基于具有极化和空模自由度的单光子的半量子密钥分配网络协议

叶天语，叶腾琦，马鹏辉，李霞
（浙江工商大学信息与电子工程学院，浙江 杭州 310018）

摘　要：为了使位于网络上不同节点的通信方利用半量子密钥分发技术在整体上组成一个安全的半量子密钥分配网络，提出了一种新颖的具有极化和空模自由度的单光子的半量子密钥分配网络协议。该协议只需单光子而非量子纠缠态作为量子资源，只需进行单光子测量，且无须量子纠缠交换操作、量子延迟线以及哈达玛操作。在该协议中，一个拥有完全量子能力的参与者与每个半量子参与者建立不同密钥，同时又帮助每2个相邻半量子参与者建立不同密钥。该协议可被应用于半量子求和、半量子隐私比较和半量子秘密共享，具有广泛的应用潜力。由于对具有极化和空模自由度的单光子进行制备、测量和施加酉操作在目前技术条件下是很容易实现的，该协议具有良好的实际可行性。

关键词：半量子密码；半量子密钥分配网络；单光子；极化自由度；空模自由度
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025054

Semiquantum key distribution network protocol with single photons in both polarization and spatial-mode degrees of freedom

YE Tianyu, YE Tengqi, MA Penghui, LI Xia
College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

Abstract: In order to make the communicants at different nodes of network use the semiquantum key distribution technology to constitute a secure semiquantum key distribution network as a whole, a novel semiquantum key distribution network protocol was proposed by using single photons with polarization and spatial-mode degrees of freedom. Only single photons rather than quantum entangled states were adopted as quantum resource, only single-photon measurements were required, and none of quantum entanglement swapping operations, quantum delay lines and Hadamard operations were needed. Within the proposed protocol, a participant with full quantum capabilities establishesd a private key with each semiquantum participant, and simultaneously helped two adjacent semiquantum participants to establish a private key between them. The proposed protocol could be applied into semiquantum summation, semiquantum private comparison and semiquantum secret sharing, which meaned that it had extensive application potential. As the preparation, the measurement and the implementation with unitary operations on single photons with polarization and spatial-mode degrees of freedom are all easy to realize under the present technologies, this protocol possesses the good practical feasibility.

Keywords: semiquantum cryptography, semiquantum key distribution network, single photon, polarization degree of freedom, spatial-mode degree of freedom

收稿日期：2024–11–19；**修回日期：**2025–03–11
通信作者：叶天语，yetianyu@zjgsu.edu.cn
基金项目：国家自然科学基金资助项目（No.62071430）；浙江省大学生科技创新活动计划（新苗人才计划）基金资助项目（No.2024R408B082）
Foundation Items: The National Natural Science Foundation of China (No.62071430), Zhejiang Students' Technology and Innovation Program (No.2024R408B082)

0　引言

在信息时代，数据的监听、窃取事件频频发生，给个人隐私、金融安全、国家安全等带来了巨大威胁。因此，数据的安全性已经成为一个极为重要的课题。传统的基于计算复杂度的经典加密算法一直以来是保护数据信息安全的重要基石，但随着量子计算技术的兴起与发展，这些算法正面临着日益严峻的挑战。因此，人们迫切地需要寻找另一种安全而有效的数据保护方案。Bennett 等[1]提出首个量子密钥分配（QKD，quantum key distribution）协议，即著名的 BB84 协议，这标志着量子密码学的诞生。QKD 的功能在于利用量子力学规律在 2 个远距离用户之间建立密钥。目前，随着量子技术的不断进步，许多优秀的 QKD 协议[2-8]又相继被设计出来。QKD 有望成为未来数据保护的核心技术之一。

包括 QKD 在内的量子密码协议往往要求所有用户都具备完全的量子能力，包括制备量子叠加态和量子纠缠态的能力、测量量子叠加态和量子纠缠态的能力、执行酉操作的能力等。这无疑会使所有用户承担起沉重的量子设备负担。为了减轻部分用户的量子设备负担，Boyer 等[9-10]率先提出“半量子”的概念并设计出最初的 2 个半量子密钥分配（SQKD，semiquantum key distribution）协议，这标志着半量子密码学的诞生。“半量子”概念的核心思想是限制协议部分参与者的量子操作能力。在半量子密码协议中，不具备完全量子能力的参与者被称为半量子参与者，半量子参与者被限制只能执行利用 $\{|0\rangle,|1\rangle\}$ 基测量粒子、制备粒子处于 $\{|0\rangle,|1\rangle\}$ 基、通过量子信道传送粒子、置乱粒子以及对粒子施加酉操作等操作[9-11]。目前，许多有趣的 SQKD 协议[9-10,12-22]从不同角度被设计出来。按照用户数量进行划分，SQKD 可被进一步分为两方半量子密钥分配（TSQKD，two-party semiquantum key distribution）[9-10,12-17]和多方半量子密钥分配（MSQKD，multi-party semiquantum key distribution）[18-22]。据笔者所知，目前只有文献[18-22]这几个为数不多的 MSQKD 协议。Zhang 等[18]提出的 MSQKD 协议实现了“量子参与者与一群半量子参与者一起建立同一密钥”的功能；Zhou 等[19]提出的 MSQKD 协议实现了“量子参与者与两群半量子参与者建立不同密钥”的功能；Tian 等[20]提出的 MSQKD 协议具有“量子参与者与一群半量子参与者一起建立同一密钥”的功能；Pan[21]提出的 MSQKD 协议具有“量子参与者与每个半量子参与者建立不同密钥”的功能；Tsai 等[22]提出的 MSQKD 协议具有“量子参与者帮助一个半量子参与者与一群其他半量子参与者一起建立同一密钥”的功能。然而，以上 MSQKD 协议[18-22]都只具备单一功能，在更复杂的拓扑网络结构中未必适用。

