可分为两部分：第一部分是从A点进入信道，至到达分束器9的B点，信道对偏振的旋转效应；第二部分是从分束器9的B2端口出来，至D1点和D2点，第一偏振光2和第二偏振光2的不同的相位差 $\theta_{D1}, \theta_{D2}$ 。

15 当光脉冲在D1点和D2点的正则分量（即第二光信号到达HD88和HD89时，在第一偏振方向和第二偏振方向上的正则分量），与在A点时光脉冲在第一偏振方向上和第二偏振方向上的正则分量之间的关系，可以表示为如下：

$$(\hat{x}_{D1}, \hat{p}_{D1}, \hat{x}_{D2}, \hat{p}_{D2})^T = R_D S (\hat{x}_{A1}, \hat{p}_{A1}, \hat{x}_{A2}, \hat{p}_{A2})^T$$

其中，

$$20 \quad R_D = \begin{pmatrix} R(\theta_{D1}) & 0 \\ 0 & R(\theta_{D2}) \end{pmatrix}.$$

可以理解的是，矩阵S是由长距离的信道光纤引起的变化，其变化速率相对较快，而 $R_C$ 、 $R_D$ 是接收设备内部较短的连接光纤引起的变化，其变化速率相对较慢。

当接收设备利用HD88和HD89获得第二探测数据后，即可计算出第二光信号所经历的整的编号矩阵 $S_2$ ， $S_2 = R_D S$ 。

25 对于接收设备利用HD81和HD82对获得的第一探测数据，由于为了测量量子光，HD81和HD82是高增益探测器，在对第一光信号的探测过程中，电噪声的幅度也较大。因此，HD81和HD82对第一光信号中参考光的测量结果的精确度，低于HD88和HD89对第二光信号中参考

光的测量结果的精确度。第一探测数据和第二探测数据之间的关系可以如下所示：

$$(\hat{x}_{C1.ref}, \hat{p}_{C1.ref}, \hat{x}_{C2.ref}, \hat{p}_{C2.ref})^T = R_C R_D^{-1} (\hat{x}_{D1.ref}, \hat{p}_{D1.ref}, \hat{x}_{D2.ref}, \hat{p}_{D2.ref})^T + (\hat{N}_{1x}, \hat{N}_{1p}, \hat{N}_{2x}, \hat{N}_{2p})^T$$

其中， $(\hat{N}_{1x}, \hat{N}_{1p}, \hat{N}_{2x}, \hat{N}_{2p})^T$  相表示噪声（包括真空噪声和电噪声）。

5 由于 $R_C$ 、 $R_D$ 是变化速率相对较慢的矩阵，对相邻较多个计算周期内的参考光具有同样的变换作用。因此，如果将多个相邻周期内的HD81、HD82的测量结果和HD88、HD89的测量结果做互相关操作后，可以得到线性方程组。在本示例中，由于噪声测量的随机性，在互相关操作中取平均时，可以压缩噪声的方差，即降低噪声对估算不确定性的影响。

例如，以两组互相关数据 $\langle \hat{x}_{C1.ref} \hat{x}_{D1.ref} \rangle$ （表示第一光信号中的参考光在第一偏振方向上的x分量，和  
10  $\langle \hat{x}_{C1.ref} \hat{p}_{D1.ref} \rangle$ （表示第一光信号中的参考光在第一偏振方向上的x分量，和第二光信号中的参考光在第一偏振方向上的p分量的乘积的平均值）为例。对这两组数据执行互相关操作，可以得到如下方程组：

$$\begin{aligned} \langle \hat{x}_{C1.ref} \hat{x}_{D1.ref} \rangle &= \cos(\theta_{C1} - \theta_{D1}) \langle \hat{x}_{D1.ref} \hat{x}_{D1.ref} \rangle + \sin(\theta_{C1} - \theta_{D1}) \langle \hat{p}_{D1.ref} \hat{x}_{D1.ref} \rangle + \sum_{\{C1x, C1p, C2x, C2p\}} \langle \hat{N}_k, \hat{x}_{D1.ref} \rangle \\ \langle \hat{x}_{C1.ref} \hat{p}_{D1.ref} \rangle &= \cos(\theta_{C1} - \theta_{D1}) \langle \hat{x}_{D1.ref} \hat{p}_{D1.ref} \rangle + \sin(\theta_{C1} - \theta_{D1}) \langle \hat{p}_{D1.ref}^2 \rangle + \sum_{\{C1x, C1p, C2x, C2p\}} \langle \hat{N}_k, \hat{x}_{D1.ref} \rangle \end{aligned} \quad \text{方程组 (1)}$$

15 由于噪声和任何数据都没有关联，结合噪声在取平均后近似为零的特性，那么上述方程组（1）即可近似表示为方程组（2）。

$$\begin{aligned} \langle \hat{x}_{C1.ref} \hat{x}_{D1.ref} \rangle &= \cos(\theta_{C1} - \theta_{D1}) \langle \hat{x}_{D1.ref} \hat{x}_{D1.ref} \rangle + \sin(\theta_{C1} - \theta_{D1}) \langle \hat{p}_{D1.ref} \hat{x}_{D1.ref} \rangle \\ \langle \hat{x}_{C1.ref} \hat{p}_{D1.ref} \rangle &= \cos(\theta_{C1} - \theta_{D1}) \langle \hat{x}_{D1.ref} \hat{p}_{D1.ref} \rangle + \sin(\theta_{C1} - \theta_{D1}) \langle \hat{p}_{D1.ref}^2 \rangle \end{aligned} \quad \text{方程组 (2)}$$

通过上述方程组（2）即可求解出 $R(\theta_{C1})R^{-1}(\theta_{D1})$ 。

同理，可以根据 $\langle \hat{x}_{C2.ref} \hat{x}_{D2.ref} \rangle$ 和 $\langle \hat{x}_{C2.ref} \hat{p}_{D2.ref} \rangle$ 求解出 $R(\theta_{C2})R^{-1}(\theta_{D2})$ 。那么，根据求解出的 $R(\theta_{C1})R^{-1}(\theta_{D1})$ 以及 $R(\theta_{C2})R^{-1}(\theta_{D2})$ ，就可以求解出矩阵 $R_C R_D^{-1}$ 。

20 进一步的，在得到矩阵 $R_C R_D^{-1}$ 后，就可以计算出量子光到达HD81和HD82时所经历的变换矩阵即：

$$S_1 = R_C S = R_C R_D^{-1} R_D S = R_C R_D^{-1} S_2$$

可以理解的是矩阵 $S_1$ 即为第一修正参数。

25 当接收设备计算得到第一修正参数后，接收设备和/或发送设备即可利用第一修正参数执行数据修正操作，以使得发送设备和接收设备能够确定相同的两个随机数据。

下面将结合 4 种可能的实现方式，对接收设备和/或发送设备即可利用第一修正参数

执行数据修正操作进行示例性的说明。

在一个示例中，如图 4 所示，在上述步骤 408 之后，该方法还包括：

步骤 409，接收设备根据第一修正参数，对第三随机数据和第四随机数据进行数据修正。

5 在该示例中，由接收设备直接对探测到的随机数据进行数据修正操作。以第一修正参数为上述矩阵  $S'$  为例， $(x_{B1}, p_{B1})$  和  $(x_{B2}, p_{B2})$  分别为接收设备探测到的第三随机数据和第四随机数据。接收设备可以将  $(x_{B1}, p_{B1}, x_{B2}, p_{B2})$  与矩阵  $S'$  的逆矩阵  $S'^T$  相乘，得到修正后的第三随机数据  $(x'_{B1}, p'_{B1})$  和第四随机数据  $(x'_{B2}, p'_{B2})$ ，即  $(x'_{B1}, p'_{B1}, x'_{B2}, p'_{B2})^T = S'^T (x_{B1}, p_{B1}, x_{B2}, p_{B2})^T$ 。

10 值得说明的是，假设发送设备在量子光的第一偏振方向上加载的第一随机数据为  $(x_{A1}, p_{A1})$ ，在第二偏振方向上加载的第二随机数据为  $(x_{A2}, p_{A2})$ 。那么， $(x_{B1}, p_{B1}, x_{B2}, p_{B2})$  和  $(x_{A1}, p_{A1}, x_{A2}, p_{A2})$  具有如下关系：

$$(x_{B1}, p_{B1}, x_{B2}, p_{B2})^T = \lambda \cdot S' (x_{A1}, p_{A1}, x_{A2}, p_{A2})^T + (N_{A1x}, N_{A1p}, N_{A2x}, N_{A2p})^T$$

15 其中， $N$  代表真空噪声， $\lambda$  代表与调制方差相关的参数。由于矩阵  $S'$  是么正的，那么根据么正矩阵的特性，可以得到如下变换：

$$\begin{aligned} & (x'_{B1}, p'_{B1}, x'_{B2}, p'_{B2})^T \\ &= S'^T (x_{B1}, p_{B1}, x_{B2}, p_{B2})^T \\ &= \lambda \cdot S'^T S' (x_{A1}, p_{A1}, x_{A2}, p_{A2})^T + S'^T (N_{A1x}, N_{A1p}, N_{A2x}, N_{A2p})^T \\ &= \lambda \cdot (x_{A1}, p_{A1}, x_{A2}, p_{A2})^T + (N'_{A1x}, N'_{A1p}, N'_{A2x}, N'_{A2p})^T \end{aligned}$$

根据么正矩阵的特性，不难算出新的噪声项  $(N'_{A1x}, N'_{A1p}, N'_{A2x}, N'_{A2p})$  中各自的方差仍为一个真空噪声方差，且相互之间是没有关联的。即上述变换保持了各真空噪声的独立性，且该噪声不为窃听者所控制。

20 可以看出，修正后的第三随机数据和第四随机数据，与发送设备生成的第一随机数据与第二随机数据具有最大关联。

可选的，结合图 4，如图 8 所示，在上述步骤 408 之后，该方法还包括：

步骤 410，该接收设备向该发送设备发送该第一修正参数。

25 步骤 411，发送设备根据第一修正参数对第一随机数据和第二随机数据进行数据修正。

在该示例中，由发送设备直接对生成的随机数据进行数据修正操作。以第一修正参数为上述矩阵  $S'$  为例， $(x_{A1}, p_{A1})$  和  $(x_{A2}, p_{A2})$  分别为第一随机数据和第二随机数据，通过将  $(x_{A1}, p_{A1}, x_{A2}, p_{A2})^T$  与矩阵  $S'$  相乘，即可得到修正后的第一随机数据  $(x_{A1}, p_{A1})$  和第二随机数据  $(x_{A2}, p_{A2})$ 。即  $(x_{A1}, p_{A1}, x_{A2}, p_{A2})^T = S' (x_{A1}, p_{A1}, x_{A2}, p_{A2})^T$ 。

30 值得说明的是，在本示例中，由发送设备对随机数据进行修正操作。对于反向协调协议，由于未修正前的随机数据足以完成安全性评估的关键步骤，即评估窃听者获取了多少关于接收设备测量数据的信息。因此，此时发送设备对随机数据进行修正能够使发送设备的随机数据和接收设备的随机数据具有最大关联，以降低纠错所需要的校验信息量。

可选的，结合图 4，如图 9 所示，在上述步骤 408 之后，该方法还包括：

步骤 412，该接收设备向该发送设备发送该第一修正参数。

步骤 413，发送设备获取第二修正参数。

5 步骤 414，发送设备根据第一修正参数和第二修正参数，对第一随机数据和第二随机数据进行数据修正。

假设以第一修正参数为上述矩阵  $S'$ ，第二修正参数为  $S_3$  为例， $(x_{A1}, p_{A1})$  和  $(x_{A2}, p_{A2})$  分别为第一随机数据和第二随机数据，通过将  $(x_{A1}, p_{A1}, x_{A2}, p_{A2})^T$  与矩阵  $S'$  和  $S_3$  相乘，即可得到修正后的第一随机数据  $(x_{A1'}, p_{A1'})$  和第二随机数据  $(x_{A2'}, p_{A2'})$ 。即  $(x_{A1'}, p_{A1'}, x_{A2'}, p_{A2'})^T = S_3 \cdot S' \cdot (x_{A1}, p_{A1}, x_{A2}, p_{A2})^T$ 。

10 步骤 415，接收设备获取第二修正参数。

步骤 416，接收设备根据第二修正参数，将第三随机数据修正为第五随机数据，将第四随机数据修正为第六随机数据。

假设  $(x_{B1}, p_{B1})$  和  $(x_{B2}, p_{B2})$  分别为接收设备探测到的第三随机数据和第四随机数据。接收设备可以将  $(x_{B1}, p_{B1}, x_{B2}, p_{B2})$  与矩阵  $S_3$  相乘，得到修正后的第三随机数据  $(x'_{B1}, p'_{B1})$  和第四随机数据  $(x'_{B2}, p'_{B2})$ ，即  $(x'_{B1}, p'_{B1}, x'_{B2}, p'_{B2})^T = S_3 \cdot (x_{B1}, p_{B1}, x_{B2}, p_{B2})^T$ 。

在该示例中，接收设备和发送设备均对随机数据进行数据修正，以使得修正后的第一随机数据和第二随机数据与修正后的第三随机数据和第四随机数据具有最大关联。

需要说明的是，第二修正参数可以预设于发送设备和/或接收设备中。即，对于发送设备来说，第二修正参数可以与设置在发送设备中，也可以接收接收设备发送的第二修正参数。同理，对于接收设备来说，第二修正参数可以与设置在接收设备中，也可以接收发送设备发送的第二修正参数。

可选的，结合图 4，如图 10 所示，在上述步骤 408 之后，该方法还包括：

步骤 417，发送设备获取第二修正参数。

25 步骤 418，发送设备根据第二修正参数，将第一随机数据修正为第七随机数据，将第二随机数据修正为第八随机数据。

示例性的，假设第二修正参数为  $S_3$ ， $(x_{A1}, p_{A1})$  和  $(x_{A2}, p_{A2})$  分别为第一随机数据和第二随机数据，通过将  $(x_{A1}, p_{A1}, x_{A2}, p_{A2})^T$  与和  $S_3$  相乘，即可得到修正后的第一随机数据  $(x_{A1'}, p_{A1'})$  和第二随机数据  $(x_{A2'}, p_{A2'})$ 。即  $(x_{A1'}, p_{A1'}, x_{A2'}, p_{A2'})^T = S_3 \cdot (x_{A1}, p_{A1}, x_{A2}, p_{A2})^T$ 。

步骤 419，接收设备获取第二修正参数。

30 步骤 420，接收设备根据第一修正参数和第二修正参数，对第三随机数据和第四随机数据进行数据修正。

假设第一修正参数为上述矩阵  $S'$ ， $(x_{B1}, p_{B1})$  和  $(x_{B2}, p_{B2})$  分别为接收设备探测到的第三随机数据和第四随机数据。接收设备可以将  $(x_{B1}, p_{B1}, x_{B2}, p_{B2})$  与矩阵  $S'$  的逆矩阵  $S'^T$  和矩阵  $S_3$  相乘，得到修正后的第三随机数据  $(x'_{B1}, p'_{B1})$  和第四随机数据  $(x'_{B2}, p'_{B2})$ ，即  $(x'_{B1}, p'_{B1}, x'_{B2}, p'_{B2})^T = S_3 \cdot S'^T \cdot (x_{B1}, p_{B1}, x_{B2}, p_{B2})^T$ 。

在该示例中，接收设备和发送设备均对随机数据进行数据修正，以使得修正后的第一随机数据和第二随机数据与修正后的第三随机数据和第四随机数据具有最大关联。

需要说明的是，在步骤 408 之后，上述列举的 4 种数据修正操作择一执行。

可选的，当接收设备和/或发送设备完成数据修正操作之后，接收设备和/或发送设备即可进一步对修正后的随机数据进行后处理操作，例如，测量基比对与数据筛选、参数估计、数据纠错、保密增强等后处理操作。

5 从上述实施例可以看出，采用本申请提供的数据传输方法，发送设备通过对第一激光信号的两个相互垂直的偏振方向上进行调制，使得得到的第二激光信号在这两个偏振方向上，分别加载了两个相互独立的随机数据，由于这两个偏振方向相互垂直，相互之间无串扰，因此，在保证不影响系统安全性的情况下，充分利用了信道资源，将系统的成码率提高了一倍，从而解决了信道资源浪费的问题。

10 参见图 11A，为本申请提供的一种发送设备的一个实施例的结构示意图。所述发送设备用于执行图 4、以及图 8 至图 10 所对应的数据传输方法。

如图 11A 所示，所述发送设备包括：

生成单元 1101，用于生成第一随机数据和第二随机数据。

所述生成单元 1101，还用于确定至少两个参考数据，所述至少两个参考数据中的任意两个参考数据满足以下条件。

15 所述任意两个参考数据中的一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且  $(X_1, X_2, Y_1, Y_2)^T$  与  $(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵

$$\begin{pmatrix} X_1 & X_2 & Y_1 \\ X_2 & -X_1 & Y_2 \\ X_3 & X_4 & Y_3 \\ X_4 & -X_3 & Y_4 \end{pmatrix} \text{ 满秩。}$$

所述生成单元 1101，还用于根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号。

20 调制单元 1102，用于使用所述生成单元 1101 生成的所述调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号，所述第一偏振方向和所述第二偏振方向相互垂直，所述第二激光信号包括量子光和参考光。

25 其中，所述第二激光信号中的每一个计算周期包括一组量子光和两组参考光，所述一组量子光在第一偏振方向上加载了所述第一随机数据，所述一组量子光在第二偏振方向上加载了所述第二随机数据，所述两组参考光中的第一组参考光在第一偏振方向上的 x 分量上加载了  $X_1$ ，所述第一组参考光在第一偏振方向上的 p 分量上加载了  $X_2$ ，所述第一组参考光在第二偏振方向上的 x 分量上加载了  $Y_1$ ，所述第一组参考光在第二偏振方向上的 p 分量上加载了  $Y_2$ ，所述两组参考光中的第二组参考光在第一偏振方向上的 x 分量上加载了  $X_3$ ，所述第二组参考光在第一偏振方向上的 p 分量上加载了  $X_4$ ，  
30 所述第二组参考光在第二偏振方向上的 x 分量上加载了  $Y_3$ ，所述第二组参考光在第二偏振方向上的 p 分量上加载了  $Y_4$ 。

发送单元 1103，用于发送所述第二激光信号。

35 需要说明的是，在本申请中，上述生成单元 1101 可以包括随机数据源、处理器、存储器等。调制单元 1102 可以包括但不限于强度调制器、相位调制器、以及每个调制

器所需的驱动器。还可以包括环形器、分束器、偏振分束器、90°偏振旋转器以及延时器等中的一个或多个器件。发送单元 1103 可以是激光信号经过调制之后的输出端口。

5 可选的，结合图 11A，如图 11B 所示，所述发送设备还包括分束单元 1104。所述分束单元 1104，用于在所述调制单元 1102 使用所述调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号之前，将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光。

可选的，所述分束单元 1104 将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光，具体包括：利用偏振分束器 PBS 或者分束器 BS，将所述第一激光信号分为所述第一偏振方向上的分量光和所述第二偏振方向上的分量光。

10 可以理解的是，本申请中分束单元 1104 可以包括偏振分束器和/或者分束器。

示例性的，调制单元 1102 和分束单元 1104 可以是如图 6A-6E 任一所示的双偏振调制模块 3。可以理解的是，以图 6A 为例，发送单元可以是环形器 31 的输出端口 313。以图 6C 为例，发送单元可以是偏振分束器 312 的输出端口 3123。

15 可选的，所述调制信号的个数为 2，所述调制单元 1102 使用所述调制信号对第一激光信号进行调制，得到第二激光信号，具体包括：将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光；采用两个调制信号中的第一个调制信号对所述第一偏振方向上的分量光进行调制，采用所述两个调制信号中的第二个调制信号对所述第二偏振方向上的分量光进行调制；将调制后的所述第一偏振方向上的分量光进行 90°偏振旋转；将调制后的所述第二偏振方向上的分量光进行延时，使得调制后的所述第一偏振方向上的分量光与调制后的所述第二偏振方向上的分量光在时域上重合；将经过 90°偏振旋转后的所述第一偏振方向上的分量光，和经过延时后的所述  
20 第二偏振方向上的分量光进行合束，得到所述第二激光信号。

可选的，所述生成单元 1101 根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号，具体包括：根据信道特性确定用于产生参考光的信号和用于产生量子光的信号的组合模式，所述信道特性为传输所述第二激光信号的信道的特性；按照所述组合模式将所述第一随机数据、所述第二随机数据以及所述至少  
25 两个参考数据进行排列组合，生成所述调制信号。

30 可选的，所述组合模式为时分模式，所述时分模式包括所述用于产生量子光的信号的数量和所述用于产生参考光的信号的数量，以及所述用于产生量子光的信号和所述用于产生参考光的信号在时域上的分布方式。

可选的，所述组合模式包括频分模式，所述频分模式包括所述用于产生量子光的信号的数量和所述用于产生参考光的信号的数量，以及所述用于产生量子光的信号和所述用于产生参考光的信号在频域上的分布方式。

35 可选的，结合图 11B，如图 11C 所示，所述发送设备还包括接收单元 1105 和修正单元 1106，所述接收单元 1105，用于接收接收设备发送的第一修正参数；所述修正单元 1106，用于根据所述接收单元 1105 接收的所述第一修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

可选的，结合图 11B，如图 11D 所示，所述发送设备还包括接收单元 1105、获取单元 1107 和修正单元 1106。

所述接收单元 1105，用于接收所述接收设备发送的第一修正参数。

所述获取单元 1107，用于获取第二修正参数。

所述修正单元 1106，用于根据所述获取单元 1107 获取的所述第二修正参数和所述接收单元 1105 接收的所述第一修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

可选的，结合图 11B，如图 11E 所示，所述发送设备还包括获取单元 1106 和修正单元 1107。

所述获取单元 1107，用于获取第二修正参数。

所述修正单元 1106，用于根据所述获取单元 1107 获取的所述第二修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

需要说明的是，上述接收单元可以是无线通信接口，也可以是有线通信接口。修正单元和获取单元可以是处理器和存储器的结合。

采用本申请提供的发送设备，通过对第一激光信号在两个相互垂直的偏振方向上进行调制，使得得到的第二激光信号在这偏振方向上，分别加载了两个相互独立的随机数据，由于这两个偏振方向相互垂直，相互之间无串扰，因此，在保证不影响系统安全性的情况下，充分利用了信道资源，将系统的成码率提高了一倍，从而解决了信道资源浪费的问题。