鉴于以上分析，为了实现“一个拥有完全量子能力的参与者与每个半量子参与者建立不同密钥，同时又帮助每 2 个相邻半量子参与者建立不同密钥”的功能，本文利用具有极化和空模自由度的单光子构建了一个新颖的半量子密钥分配网络协议。该协议只需单光子作为量子资源且只需进行单光子测量，不需要使用量子纠缠交换操作、量子延迟线以及哈达玛操作，可被应用于半量子求和、半量子隐私比较和半量子秘密共享。

1　协议描述

1.1　预备知识

双自由度单光子相比于单自由度单光子有更大的量子通信容量，所以近年来许多研究者致力于利用双自由度单光子设计高容量量子通信协议。具有极化和空模双自由度的单光子 $|\phi\rangle$ 可被定义为[23]

$$|\phi\rangle=|\phi\rangle_P\otimes|\phi\rangle_S \tag{1}$$

其中，$|\phi\rangle_P\in\{|H\rangle,|V\rangle,|S\rangle,|A\rangle\}$ 和 $|\phi\rangle_S\in\{|b_1\rangle,|b_2\rangle,|s\rangle,|a\rangle\}$ 分别是 $|\phi\rangle$ 的极化态和空模态。$|S\rangle$、$|A\rangle$、$|s\rangle$、$|a\rangle$ 分别为

$$\begin{aligned}|S\rangle&=\frac{1}{\sqrt{2}}\left(|H\rangle+|V\rangle\right)\\|A\rangle&=\frac{1}{\sqrt{2}}\left(|H\rangle-|V\rangle\right)\\|s\rangle&=\frac{1}{\sqrt{2}}\left(|b_1\rangle+|b_2\rangle\right)\\|a\rangle&=\frac{1}{\sqrt{2}}\left(|b_1\rangle-|b_2\rangle\right)\end{aligned} \tag{2}$$

其中，$|H\rangle$ 和 $|V\rangle$ 分别为光子的水平极化和垂直极化，$|b_1\rangle$ 和 $|b_2\rangle$ 分别为光子的上空模和下空模。

极化自由度下单光子的 2 个非正交测量基可被

定义为$Z_P=\{|H\rangle,|V\rangle\}$和$X_P=\{|R\rangle,|A\rangle\}$，空模自由度下单光子的2个非正交测量基可被定义为$Z_S=\{|b_1\rangle,|b_2\rangle\}$和$X_S=\{|s\rangle,|a\rangle\}$。极化自由度下单光子的2个酉操作可被描述为$I_P=|H\rangle\langle H|+|V\rangle\langle V|$和$U_P=|V\rangle\langle H|+|H\rangle\langle V|$，空模自由度下单光子的2个酉操作可被描述为$I_S=|b_1\rangle\langle b_1|+|b_2\rangle\langle b_2|$和$U_S=|b_2\rangle\langle b_1|+|b_1\rangle\langle b_2|$。容易得到

$$\begin{aligned}&U_P|H\rangle=|V\rangle,U_P|V\rangle=|H\rangle\\&U_P|S\rangle=|S\rangle,U_P|A\rangle=-|A\rangle\\&U_S|b_1\rangle=|b_2\rangle,U_S|b_2\rangle=|b_1\rangle\\&U_S|s\rangle=|s\rangle,U_S|a\rangle=-|a\rangle\end{aligned}\tag{3}$$

显然，U_P和U_S都不会改变相应自由度下的测量基。

定义$U_{PS}^{kl}=U_P^k\otimes U_S^l$，其中$k,l\in\{0,1\}$，则有

$$U_{PS}^{kl}|\phi\rangle=U_P^k|\phi\rangle_P\otimes U_S^l|\phi\rangle_S\tag{4}$$

定义

$$\begin{aligned}&U_P^0=I_P,U_P^1=U_P\\&U_S^0=I_S,U_S^1=U_S\end{aligned}\tag{5}$$

1.2 半量子密钥分配网络协议

半量子密钥分配网络协议旨在使位于网络上不同节点的通信方通过量子信道利用半量子密钥分发技术生成并共享理论上具有无条件安全性的随机密钥，从而在整体上组成一个安全的半量子密钥分配网络。