参见图 12A，为本申请提供的一种接收设备的一个实施例的结构示意图。所述接收设备用于执行图 4、以及图 8 至图 10 所对应的数据传输方法。

如图 12A 所示，所述接收设备包括：

接收单元 1201，用于接收第二激光信号，所述第二激光信号包括量子光和参考光。

探测单元 1202，用于对所述接收单元 1201 接收到的所述第二激光信号进行相干探测，以从所述量子光中获取第三随机数据和第四随机数据，以及从所述参考光中获取探测数据。

获取单元 1203，用于获取所述参考光的参考数据，所述参考数据为所述发送设备在调制所述参考光时使用的参考数据。

计算单元 1204，用于根据所述获取单元 1203 获取的所述参考光的参考数据和所述探测单元 1202 探测的所述探测数据，计算第一修正参数。

其中，所述第二激光信号中的每一组量子光和两组参考光为一个计算周期，所述两组参考光中的第一组参考光的参考数据  $(X_1, X_2, Y_1, Y_2)^T$  和所述两组参考光中的第

二组参考光的参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩， $X_1$  为

所述第一组参考光在第一偏振方向上的 x 分量上加载的参考数据， $X_2$  为所述第一组参考光在第一偏振方向上的 p 分量上加载的参考数据， $Y_1$  为所述第一组参考光在第二偏振方向上的 x 分量上加载的参考数据， $Y_2$  为所述第一组参考光在第二偏振方向上的 p 分量上加载的参考数据， $X_3$  为所述第二组参考光在第一偏振方向上的 x 分量上加载的参考数据， $X_4$  为所述第二组参考光在第一偏振方向上的 p 分量上加载的参考数据， $Y_3$

为所述第二组参考光在第二偏振方向上的 x 分量上加载的参考数据， $Y_4$  为所述第二组参考光在第二偏振方向上的 p 分量上加载的参考数据。

需要说明的是，在本申请中，上述接收单元 1201，可以是接收设备与光纤信道连接的接口，例如，是接收设备中与光纤信道连接的 BS 或者 PBS 的输入接口。探测单元  
5 可以包括本地本振光源、BHD、HD、ADC、延时器、分束器、偏振分束器等器件。获取单元和计算单元可以是存储器以及处理器的结合。

示例性的，接收设备的接收单元和探测单元的结构可以参见如图 7A-7C 任一所示的结构示意图。以如 7A 为例，接收单元可以是偏振分束器 4 与信道连接的输入端口。以图 7C 为例，接收单元可以是分束器 9 与信道连接的输入端口。

10 可选的，所述探测数据包括第一部分探测数据和第二部分探测数据，所述探测单元 1202 对所述第二激光信号进行相干探测，以从所述量子光中获取第三随机数据和第四随机数据，以及从所述参考光中获取探测数据，具体包括：将所述第二激光信号划分为第一光信号和第二光信号；采用第一相干探测方式对所述第一光信号进行相干探测，以从所述第一光信号中的参考光中获取所述第一部分探测数据，以及从所述第一  
15 光信号中的量子光中获取所述第三随机数据和所述第四随机数据；采用第二相干探测方式对所述第二光信号进行相干探测，以所述第二光信号中的参考光中获取所述第二部分探测数据。

20 可选的，结合图 12A，如图 12B 所示，所述接收设备还包括发送单元 1205，所述发送单元 1205，用于在所述计算单元 1204 根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，向所述发送设备发送所述计算单元 1204 计算的所述第一修正参数。

需要说明的是，可以是通信接口，例如无线接口，或者有线接口。

可选的，结合图 12A，如图 12C 所示，所述接收设备根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，所述接收设备还包括修正单元 1206。

25 所述修正单元 1206，用于在所述计算单元 1204 根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，根据所述计算单元 1204 计算的所述第一修正参数对所述第三随机数据和所述第四随机数据进行数据修正。

可选的，结合图 12B，如图 12D 所示，所述接收设备还包括修正单元 1206。

30 所述获取单元 1203，还用于在所述探测单元 1202 获取所述第三随机数据和所述第四随机数据之后，获取第二修正参数。

所述修正单元 1206，用于根据所述获取单元 1203 获取的所述第二修正参数对所述第三随机数据和所述第四随机数据进行数据修正。

可选的，结合图 12B，如图 12D 所示，所述接收设备还包括修正单元 1206。

35 所述获取单元 1203，还用于在所述计算单元 1204 根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，获取第二修正参数；

所述修正单元 1206，用于根据所述计算单元 1204 计算的所述第一修正参数和所述获取单元 1203 获取的所述第二修正参数，对所述第三随机数据和所述第四随机数据进行数据修正。

需要说明的是，上述发送单元可以是有线通信接口或者无线通信接口，修正单元

可以是处理器和存储器的结合。

5 从上述实施例可以看出，采用本申请提供的接收设备方法，能够在第二激光信号中获取第三随机数据和第四随机数据。由于发送设备在第二激光信号的两个相互垂直的偏振方向上，分别加载了两个相互独立的随机数据，这两个偏振方向相互垂直，相互之间无串扰，因此，在保证不影响系统安全性的情况下，充分利用了信道资源，将系统的成码率提高了一倍，从而解决了信道资源浪费的问题。。

10 具体实现中，本发明还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时可包括本发明提供的呼叫方法的部分或全部步骤。所述的存储介质可为磁碟、光盘、只读存储记忆体（英文：read-only memory，简称：ROM）或随机存储记忆体（英文：random access memory，简称：RAM）等。

15 本领域的技术人员可以清楚地了解到本发明实施例中的技术可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明实施例中的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行本发明各个实施例或者实施例的某些部分所述的方法。

本说明书中各个实施例之间相同相似的部分互相参见即可。尤其，对于发送设备的实施例和接收设备的而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例中的说明即可。

20 以上所述的本发明实施方式并不构成对本发明保护范围的限定。

# 权 利 要 求 书

1、一种数据传输方法，其特征在于，所述方法包括：

发送设备生成第一随机数据和第二随机数据；

5 所述发送设备确定至少两个参考数据，所述至少两个参考数据中的任意两个参考数据满足以下条件：

所述任意两个参考数据中的一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且  $(X_1, X_2, Y_1, Y_2)^T$  与  $(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵

$$\begin{pmatrix} X_1 & X_2 & Y_1 \\ X_2 & -X_1 & Y_2 \\ X_3 & X_4 & Y_3 \\ X_4 & -X_3 & Y_4 \end{pmatrix} \text{ 满秩；}$$

10 所述发送设备根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号；

所述发送设备使用所述调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号，所述第一偏振方向和所述第二偏振方向相互垂直，所述第二激光信号包括量子光和参考光；

15 其中，所述第二激光信号中的每个计算周期包括每一组量子光和两组参考光，所述一组量子光在第一偏振方向上加载了所述第一随机数据，所述一组量子光在第二偏振方向上加载了所述第二随机数据，所述两组参考光中的第一组参考光在第一偏振方向上的 x 分量上加载了  $X_1$ ，所述第一组参考光在第一偏振方向上的 p 分量上加载了  $X_2$ ，所述第一组参考光在第二偏振方向上的 x 分量上加载了  $Y_1$ ，所述第一组参考光在第二偏振方向上的 p 分量上加载了  $Y_2$ ，所述两组参考光中的第二组参考光在第一偏振方向上的 x 分量上加载了  $X_3$ ，所述第二组参考光在第一偏振方向上的 p 分量上加载了  $X_4$ ，  
20 所述第二组参考光在第二偏振方向上的 x 分量上加载了  $Y_3$ ，所述第二组参考光在第二偏振方向上的 p 分量上加载了  $Y_4$ ；

所述发送设备发送所述第二激光信号。

25 2、根据权利要求 1 所述的方法，其特征在于，所述发送设备使用所述调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号之前，所述方法还包括：

所述发送设备将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光。

30 3、根据权利要求 2 所述的方法，其特征在于，所述发送设备将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光，包括：

所述发送设备利用偏振分束器 PBS 或者分束器 BS，将所述第一激光信号分为所述第一偏振方向上的分量光和所述第二偏振方向上的分量光。

4、根据权利要求 2 或 3 所述的方法，其特征在于，所述调制信号的个数为 2，所述发送设备使用所述调制信号对第一激光信号进行调制，得到第二激光信号，包括：

35 所述发送设备采用两个调制信号中的第一个调制信号对所述第一偏振方向上的分

量光进行调制，采用所述两个调制信号中的第二个调制信号对所述第二偏振方向上的分量光进行调制；

所述发送设备将调制后的所述第一偏振方向上的分量光进行 $90^\circ$ 偏振旋转；

5 所述发送设备将调制后的所述第二偏振方向上的分量光进行延时，使得调制后的所述第一偏振方向上的分量光与调制后的所述第二偏振方向上的分量光在时域上重合；

所述发送设备将经过 $90^\circ$ 偏振旋转后的所述第一偏振方向上的分量光，和经过延时后的所述第二偏振方向上的分量光进行合束，得到所述第二激光信号。

5、根据权利要求1-4任一项所述的方法，其特征在于，所述发送设备根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号，包括：

10 所述发送设备根据信道特性确定用于产生参考光的信号和用于产生量子光的信号的组合模式，所述信道特性为传输所述第二激光信号的信道的特性；

所述发送设备按照所述组合模式将所述第一随机数据、所述第二随机数据以及所述至少两个参考数据进行排列组合，生成所述调制信号。

15 6、根据权利要求5所述的方法，其特征在于，所述组合模式为时分模式，所述时分模式包括所述用于产生量子光的信号的数量和所述用于产生参考光的信号的数量，以及所述用于产生量子光的信号和所述用于产生参考光的信号在时域上的分布方式。

7、根据权利要求5所述的方法，其特征在于，所述组合模式包括频分模式，所述频分模式包括所述用于产生量子光的信号的数量和所述用于产生参考光的信号的数量，以及所述用于产生量子光的信号和所述用于产生参考光的信号在频域上的分布方式。

20 8、根据权利要求1-7任一项所述的方法，其特征在于，所述方法还包括：

所述发送设备接收接收设备发送的第一修正参数；

所述发送设备根据所述第一修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

9、根据权利要求1-7任一项所述的方法，其特征在于，所述方法还包括：

25 所述发送设备接收接收设备发送的第一修正参数；

所述发送设备获取第二修正参数；

所述发送设备根据所述第二修正参数和所述第一修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

10、根据权利要求1-7任一项所述的方法，其特征在于，所述方法还包括：

30 所述发送设备获取第二修正参数；

所述发送设备根据所述第二修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

11、一种数据传输方法，其特征在于，所述方法包括：

35 接收设备接收第二激光信号，所述第二激光信号包括量子光和参考光；

所述接收设备对所述第二激光信号进行相干探测，以从所述量子光中获取第三随机数据和第四随机数据，以及从所述参考光中获取探测数据；

所述接收设备获取所述参考光的参考数据，所述参考数据为所述发送设备在调制所述参考光时使用的参考数据；

5 所述接收设备根据所述参考光的参考数据和所述探测数据，计算第一修正参数；

其中，所述第二激光信号中的每一组量子光和两组参考光为一个计算周期，所述两组参考光中的第一组参考光的参考数据  $(X_1, X_2, Y_1, Y_2)^T$  和所述两组参考光中的第