假设存在N个半量子参与者和一个量子参与者TP，其中TP是半忠诚的，即它不被允许与其他人共谋但可施加任何攻击[24]。$P_0,P_1,\cdots,P_{N-1}$和TP打算构建一个具有如下功能的半量子密钥分配网络：TP能与P_i建立密钥，同时又帮助P_i和$P_{(i+1)\bmod N}$建立密钥，其中$i\in\{0,1,\cdots,N-1\}$，其网络结构如图1所示。本文所提出的半量子密钥分配网络协议由以下6个步骤构成，其中所有量子信道和经典信道都被假定是认证的，编码函数$E(x)$被定义为

$$E(x)=\begin{cases}0, & x=|H\rangle\left(|b_1\rangle\right)\text{或}I_P\left(I_S\right)\\1, & x=|V\rangle\left(|b_2\rangle\right)\text{或}U_P\left(U_S\right)\end{cases}\tag{6}$$

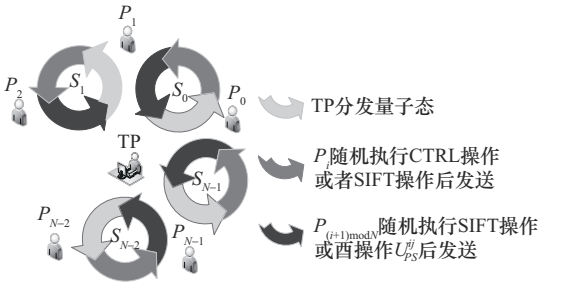


图1 半量子密钥分配网络结构

步骤1 TP随机以$Z_P\otimes X_S$基或$X_P\otimes Z_S$基制备$8nN$个双自由度单光子，并将这些单光子分成N个序列，即$S_i=\{s_i^1,s_i^2,\cdots,s_i^{8n}\}$，其中$i\in\{0,1,\cdots,N-1\}$。TP将$S_i$的单光子一个接一个地发送给$P_i$。注意，除了第一个单光子外，TP只有在接收到上一个单光子后才会发送下一个单光子。

步骤2 当收到S_i的单光子时，P_i对其随机执行CTRL操作或SITF操作后发送给$P_{(i+1)\bmod N}$。其中，CTRL操作是指对单光子不进行任何干扰，SITF操作是指采用$Z_P\otimes Z_S$基对单光子进行测量并制备一个处于相同态的新单光子。将S_i经P_i的SIFT操作和CTRL操作后形成的单光子序列分别记为S_i_SIFT序列和S_i_CTRL序列。其中，$i\in\{0,1,\cdots,N-1\}$。

步骤3 当收到来自P_i的单光子时，$P_{(i+1)\bmod N}$对其随机执行SIFT操作或酉操作（即U_{PS}^{kl}）后发送给TP。将S_i_SIFT序列经$P_{(i+1)\bmod N}$的SIFT操作和酉操作后形成的序列分别记为S_i_SIFT_SIFT序列和S_i_SIFT_U序列，将S_i_CTRL序列经$P_{(i+1)\bmod N}$的SIFT操作和酉操作后形成的序列分别记为S_i_CTRL_SIFT序列和S_i_CTRL_U序列。其中，$i\in\{0,1,\cdots,N-1\}$，$k,l\in\{0,1\}$。

步骤4 对于TP–P_i–$P_{(i+1)\bmod N}$–TP环路，TP从S_i中随机选择$\frac{1}{4}$的单光子并公布相应的位置，同时要求P_i和$P_{(i+1)\bmod N}$公布相应的操作和测量结果，最后选择如表1所示的正确测量基对收到的单光子进行测量。当P_i选择了CTRL操作且$P_{(i+1)\bmod N}$选择了酉操作时，TP根据自己对S_i中被选中的单光子的初始制备态、$P_{(i+1)\bmod N}$对S_i_CTRL序列中相应单光子施加的酉操作以及自己利用制备基对从$P_{(i+1)\bmod N}$收到的S_i_CTRL_U序列中相应单光子进

行的测量结果来计算错误率；当P_i选择了SIFT操作且$P_{(i+1)\bmod N}$选择了酉操作时，TP根据自己对S_i中被选中的单光子的初始制备态、P_i对S_i中被选中的单光子的$Z_P \otimes Z_S$基测量结果、$P_{(i+1)\bmod N}$对S_i_SIFT序列中相应单光子施加的酉操作以及自己对从$P_{(i+1)\bmod N}$收到的S_i_SIFT _U序列中相应单光子的$Z_P \otimes Z_S$基测量结果来计算错误率；当P_i选择了CTRL操作且$P_{(i+1)\bmod N}$选择了SIFT操作时，TP根据自己对S_i中被选中的单光子的初始制备态、$P_{(i+1)\bmod N}$对S_i_CTRL序列中相应单光子的$Z_P \otimes Z_S$基测量结果以及自己对从$P_{(i+1)\bmod N}$收到的S_i_CTRL _SIFT序列中相应单光子的$Z_P \otimes Z_S$基测量结果来计算错误率；当P_i选择了SIFT操作且$P_{(i+1)\bmod N}$选择了SIFT操作时，TP根据自己对S_i中被选中的单光子的初始制备态、P_i对S_i中被选中的单光子的$Z_P \otimes Z_S$基测量结果、$P_{(i+1)\bmod N}$对S_i_SIFT序列中相应单光子的$Z_P \otimes Z_S$基测量结果以及自己对从$P_{(i+1)\bmod N}$收到的S_i_SIFT _SIFT序列中相应单光子的$Z_P \otimes Z_S$基测量结果来计算错误率。如果任何一种错误率大得不合理，TP将认为量子信道不安全并提前中止协议。另外，如果在P_i公布的操作中SIFT操作占比高得不合理，协议也将被提前终止。其中，$i \in \{0,1,\cdots,N-1\}$。