二组参考光的参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩， $X_1$  为

10 所述第一组参考光在第一偏振方向上的 x 分量上加载的参考数据， $X_2$  为所述第一组参考光在第一偏振方向上的 p 分量上加载的参考数据， $Y_1$  为所述第一组参考光在第二偏振方向上的 x 分量上加载的参考数据， $Y_2$  为所述第一组参考光在第二偏振方向上的 p 分量上加载的参考数据， $X_3$  为所述第二组参考光在第一偏振方向上的 x 分量上加载的参考数据， $X_4$  为所述第二组参考光在第一偏振方向上的 p 分量上加载的参考数据， $Y_3$  为所述第二组参考光在第二偏振方向上的 x 分量上加载的参考数据， $Y_4$  为所述第二组  
15 参考光在第二偏振方向上的 p 分量上加载的参考数据。

12、根据权利要求 11 所述的方法，其特征在于，所述探测数据包括第一部分探测数据和第二部分探测数据，所述接收设备对所述第二激光信号进行相干探测，以从所述量子光中获取第三随机数据和第四随机数据，以及从所述参考光中获取探测数据，包括：

20 所述接收设备将所述第二激光信号划分为第一光信号和第二光信号；

所述接收设备采用第一相干探测方式对所述第一光信号进行相干探测，以从所述第一光信号中的参考光中获取所述第一部分探测数据，以及从所述第一光信号中的量子光中获取所述第三随机数据和所述第四随机数据；

25 所述接收设备采用第二相干探测方式对所述第二光信号进行相干探测，以所述第二光信号中的参考光中获取所述第二部分探测数据。

13、根据权利要求 11 或 12 所述的方法，其特征在于，所述接收设备根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，所述方法还包括：

所述接收设备向所述发送设备发送所述第一修正参数。

30 14、根据权利要求 11 或 12 所述的方法，其特征在于，所述接收设备根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，所述方法还包括：

所述接收设备根据所述第一修正参数对所述第三随机数据和所述第四随机数据进

行数据修正。

15、根据权利要求 13 所述的方法，其特征在于，所述接收设备获取所述第三随机数据和所述第四随机数据之后，所述方法还包括：

所述接收设备获取第二修正参数；

5 所述接收设备根据所述第二修正参数对所述第三随机数据和所述第四随机数据进行数据修正。

16、根据权利要求 13 所述的方法，其特征在于，所述接收设备根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，所述方法还包括：

所述接收设备获取第二修正参数；

10 所述接收设备根据所述第一修正参数和所述第二修正参数，对所述第三随机数据和所述第四随机数据进行数据修正。

17、一种发送设备，其特征在于，包括：

生成单元，用于生成第一随机数据和第二随机数据；

15 所述生成单元，还用于确定至少两个参考数据，所述至少两个参考数据中的任意两个参考数据满足以下条件：

所述任意两个参考数据中的一个参考数据  $(X_1, X_2, Y_1, Y_2)^T$  与另一个参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且  $(X_1, X_2, Y_1, Y_2)^T$  与  $(X_3, X_4, Y_3, Y_4)^T$  构成的矩阵

$$\begin{pmatrix} X_1 & X_2 & Y_1 \\ X_2 & -X_1 & Y_2 \\ X_3 & X_4 & Y_3 \\ X_4 & -X_3 & Y_4 \end{pmatrix} \text{ 满秩；}$$

20 所述生成单元，还用于根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号；

调制单元，用于使用所述生成单元生成的所述调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号，所述第一偏振方向和所述第二偏振方向相互垂直，所述第二激光信号包括量子光和参考光；

25 其中，所述第二激光信号中的每一个计算周期包括一组量子光和两组参考光，所述一组量子光在第一偏振方向上的分量为所述第一随机数据，所述一组量子光在第二偏振方向上的分量为所述第二随机数据，所述两组参考光中的第一组参考光在第一偏振方向上的 x 分量为  $X_1$ ，所述第一组参考光在第一偏振方向上的 p 分量为  $X_2$ ，所述第一组参考光在第二偏振方向上的 x 分量为  $Y_1$ ，所述第一组参考光在第二偏振方向上的 p 分量为  $Y_2$ ，所述两组参考光中的第二组参考光在第一偏振方向上的 x 分量为  $X_3$ ，所述第二组参考光在第一偏振方向上的 p 分量为  $X_4$ ，所述第二组参考光在第二偏振方

30

向上的 x 分量为  $Y_3$ ，所述第二组参考光在第二偏振方向上的 p 分量为  $Y_4$ ；

发送单元，用于发送所述第二激光信号。

18、根据权利要求 15 所述的发送设备，其特征在于，所述发送设备还包括分束单元，

5 所述分束单元，用于在所述调制单元使用所述调制信号对第一激光信号的第一偏振方向上的分量和第二偏振方向上的分量进行调制，得到第二激光信号之前，将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光。

19、根据权利要求 18 所述的方法，其特征在于，所述分束单元将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光，具体包括：

10 利用偏振分束器 PBS 或者分束器 BS，将所述第一激光信号分为所述第一偏振方向上的分量光和所述第二偏振方向上的分量光。

20、根据权利要求 18 或 19 所述的发送设备，其特征在于，所述调制信号的个数为 2，所述调制单元使用所述调制信号对第一激光信号进行调制，得到第二激光信号，具体包括：

15 将所述第一激光信号分为第一偏振方向上的分量光和第二偏振方向上的分量光；  
采用两个调制信号中的第一个调制信号对所述第一偏振方向上的分量光进行调制，  
采用所述两个调制信号中的第二个调制信号对所述第二偏振方向上的分量光进行调制；  
将调制后的所述第一偏振方向上的分量光进行  $90^\circ$  偏振旋转；

20 将调制后的所述第二偏振方向上的分量光进行延时，使得调制后的所述第一偏振方向上的分量光与调制后的所述第二偏振方向上的分量光在时域上重合；

将经过  $90^\circ$  偏振旋转后的所述第一偏振方向上的分量光，和经过延时后的所述第二偏振方向上的分量光进行合束，得到所述第二激光信号。

25 21、根据权利要求 17-20 任一项所述的发送设备，其特征在于，所述生成单元根据所述第一随机数据、所述第二随机数据以及所述至少两个参考数据生成调制信号，具体包括：

根据信道特性确定用于产生参考光的信号和用于产生量子光的信号的组合模式，所述信道特性为传输所述第二激光信号的信道的特性；

按照所述组合模式将所述第一随机数据、所述第二随机数据以及所述至少两个参考数据进行排列组合，生成所述调制信号。

30 22、根据权利要求 21 所述的发送设备，其特征在于，所述组合模式为时分模式，所述时分模式包括所述用于产生量子光的信号的数量和所述用于产生参考光的信号的数量，以及所述用于产生量子光的信号和所述用于产生参考光的信号在时域上的分布方式。

23、根据权利要求 21 所述的发送设备，其特征在于，所述组合模式包括频分模式，

所述频分模式包括所述用于产生量子光的信号的数量和所述用于产生参考光的信号的数量，以及所述用于产生量子光的信号和所述用于产生参考光的信号在频域上的分布方式。

24、根据权利要求 17-23 任一项所述的发送设备，其特征在于，所述发送设备还包括接收单元和修正单元，

所述接收单元，用于接收接收设备发送的第一修正参数；

所述修正单元，用于根据所述接收单元接收的所述第一修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

25、根据权利要求 17-23 任一项所述的发送设备，其特征在于，所述发送设备还包括接收单元、获取单元和修正单元，

所述接收单元，用于接收所述接收设备发送的第一修正参数；

所述获取单元，用于获取第二修正参数；

所述修正单元，用于根据所述获取单元获取的所述第二修正参数和所述接收单元接收的所述第一修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

26、根据权利要求 17-23 任一项所述的发送设备，其特征在于，所述发送设备还包括获取单元和修正单元，

所述获取单元，用于获取第二修正参数；

所述修正单元，用于根据所述获取单元获取的所述第二修正参数，对所述第一随机数据和所述第二随机数据进行数据修正。

27、一种接收设备，其特征在于，包括：  
接收单元，用于接收第二激光信号，所述第二激光信号包括量子光和参考光；

探测单元，用于对所述接收单元接收到的所述第二激光信号进行相干探测，以从所述量子光中获取第三随机数据和第四随机数据，以及从所述参考光中获取探测数据；

获取单元，用于获取所述参考光的参考数据，所述参考数据为所述发送设备在调制所述参考光时使用的参考数据；

计算单元，用于根据所述获取单元获取的所述参考光的参考数据和所述探测单元探测的所述探测数据，计算第一修正参数；

其中，所述第二激光信号中的每一组量子光和两组参考光为一个计算周期，所述两组参考光中的第一组参考光的参考数据  $(X_1, X_2, Y_1, Y_2)^T$  和所述两组参考光中的第

二组参考光的参考数据  $(X_3, X_4, Y_3, Y_4)^T$  不同，且矩阵  $\begin{pmatrix} X_1 & X_2 & Y_1 & Y_2 \\ X_2 & -X_1 & Y_2 & -Y_1 \\ X_3 & X_4 & Y_3 & Y_4 \\ X_4 & -X_3 & Y_4 & -Y_3 \end{pmatrix}$  满秩， $X_1$  为

所述第一组参考光在第一偏振方向上的 x 分量上加载的参考数据,  $X_2$  为所述第一组参考光在第一偏振方向上的 p 分量上加载的参考数据,  $Y_1$  为所述第一组参考光在第二偏振方向上的 x 分量上加载的参考数据,  $Y_2$  为所述第一组参考光在第二偏振方向上的 p 分量上加载的参考数据,  $X_3$  为所述第二组参考光在第一偏振方向上的 x 分量上加载的参考数据,  $X_4$  为所述第二组参考光在第一偏振方向上的 p 分量上加载的参考数据,  $Y_3$  为所述第二组参考光在第二偏振方向上的 x 分量上加载的参考数据,  $Y_4$  为所述第二组参考光在第二偏振方向上的 p 分量上加载的参考数据。

28、根据权利要求 27 所述的接收设备, 其特征在于, 所述探测数据包括第一部分探测数据和第二部分探测数据, 所述探测单元对所述第二激光信号进行相干探测, 以从所述量子光中获取第三随机数据和第四随机数据, 以及从所述参考光中获取探测数据, 具体包括:

将所述第二激光信号划分为第一光信号和第二光信号;

采用第一相干探测方式对所述第一光信号进行相干探测, 以从所述第一光信号中的参考光中获取所述第一部分探测数据, 以及从所述第一光信号中的量子光中获取所述第三随机数据和所述第四随机数据;

采用第二相干探测方式对所述第二光信号进行相干探测, 以所述第二光信号中的参考光中获取所述第二部分探测数据。

29、根据权利要求 27 或 28 所述的接收设备, 其特征在于, 所述接收设备还包括发送单元,

所述发送单元, 用于在所述计算单元根据所述参考光的参考数据和所述探测数据, 计算第一修正参数之后, 向所述发送设备发送所述计算单元计算的所述第一修正参数。

30、根据权利要求 27 或 28 所述的接收设备, 其特征在于, 所述接收设备根据所述参考光的参考数据和所述探测数据, 计算第一修正参数之后, 所述接收设备还包括修正单元,

所述修正单元, 用于在所述计算单元根据所述参考光的参考数据和所述探测数据, 计算第一修正参数之后, 根据所述计算单元计算的所述第一修正参数对所述第三随机数据和所述第四随机数据进行数据修正。

31、根据权利要求 29 所述的接收设备, 其特征在于, 所述接收设备还包括修正单元,

所述获取单元, 还用于在所述探测单元获取所述第三随机数据和所述第四随机数据之后, 获取第二修正参数;

所述修正单元, 用于根据所述获取单元获取的所述第二修正参数对所述第三随机数据和所述第四随机数据进行数据修正。

32、根据权利要求 29 所述的接收设备, 其特征在于, 所述接收设备还包括修正单

元，

所述获取单元，还用于在所述计算单元根据所述参考光的参考数据和所述探测数据，计算第一修正参数之后，获取第二修正参数；

所述修正单元，用于根据所述计算单元计算的所述第一修正参数和所述获取单元  
5 获取的所述第二修正参数，对所述第三随机数据和所述第四随机数据进行数据修正。

33、一种通信系统，其特征在于，包括：

如权利要求 17-26 任一项所述的发送设备，和如权利要求 27-32 任一项所述的接收设备。

10

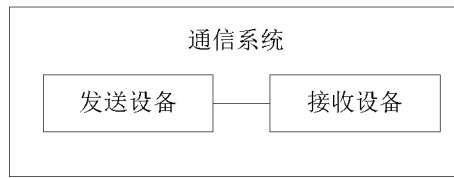


图 1

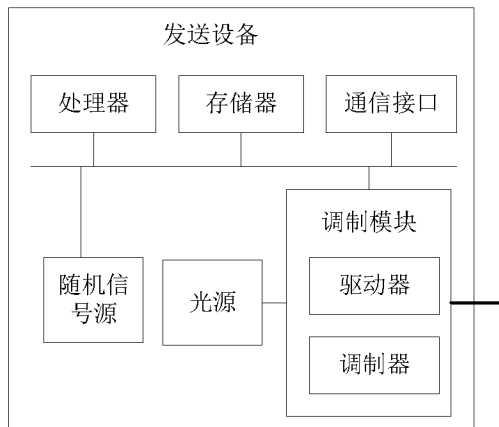


图 2

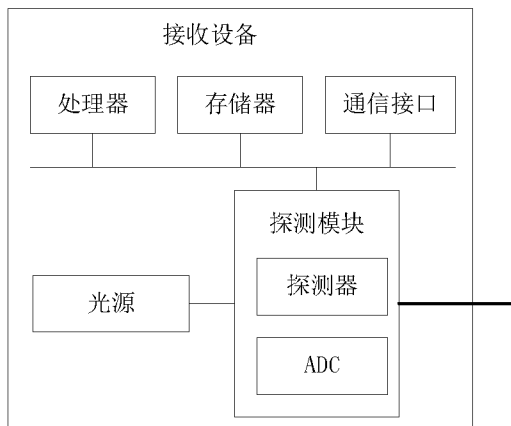


图 3

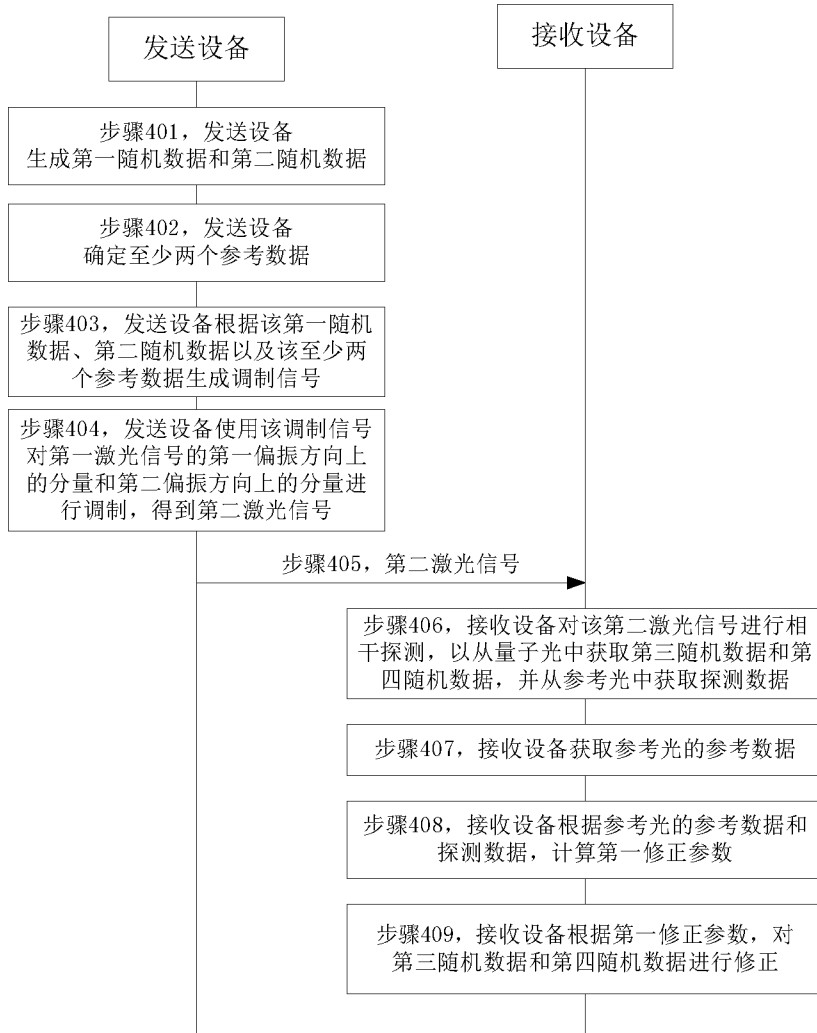


图 4

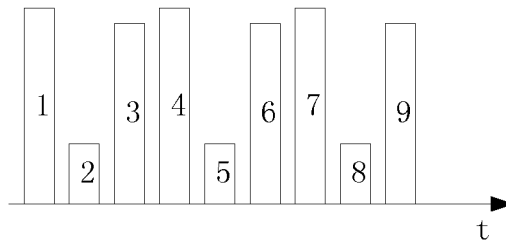


图 5A

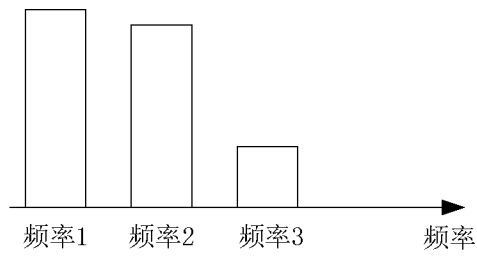


图 5B

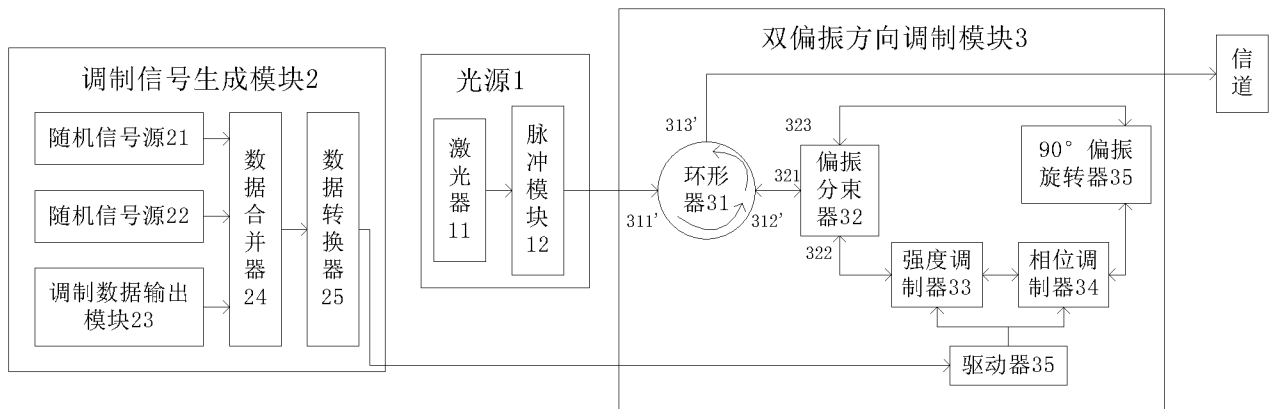


图 6A

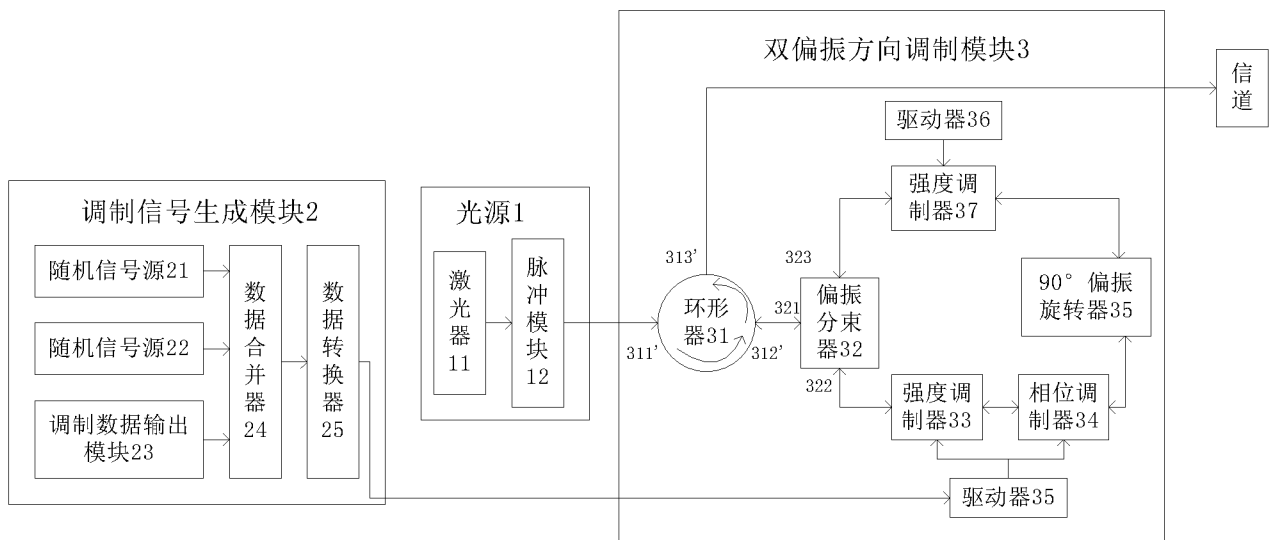


图 6B

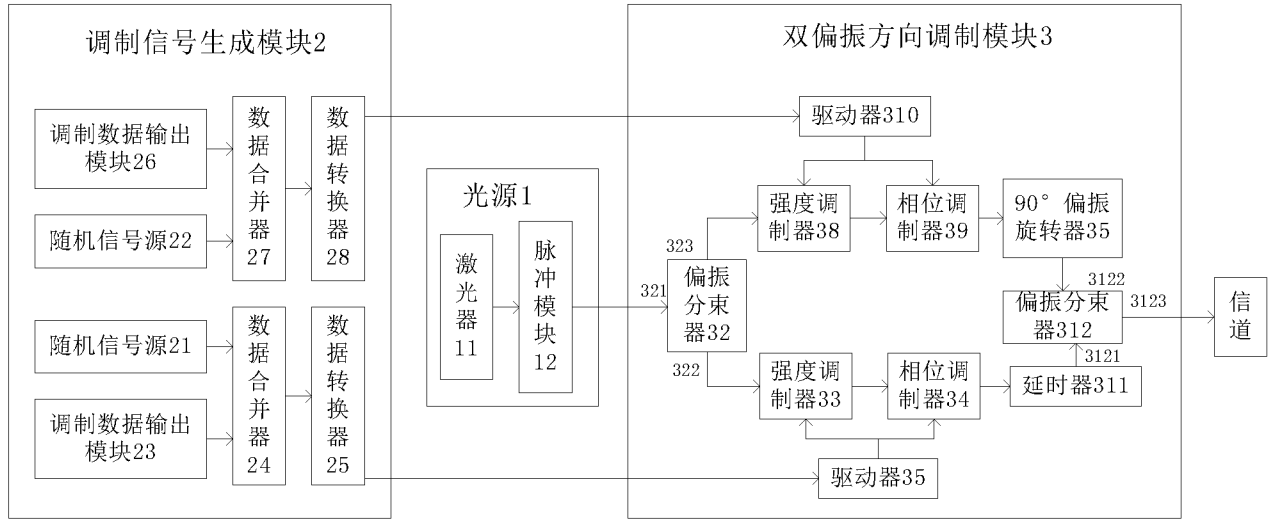


图 6C

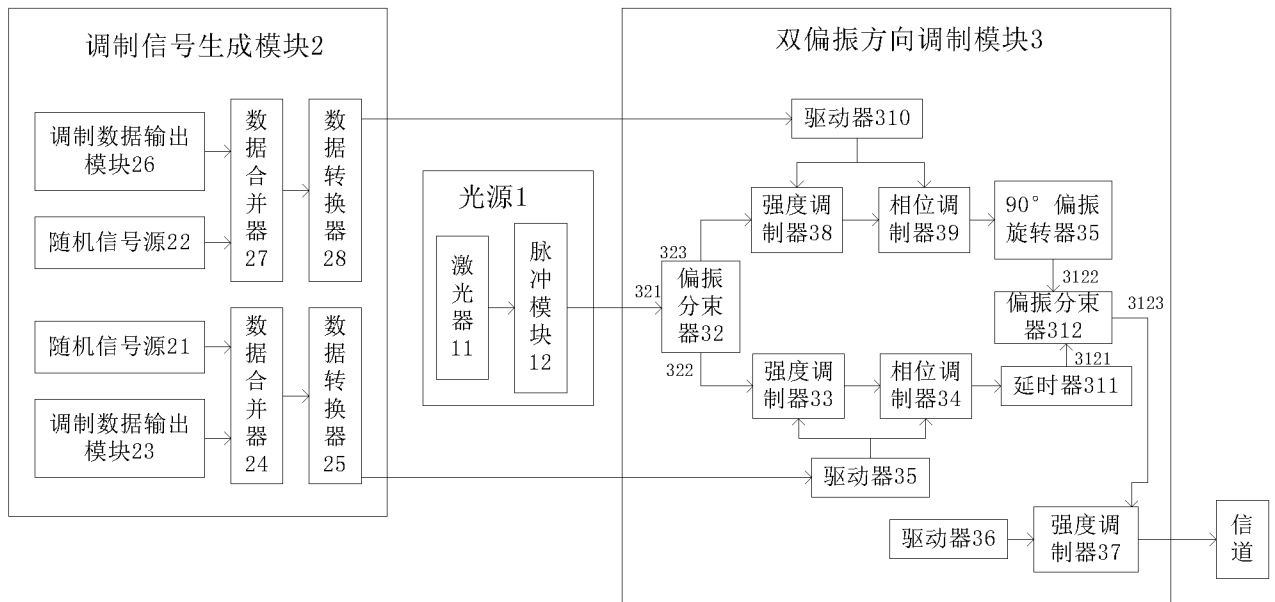


图 6D

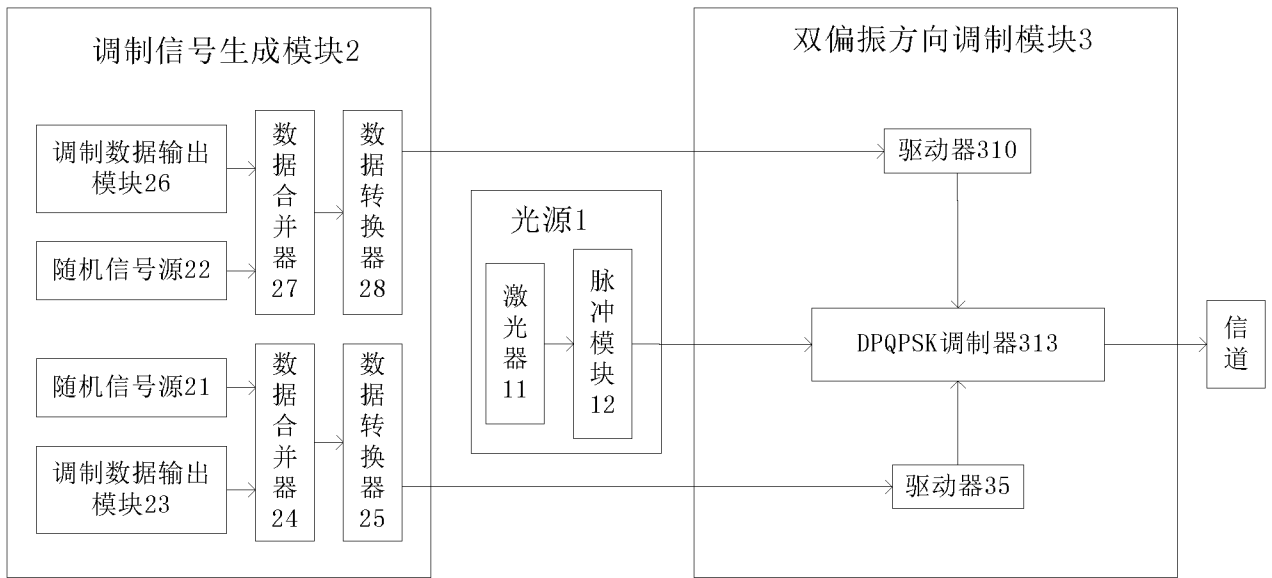


图 6E

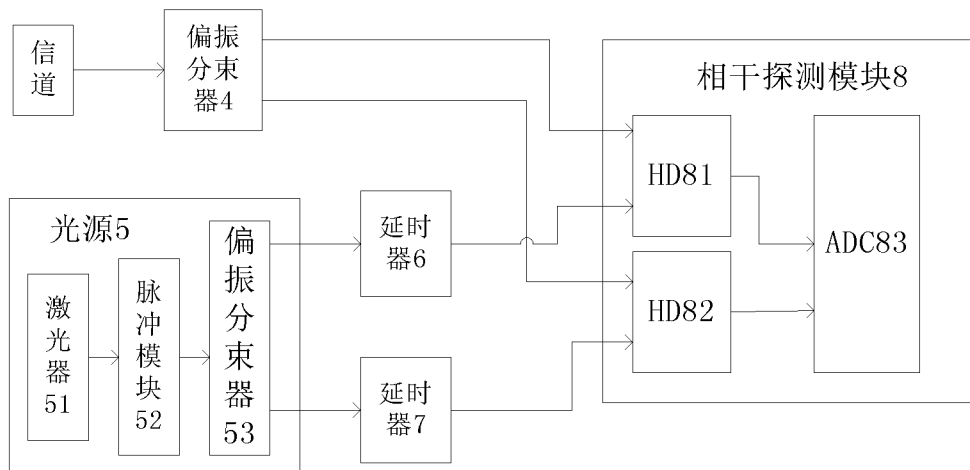


图 7A

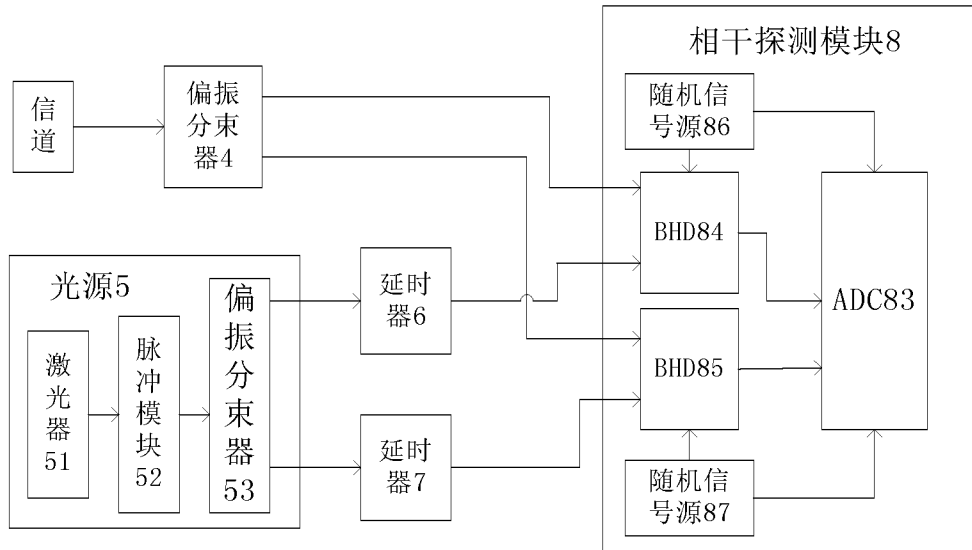


图 7B

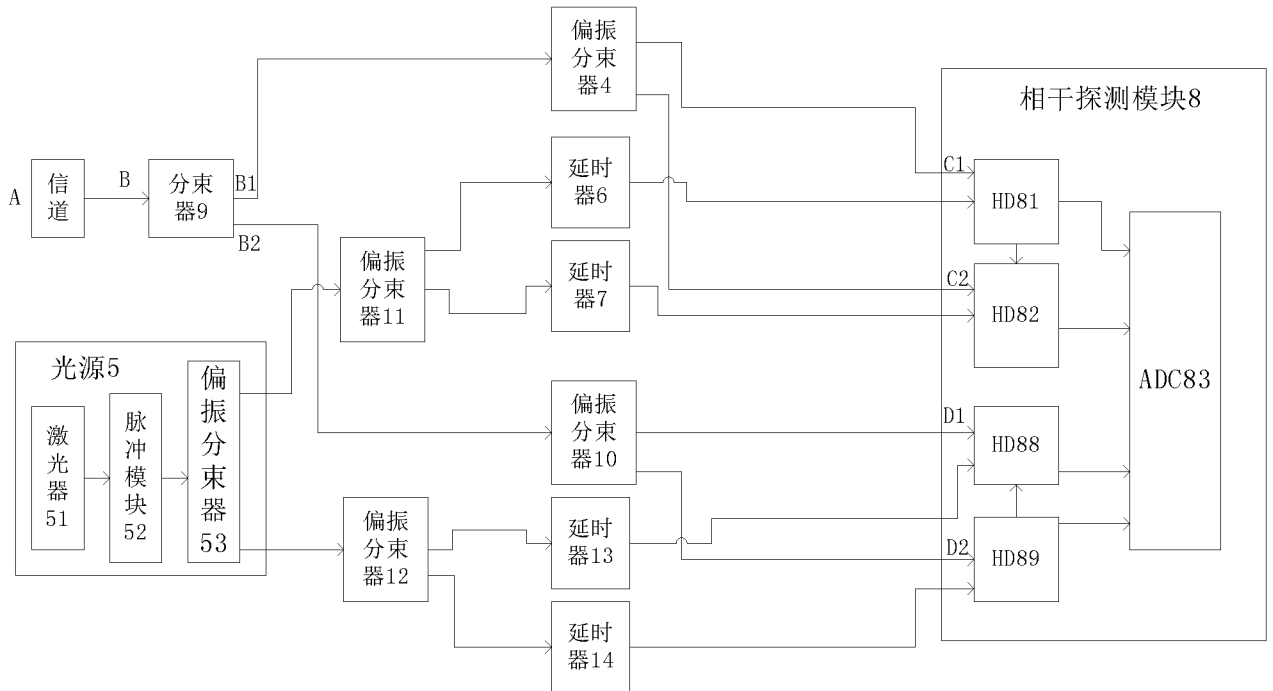


图 7C

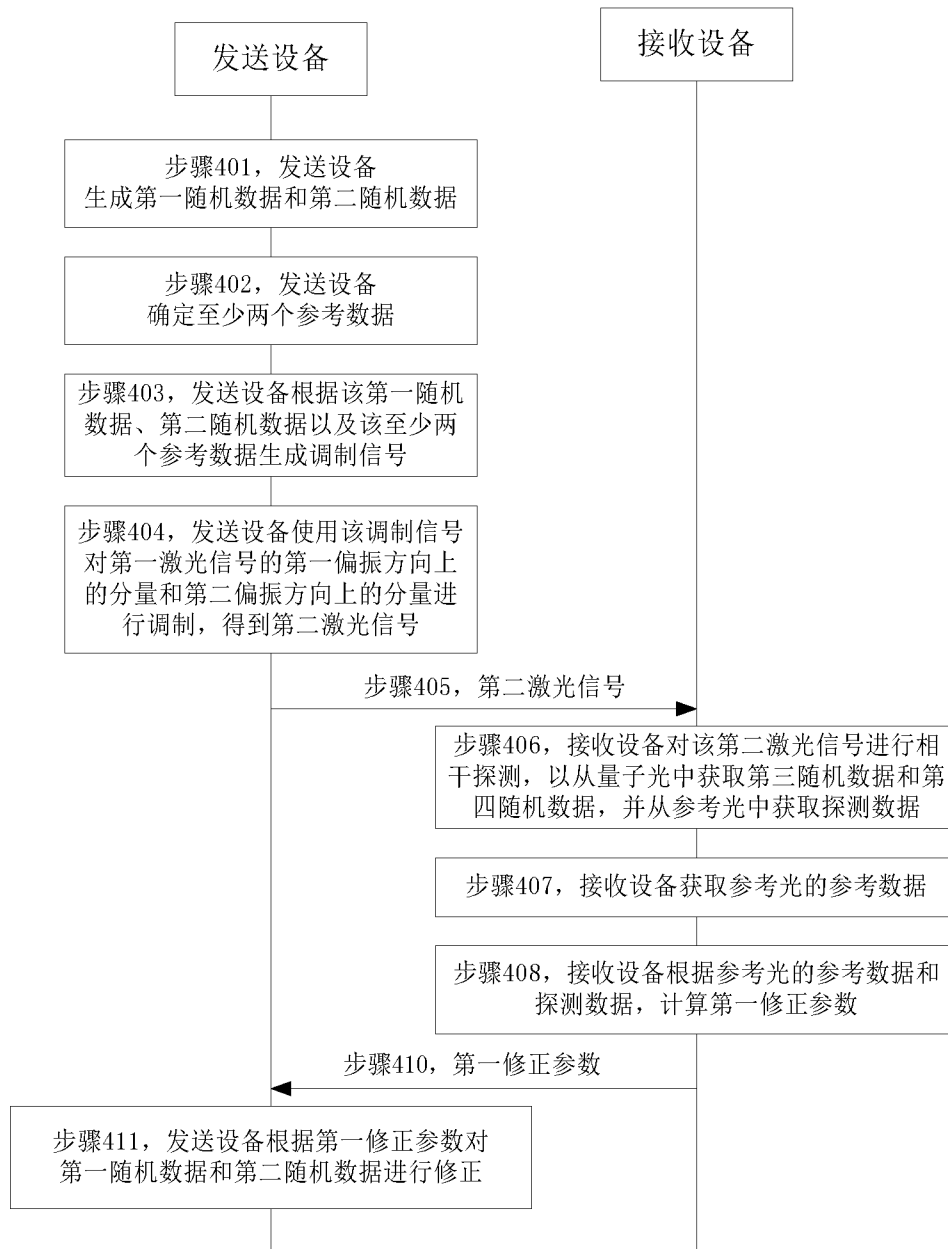


图 8

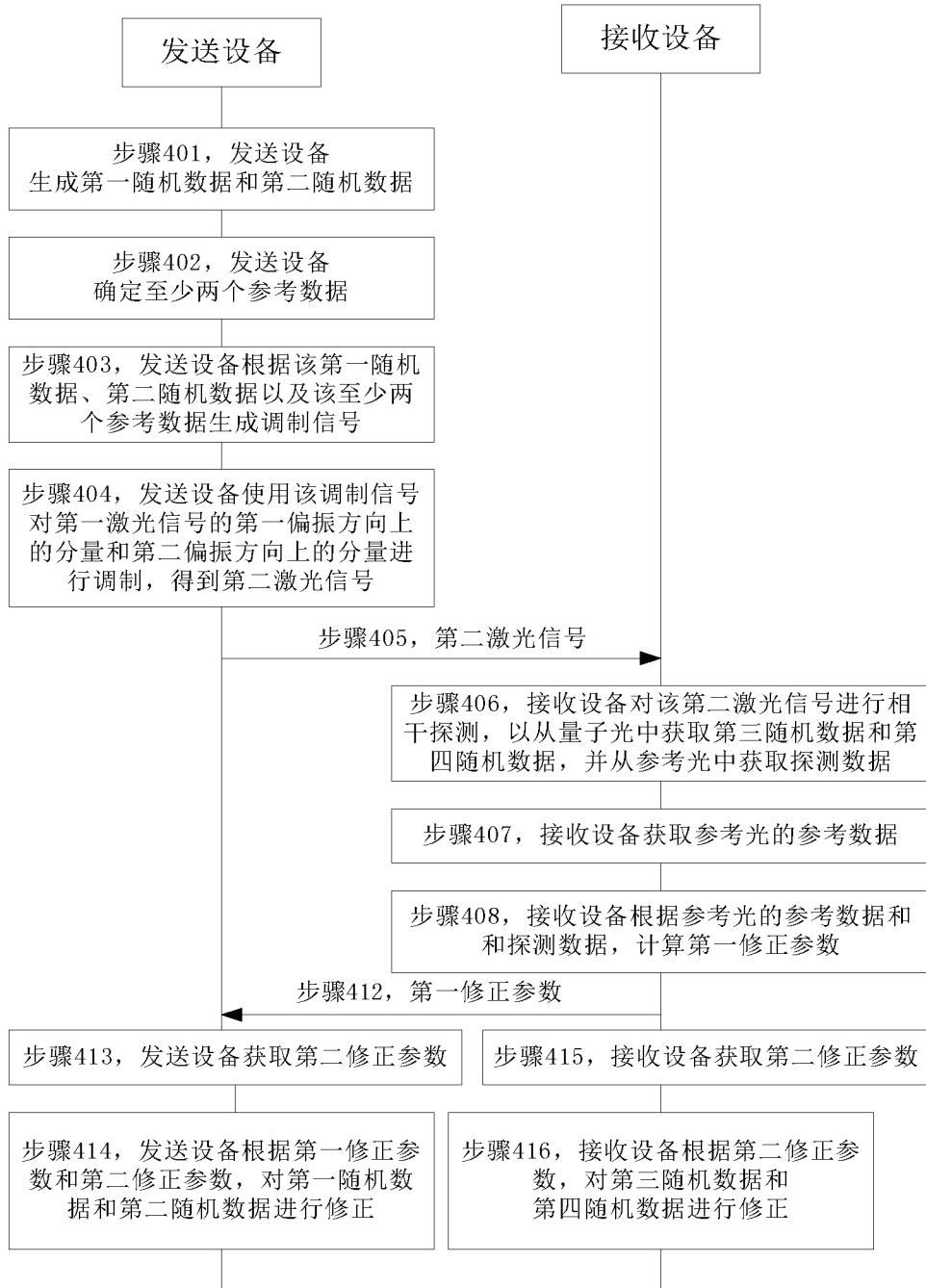


图 9

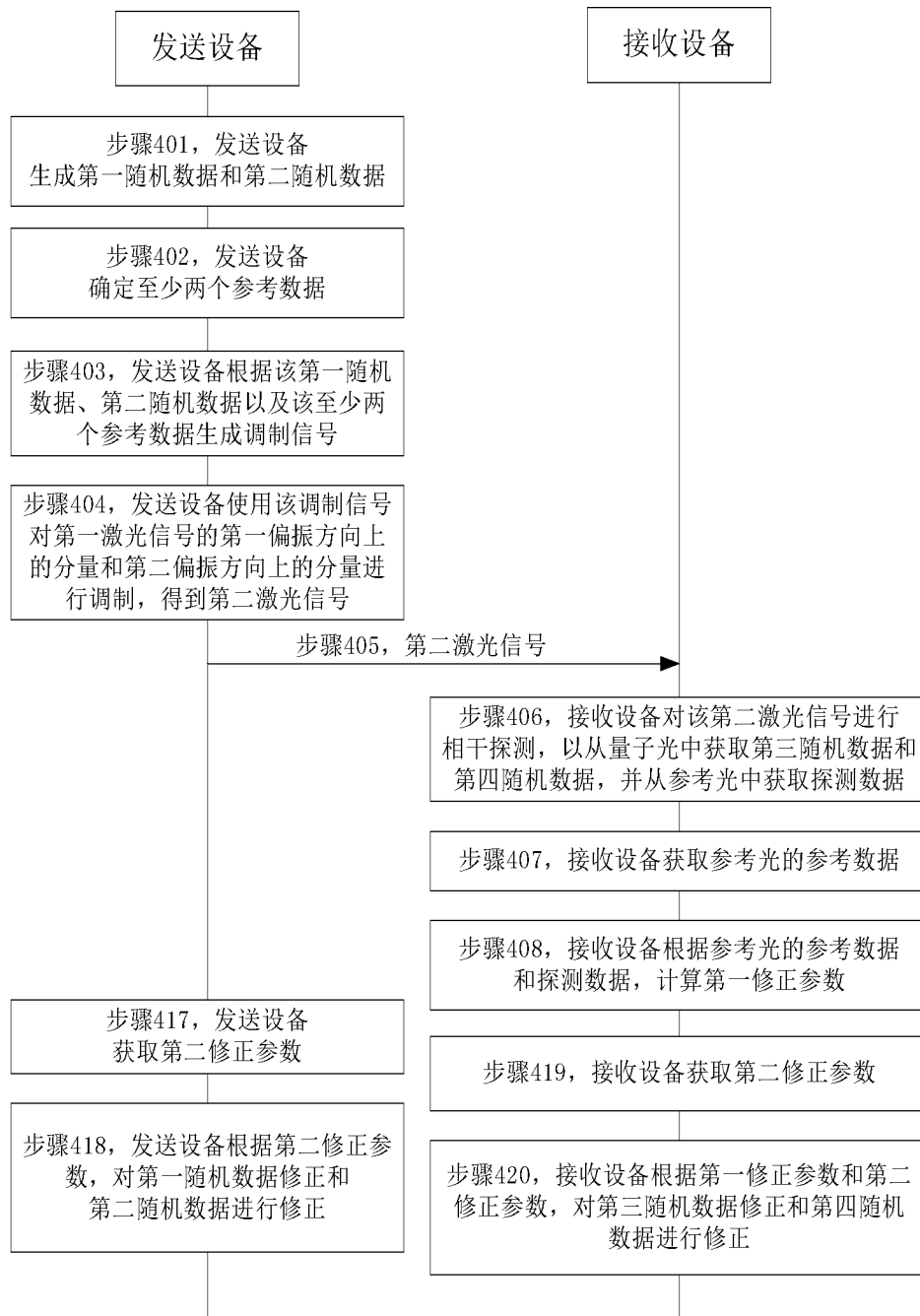


图 10

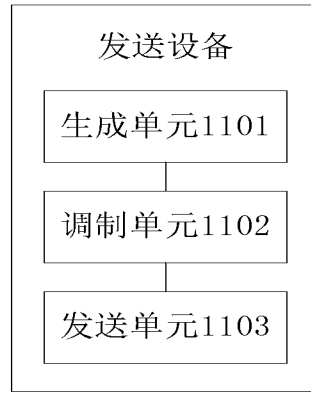


图 11A

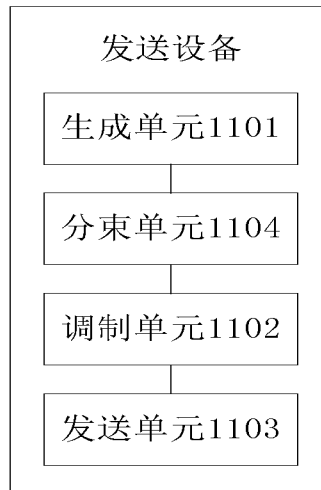


图 11B

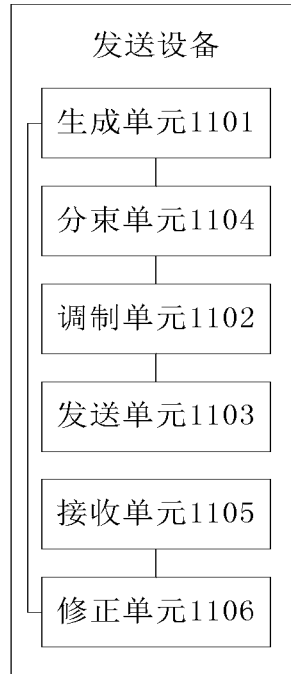


图 11C



图 11D



图 11B

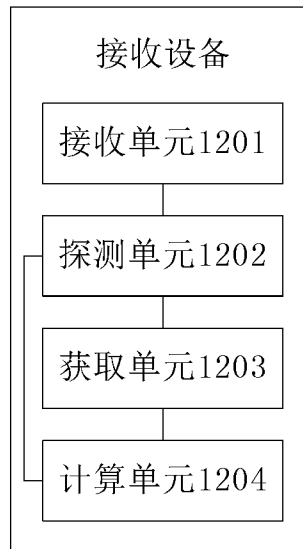


图 12A

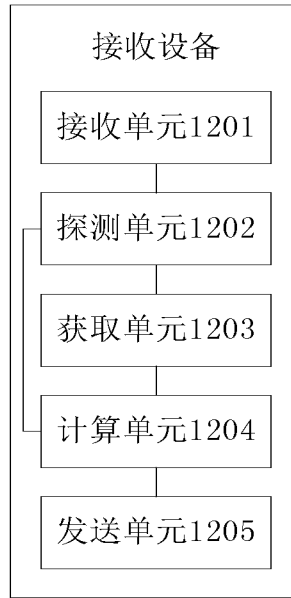


图 12B

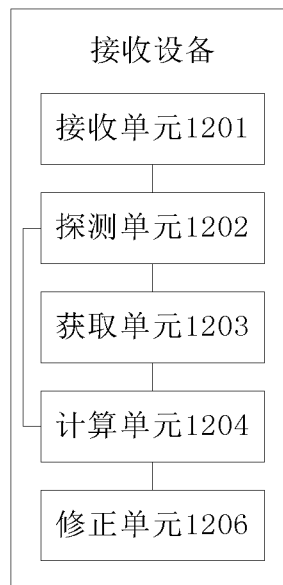


图 12C

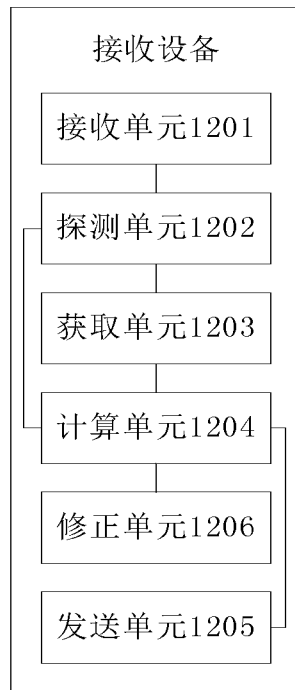


图 12D

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/090544