表1　在TP − P_i − $P_{(i+1)\bmod N}$环路中TP的正确测量基

TP的制备基	P_i的操作	$P_{(i+1)\bmod N}$的操作	TP的正确测量基
$Z_P \otimes X_S$	CTRL	SIFT	$Z_P \otimes Z_S$
		酉操作	$Z_P \otimes X_S$
$X_P \otimes Z_S$	SIFT	SIFT	$Z_P \otimes Z_S$
		酉操作	$Z_P \otimes Z_S$
$X_P \otimes Z_S$	CTRL	SIFT	$Z_P \otimes Z_S$
		酉操作	$X_P \otimes Z_S$
$Z_P \otimes X_S$	SIFT	SIFT	$Z_P \otimes Z_S$
		酉操作	$Z_P \otimes Z_S$

步骤5　对于TP–P_i–$P_{(i+1)\bmod N}$–TP环路，为了检测TP是否忠诚，P_i从S_i中随机选择$\frac{1}{4}$的单光子并公布相应的位置，然后要求TP公布对S_i中所选中单光子的初始制备态。如果TP以$Z_P \otimes X_S$基制备P_i所选中的S_i的单光子，TP将随机利用$Z_P \otimes Z_S$基或$Z_P \otimes X_S$基测量从$P_{(i+1)\bmod N}$收到的相应单光子；如果TP以$X_P \otimes Z_S$基制备P_i所选中的S_i的单光子，TP将随机利用$Z_P \otimes Z_S$基或$X_P \otimes Z_S$基测量从$P_{(i+1)\bmod N}$收到的相应单光子。P_i要求TP公布测量结果，存在以下6种情况。

情况1　P_i选择了SIFT操作，$P_{(i+1)\bmod N}$选择了SIFT操作和酉操作中的任意一种操作，而TP选择了$Z_P \otimes X_S(X_P \otimes Z_S)$基进行测量。在这种情况下，TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$P_i$所选中的$S_i$的单光子。$P_i$与$P_{(i+1)\bmod N}$根据自己的操作和测量结果以及TP公布的初始制备态和$Z_P(Z_S)$基测量结果来计算错误率。

情况2　P_i选择了SIFT操作，$P_{(i+1)\bmod N}$选择了SIFT操作和酉操作中的任意一种操作，而TP选择了$Z_P \otimes Z_S$基进行测量。在这种情况下，TP既有可能以$Z_P \otimes X_S$基又有可能以$X_P \otimes Z_S$基制备P_i所选中的S_i的单光子。当TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$P_i$所选中的$S_i$的单光子时，$P_i$与$P_{(i+1)\bmod N}$根据自己的操作和测量结果以及TP公布的初始制备态和$Z_P \otimes Z_S$基测量结果计算错误率。

情况3　P_i选择了CTRL操作，$P_{(i+1)\bmod N}$选择了酉操作，而TP选择了$Z_P \otimes X_S(X_P \otimes Z_S)$基进行测量。在这种情况下，TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$P_i$所选中的$S_i$的单光子。$P_i$与$P_{(i+1)\bmod N}$根据自己的操作以及TP公布的初始制备态和$Z_P \otimes X_S(X_P \otimes Z_S)$基测量结果计算错误率。

情况4　P_i选择了CTRL操作，$P_{(i+1)\bmod N}$选择了酉操作，而TP选择了$Z_P \otimes Z_S$基进行测量。在这种情况下，TP既有可能以$Z_P \otimes X_S$基又有可能以$X_P \otimes Z_S$基制备P_i所选中的S_i的单光子。当TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$P_i$所选中的$S_i$的单光子时，$P_i$与$P_{(i+1)\bmod N}$根据自己的操作以及TP公布的初始制备态和$Z_P(Z_S)$基测量结果来计算错误率。

情况5　P_i选择了CTRL操作，$P_{(i+1)\bmod N}$选择了SIFT操作，而TP选择了$Z_P \otimes X_S(X_P \otimes Z_S)$基进行测量。在这种情况下，TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$P_i$所选中的$S_i$的单光子。$P_i$与$P_{(i+1)\bmod N}$根据自己的操作和测量结果以及TP公布的初始制备

态和$Z_P(Z_S)$基测量结果计算错误率。

情况6 P_i选择了CTRL操作，$P_{(i+1)\bmod N}$选择了SIFT操作，而TP选择了$Z_P \otimes Z_S$基进行测量。在这种情况下，TP既有可能以$Z_P \otimes X_S$基又有可能以$X_P \otimes Z_S$基制备P_i所选中的S_i的单光子。当TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$P_i$所选中的$S_i$的单光子时，$P_i$与$P_{(i+1)\bmod N}$根据自己的操作以及TP公布的初始制备态和$Z_P \otimes Z_S$基测量结果来计算错误率。

如果上述6种情况中任何一种的错误率大得不合理，P_i和$P_{(i+1)\bmod N}$将认为TP是不忠诚的，并提前中止协议。其中，$i \in \{0,1,\cdots,N-1\}$。

步骤6 对于TP − P_i − $P_{(i+1)\bmod N}$ − TP环路中的S_i的剩余$4n$个单光子，P_i和$P_{(i+1)\bmod N}$分别公布施加的操作类型。

TP对从$P_{(i+1)\bmod N}$收到的$S_{i_}\text{SIFT}_U$序列中的相应剩余单光子进行$Z_P \otimes Z_S$基测量，并公布自己对S_i中相应单光子的初始制备基。当TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$S_i$中的相应单光子时，TP公布$Z_S(Z_P)$基测量结果。假设TP对$S_i$中相应单光子的初始制备态为$|\phi\rangle$，$|\phi\rangle$的极化态和空模态分别为$|S_{i_}P\rangle$和$|S_{i_}S\rangle$，$P_i$对$|S_{i_}P\rangle$和$|S_{i_}S\rangle$的测量结果分别为$|S_{i_}\text{SIFT}_P\rangle$和$|S_{i_}\text{SIFT}_S\rangle$，$P_{(i+1)\bmod N}$对$|S_{i_}\text{SIFT}_P\rangle$和$|S_{i_}\text{SIFT}_S\rangle$施加的酉操作分别为$S_{i_}U_P$和$S_{i_}U_S$，TP对从$P_{(i+1)\bmod N}$收到的$S_{i_}U_P|S_{i_}\text{SIFT}_P\rangle$和$S_{i_}U_S|S_{i_}\text{SIFT}_S\rangle$的测量结果分别为$|S_{i_}\text{TP}_P\rangle$和$|S_{i_}\text{TP}_S\rangle$。如果TP的初始制备基为$Z_P \otimes X_S$，将存在以下关系

$$E\left(|S_{i\_}P\rangle\right)\oplus E\left(S_{i\_}U_P\right)=E\left(|S_{i\_}\text{TP}\_P\rangle\right) \quad (7)$$

$$E\left(|S_{i\_}\text{SIFT}\_S\rangle\right)\oplus E\left(S_{i\_}U_S\right)=E\left(|S_{i\_}\text{TP}\_S\rangle\right) \quad (8)$$

如果TP的初始制备基为$X_P \otimes Z_S$，将存在以下关系

$$E\left(|S_{i\_}\text{SIFT}\_S\rangle\right)\oplus E\left(S_{i\_}U_S\right)=E\left(|S_{i\_}\text{TP}\_S\rangle\right) \quad (9)$$

$$E\left(|S_{i\_}S\rangle\right)\oplus E\left(S_{i\_}U_S\right)=E\left(|S_{i\_}\text{TP}\_S\rangle\right) \quad (10)$$

根据式(8)和式(9)，P_i和$P_{(i+1)\bmod N}$可轻易共享由$E\left(|S_{i_}\text{SIFT}_S\rangle\right)$和$E\left(|S_{i_}\text{SIFT}_P\rangle\right)$组成的密钥$K_{i((i+1)\bmod N)}$，其长度为$n$ bit，即$K_{i((i+1)\bmod N)}=\left\{K^1_{T((i+1)\bmod N)},K^2_{T((i+1)\bmod N)},\cdots,K^n_{T((i+1)\bmod N)}\right\}$。其中，$i \in \{0,1,\cdots,N-1\}$。

TP选择正确的测量基对从$P_{(i+1)\bmod N}$收到的$S_{i_}\text{CTRL}_U$序列中的相应剩余单光子进行测量，并公布自己对S_i中相应单光子的初始制备基。假设TP对S_i中相应单光子的初始制备态为$|\varphi\rangle$，$|\varphi\rangle$的极化态和空模态分别为$|S_{i_}P'\rangle$和$|S_{i_}S'\rangle$，$P_{(i+1)\bmod N}$对$|S_{i_}P'\rangle$和$|S_{i_}S'\rangle$施加的酉操作分别为$S_{i_}U'_P$和$S_{i_}U'_S$，TP对从$P_{(i+1)\bmod N}$收到的$S_{i_}U'_P|S_{i_}P'\rangle$和$S_{i_}U'_S|S_{i_}S'\rangle$的测量结果分别为$|S_{i_}\text{TP}_P'\rangle$和$|S_{i_}\text{TP}_S'\rangle$。如果TP的初始制备基为$Z_P \otimes X_S$，将存在以下关系

$$E\left(|S_{i\_}P'\rangle\right)\oplus E\left(S_{i\_}U'_P\right)=E\left(|S_{i\_}\text{TP}\_P'\rangle\right) \quad (11)$$