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
H04B 10/70(2013.01)i		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols)		
H04B,H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT; IEEE; 百度学术, BAIDU SCHOLAR: 自参考连续变量量子密钥分发, 量子密钥分发, 偏振, 第一偏振方向, 第二偏振方向, 参考, 随机, 激光, self-referenced continuous-variable quantum key distribution, quantum key distribution, random, polarizat+, reference, SR-CV-QDK, QDK		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SOH, D.B.S. et al. "Self-Referenced Continuous-Variable Quantum Key Distribution Protocol" <i>Physical Review X</i> , 29 October 2015 (2015-10-29), main text, section 2	1-33
A	CN 106850217 A (SHANXI UNIVERSITY) 13 June 2017 (2017-06-13) entire document	1-33
A	CN 104065475 A (SHANGHAI JIAO TONG UNIVERSITY) 24 September 2014 (2014-09-24) entire document	1-33
A	US 9553677 B1 (SANDIA CORP.) 24 January 2017 (2017-01-24) entire document	1-33
A	WO 2016099565 A1 (NOKIA TECHNOLOGIES OY ET AL) 23 June 2016 (2016-06-23) entire document	1-33
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
30 July 2018		21 August 2018
Name and mailing address of the ISA/CN		Authorized officer
State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088 China		
Facsimile No. (86-10)62019451		Telephone No.

**INTERNATIONAL SEARCH REPORT**  
**Information on patent family members**

International application No.

**PCT/CN2018/090544**

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	106850217	A	13 June 2017	None			
CN	104065475	A	24 September 2014	CN	104065475	B	08 September 2017
US	9553677	B1	24 January 2017	None			
WO	2016099565	A1	23 June 2016	None			

<p><b>A. 主题的分类</b> H04B 10/70 (2013.01) i</p> <p>按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类</p>																				