如果TP的初始制备基为$X_P \otimes Z_S$，将存在以下关系

$$E\left(|S_{i\_}S'\rangle\right)\oplus E\left(S_{i\_}U'_S\right)=E\left(|S_{i\_}\text{TP}\_S'\rangle\right) \quad (12)$$

因此，$P_{(i+1)\bmod N}$和TP可轻易共享由$E\left(S_{i_}U'_P\right)$和$E\left(S_{i_}U'_S\right)$组成的密钥$K_{T((i+1)\bmod N)}$，其中$K_{T((i+1)\bmod N)}$的长度为n bit，即$K_{T((i+1)\bmod N)}=\left\{K^1_{T((i+1)\bmod N)},K^2_{T((i+1)\bmod N)},\cdots,K^n_{T((i+1)\bmod N)}\right\}$。其中，$i \in \{0,1,\cdots,N-1\}$。

至此完成了对本文所提出的半量子密钥分配网络协议的流程的描述。该协议的功能为：量子参与者与每个网络节点的半量子参与者建立不同密钥，同时又帮助每2个相邻网络节点的半量子参与者建立不同密钥，从而在整体上组成一个安全的半量子密钥分配网络。

2 安全性分析

2.1 抗外部攻击安全性

本节将证实所提出的半量子密钥分配网络协议具备良好的抗外在窃听者发起的截获−重发攻击、测量−重发攻击、纠缠−测量攻击和特洛伊木马攻击的安全性。

2.1.1　抗截获-重发攻击安全性

Eve截获TP发送给P_i的S_i的单光子，将事先制备好的随机处于$Z_P \otimes X_S$基或$X_P \otimes Z_S$基的假单光子发送给P_i。显然，Eve只有$\frac{1}{8}$的概率制备与真实单光子处于相同量子态的假单光子。Eve的这种攻击将不可避免地在步骤4中被发现，这是因为无论是TP的初始制备态还是P_i和$P_{(i+1)\bmod N}$的操作对于Eve来说都是随机的。对于一个被选中用于步骤4窃听检测的单光子来说，当P_i选择对其执行CTRL操作且$P_{(i+1)\bmod N}$对来自P_i的单光子进行酉操作时，Eve会以$\frac{1}{8}\times 3+\frac{1}{8}\times\frac{3}{4}\times 4=\frac{3}{4}$的概率被检测到；当$P_i$选择对其执行CTRL操作且对来自$P_i$的单光子执行SIFT操作时，Eve会以$\frac{1}{8}\times 2+\frac{1}{8}\times\frac{1}{2}\times 4=\frac{1}{2}$的概率被检测到；当$P_i$选择对其执行SIFT操作且$P_{(i+1)\bmod N}$对来自$P_i$的单光子进行酉操作时，Eve会以$\frac{1}{8}\times 2+\frac{1}{8}\times\frac{1}{2}\times 4=\frac{1}{2}$的概率被检测到；当$P_i$选择对其执行SIFT操作且$P_{(i+1)\bmod N}$对来自$P_i$的单光子执行SIFT操作时，Eve会以$\frac{1}{8}\times 2+\frac{1}{8}\times\frac{1}{2}\times 4=\frac{1}{2}$的概率被检测到。由于一个单光子被选中用于步骤4的窃听检测的概率为$\frac{1}{4}$，因此Eve对S_i发起的截获-重发攻击会被检测到的概率为

$$P_1=1-\left[1-\frac{1}{4}\times\left(\frac{1}{4}\times\frac{3}{4}+\frac{1}{4}\times\frac{1}{2}\times 3\right)\right]^{4n}=1-\left(\frac{55}{64}\right)^{4n} \tag{13}$$

当n足够大时，Eve会以趋近于1的概率在步骤4中被检测到。其中，$i\in\{0,1,\cdots,N-1\}$。

2.1.2　抗测量-重发攻击安全性

Eve截获TP发送给P_i的单光子，利用$Z_P \otimes Z_S$基对其进行测量并重新生成一个处于相同态的新单光子，然后将其发送给P_i。Eve的这种攻击将不可避免地在步骤4中被发现，这是因为Eve的测量会破坏单光子的原始状态。对于一个被选中用于步骤4窃听检测的单光子来说，当P_i选择对其执行SIFT操作时，无论$P_{(i+1)\bmod N}$对来自P_i的单光子执行SIFT操作还是酉操作，Eve都会以0的概率被检测到；当P_i选择对其执行CTRL操作且$P_{(i+1)\bmod N}$对来自P_i的单光子执行SIFT操作时，Eve会以0的概率被检测到；当P_i选择对其执行CTRL操作且$P_{(i+1)\bmod N}$对来自P_i的单光子进行酉操作时，Eve会以$\frac{1}{2}$的概率被检测到。由于一个单光子被选中用于步骤4的窃听检测的概率为$\frac{1}{4}$，因此Eve对S_i发起的测量-重发攻击会被检测到的概率为

$$P_1=1-\left[1-\frac{1}{4}\times\left(\frac{1}{4}\times 0\times 3+\frac{1}{4}\times\frac{1}{2}\right)\right]^{4n}=1-\left(\frac{31}{32}\right)^{4n} \tag{14}$$