<p><b>B. 检索领域</b></p> <p>检索的最低限度文献 (标明分类系统和分类号) H04B, H04L</p> <p>包含在检索领域中的除最低限度文献以外的检索文献</p> <p>在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNABS; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT; IEEE; 百度学术: 自参考连续变量量子密钥分发, 量子密钥分发, 偏振, 第一偏振方向, 第二偏振方向, 参考, 随机, 激光, self-referenced continuous-variable quantum key distribution, quantum key distribution, random, polarizat+, reference, SR-CV-QDK, QDK</p>																				
<p><b>C. 相关文件</b></p> <table border="1"> <thead> <tr> <th>类型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>Daniel B. S. Soh 等. "Self-referenced continuous-variable quantum key distribution protocol" Physical Review X, 2015年 10月 29日 (2015 - 10 - 29), 正文第二部分</td> <td>1-33</td> </tr> <tr> <td>A</td> <td>CN 106850217 A (山西大学) 2017年 6月 13日 (2017 - 06 - 13) 全文</td> <td>1-33</td> </tr> <tr> <td>A</td> <td>CN 104065475 A (上海交通大学) 2014年 9月 24日 (2014 - 09 - 24) 全文</td> <td>1-33</td> </tr> <tr> <td>A</td> <td>US 9553677 B1 (SANDIA CORP) 2017年 1月 24日 (2017 - 01 - 24) 全文</td> <td>1-33</td> </tr> <tr> <td>A</td> <td>WO 2016099565 A1 (NOKIA TECHNOLOGIES OY等) 2016年 6月 23日 (2016 - 06 - 23) 全文</td> <td>1-33</td> </tr> </tbody> </table>			类型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	Daniel B. S. Soh 等. "Self-referenced continuous-variable quantum key distribution protocol" Physical Review X, 2015年 10月 29日 (2015 - 10 - 29), 正文第二部分	1-33	A	CN 106850217 A (山西大学) 2017年 6月 13日 (2017 - 06 - 13) 全文	1-33	A	CN 104065475 A (上海交通大学) 2014年 9月 24日 (2014 - 09 - 24) 全文	1-33	A	US 9553677 B1 (SANDIA CORP) 2017年 1月 24日 (2017 - 01 - 24) 全文	1-33	A	WO 2016099565 A1 (NOKIA TECHNOLOGIES OY等) 2016年 6月 23日 (2016 - 06 - 23) 全文	1-33
类型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