当n足够大时，Eve会以趋近于1的概率在步骤4中被发现。其中，$i\in\{0,1,\cdots,N-1\}$。

2.1.3　抗纠缠-测量攻击安全性

Eve所发起的纠缠-测量攻击可用图2来表示[9-10]。具体来说，Eve对TP发送给P_i的单光子和P_i发送给$P_{(i+1)\bmod N}$的单光子分别执行$\hat{U}_E$和$\hat{U}_F$，其中$\hat{U}_E$和$\hat{U}_F$是Eve的共享初始态为$|\varepsilon\rangle$的共同探测空间的2个酉操作。其中，$i\in\{0,1,\cdots,N-1\}$。

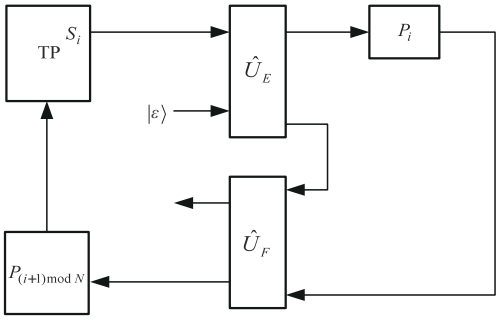


图2　Eve通过$\hat{U}_E$和$\hat{U}_F$发起的纠缠-测量攻击

定理1　假设Eve发起的纠缠-测量攻击如图2所示，为了在步骤4中不引发任何错误，Eve的探测态的最终状态应与P_i和$P_{(i+1)\bmod N}$的操作及测量结果都无关，因此Eve无法得到关于$K_{i((i+1)\bmod N)}$和$K_{T((i+1)\bmod N)}$的任何有用信息。

证明　由TP制备的初始态和Eve的$|\varepsilon\rangle$组合而成的复合系统的全局状态为$|\phi\rangle|\varepsilon\rangle$，其中$|\phi\rangle$由TP

随机以$Z_P \otimes X_S$基或$X_P \otimes Z_S$基生成。在Eve执行$\hat{U}_E$后，全局状态转变为

$$\hat{U}_E\left(|\phi\rangle|\varepsilon\rangle\right)=|Hb_1\rangle|\gamma_{Hb_1}\rangle+|Hb_2\rangle|\gamma_{Hb_2}\rangle+|Vb_1\rangle|\gamma_{Vb_1}\rangle+|Vb_2\rangle|\gamma_{Vb_2}\rangle \tag{15}$$

其中，$|\gamma_{Hb_1}\rangle$、$|\gamma_{Hb_2}\rangle$、$|\gamma_{Vb_1}\rangle$和$|\gamma_{Vb_2}\rangle$为Eve的探测粒子的非归一化态。不失一般性，以下假设TP的初始制备态为$|Hs\rangle$。

在收到TP的单光子后，P_i随机施加CTRL操作或SIFT操作后再随机发送给$P_{(i+1)\bmod N}$。当收到来自P_i的单光子时，$P_{(i+1)\bmod N}$对其随机执行SIFT操作或酉操作（即U_{PS}^{kl}）后发送给TP。这里分2种情况进行讨论。

1) P_i施加SITF操作。这时，式(15)的全局状态会被随机坍缩到$|Hb_1\rangle|\gamma_{Hb_1}\rangle$、$|Hb_2\rangle|\gamma_{Hb_2}\rangle$、$|Vb_1\rangle|\gamma_{Vb_1}\rangle$和$|Vb_2\rangle|\gamma_{Vb_2}\rangle$中的一种。Eve在$P_i$发送给$P_{(i+1)\bmod N}$的单光子上施加$\hat{U}_F$，无论$P_{(i+1)\bmod N}$对来自$P_i$的单光子执行SIFT操作还是酉操作，为了使Eve的攻击不在步骤4引发任何错误，都需满足

$$\hat{U}_F\left(|Hb_1\rangle|\gamma_{Hb_1}\rangle\right)=|Hb_1\rangle|\lambda_{Hb_1}\rangle \tag{16}$$

$$\hat{U}_F\left(|Hb_2\rangle|\gamma_{Hb_2}\rangle\right)=|Hb_2\rangle|\lambda_{Hb_2}\rangle \tag{17}$$

$$\hat{U}_F\left(|Vb_1\rangle|\gamma_{Vb_1}\rangle\right)=|Vb_1\rangle|\lambda_{Vb_1}\rangle \tag{18}$$

$$\hat{U}_F\left(|Vb_2\rangle|\gamma_{Vb_2}\rangle\right)=|Vb_2\rangle|\lambda_{Vb_2}\rangle \tag{19}$$