A	Daniel B. S. Soh 等. "Self-referenced continuous-variable quantum key distribution protocol" Physical Review X, 2015年 10月 29日 (2015 - 10 - 29), 正文第二部分	1-33																		
A	CN 106850217 A (山西大学) 2017年 6月 13日 (2017 - 06 - 13) 全文	1-33																		
A	CN 104065475 A (上海交通大学) 2014年 9月 24日 (2014 - 09 - 24) 全文	1-33																		
A	US 9553677 B1 (SANDIA CORP) 2017年 1月 24日 (2017 - 01 - 24) 全文	1-33																		
A	WO 2016099565 A1 (NOKIA TECHNOLOGIES OY等) 2016年 6月 23日 (2016 - 06 - 23) 全文	1-33																		
<p><input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。</p>																				
<p>* 引用文件的具体类型:                      "A" 认为不特别相关的表示了现有技术一般状态的文件                      "E" 在国际申请日的当天或之后公布的在先申请或专利                      "L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)                      "O" 涉及口头公开、使用、展览或其他方式公开的文件                      "P" 公布日先于国际申请日但迟于所要求的优先权日的文件                      "T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件                      "X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性                      "Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性                      "&amp;" 同族专利的文件</p>																				
国际检索实际完成的日期	国际检索报告邮寄日期																			
2018年 7月 30日	2018年 8月 21日																			
ISA/CN的名称和邮寄地址	受权官员																			
中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	谭美玲																			
传真号 (86-10) 62019451	电话号码 86-(20)-28950742																			

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2018/090544

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	106850217	A	2017年 6月 13日	无			
CN	104065475	A	2014年 9月 24日	CN	104065475	B	2017年 9月 8日
US	9553677	B1	2017年 1月 24日	无			
WO	2016099565	A1	2016年 6月 23日	无			