也就是说，$\hat{U}_F$不能改变P_i施加SITF操作后坍塌得到的单光子的状态。

2) P_i施加CTRL操作。Eve在P_i发送给$P_{(i+1)\bmod N}$的单光子上施加$\hat{U}_F$。根据式(16)~式(19)，式(15)的全局状态会被转化成

$$\hat{U}_F\left(|Hb_1\rangle|\gamma_{Hb_1}\rangle+|Hb_2\rangle|\gamma_{Hb_2}\rangle+|Vb_1\rangle|\gamma_{Vb_1}\rangle+|Vb_2\rangle|\gamma_{Vb_2}\rangle\right)=|Hb_1\rangle|\lambda_{Hb_1}\rangle+|Hb_2\rangle|\lambda_{Hb_2}\rangle+|Vb_1\rangle|\lambda_{Vb_1}\rangle+|Vb_2\rangle|\lambda_{Vb_2}\rangle \tag{20}$$

当$P_{(i+1)\bmod N}$对来自P_i的单光子进行酉操作时，为了使Eve的攻击不在步骤4引发任何错误，需满足

$$|\lambda_{Hb_1}\rangle=|\lambda_{Hb_2}\rangle=|\lambda\rangle \tag{21}$$

$$|\lambda_{Vb_1}\rangle=|\lambda_{Vb_2}\rangle=0 \tag{22}$$

当$P_{(i+1)\bmod N}$对来自P_i的单光子执行SIFT操作时，式(20)的全局状态会被随机坍缩到$|Hb_1\rangle|\lambda_{Hb_1}\rangle$、$|Hb_2\rangle|\lambda_{Hb_2}\rangle$、$|Vb_1\rangle|\lambda_{Vb_1}\rangle$和$|Vb_2\rangle|\lambda_{Vb_2}\rangle$中的一种。根据式(21)和式(22)，这时Eve的攻击不在步骤4引发任何错误。

综上所述，当TP的初始制备态为$|Hs\rangle$时，为了使Eve的攻击不在步骤4引发任何错误，Eve的探测态的最终状态应与P_i和$P_{(i+1)\bmod N}$的操作及测量结果都无关，因此Eve无法得到关于$K_{i((i+1)\bmod N)}$和$K_{T((i+1)\bmod N)}$的任何有用信息。

不难发现，当TP的初始制备态为处于$Z_P \otimes X_S$基或$X_P \otimes Z_S$基的其他量子态时，可以用类似的方法证明定理1成立。证毕。

2.1.4 抗特洛伊木马攻击安全性

Eve可以利用往返传输的光子发起特洛伊木马攻击来试图获取有用信息。Eve可发起不可见光子窃听攻击[25]以及延迟光子特洛伊木马攻击[26-27]。根据文献[27-28]，量子信号接收者可在自己的设备前使用波长滤波器和光子数分割器来分别抵御不可见光子窃听攻击和延迟光子特洛伊木马攻击。

2.2 抗内部攻击安全性

Gao等[29]首次提出一种被称为参与者攻击的新攻击。由于参与者参与协议的执行，其威胁往往比外部窃听者Eve更大。本节将证实所提出的半量子密钥分配网络协议具备良好的抗不忠诚半量子参与者发起的攻击的安全性和良好的抗半忠诚TP发起的攻击的安全性。

2.2.1 抗不忠诚半量子参与者发起的攻击的安全性

对于TP－P_i－$P_{(i+1)\bmod N}$－TP环路，P_i可能会去尝试得到$K_{T((i+1)\bmod N)}$。由于$K_{T((i+1)\bmod N)}$是由步骤6中S_i_CTRL_U序列的相应剩余单光子产生的，P_i不发起攻击时无法获取任何有关$K_{T((i+1)\bmod N)}$的信息。如果P_i对S_i的$8n$个单光子都采取SIFT操

作，这时将不会存在$K_{T((i+1)\bmod N)}$，但是P_i在步骤4公布的SIFT操作的占比将会高得不合理，P_i将被认为是不忠诚的，从而导致协议被提前终止。另外，P_i可能发起如下攻击：P_i对S_i的单光子施加完CTRL操作后将其保存在自己手中，制备随机处于$Z_P \otimes Z_S$基的假单光子发送给$P_{(i+1)\bmod N}$；利用$Z_P \otimes Z_S$基测量$P_{(i+1)\bmod N}$操作后的假单光子，解码出$P_{(i+1)\bmod N}$施加的操作并将其施加到保存在自己手中的S_i的单光子后发送给TP。当$P_{(i+1)\bmod N}$选择执行CTRL操作时，P_i的这种攻击在步骤4不会被TP检测到。然而，当$P_{(i+1)\bmod N}$选择执行SIFT操作时，P_i的这种攻击在步骤4会被TP当成外部攻击而检测到，这是因为当$P_{(i+1)\bmod N}$选择执行SIFT操作时，TP对S_i的单光子的初始制备态、$P_{(i+1)\bmod N}$对假光子的$Z_P \otimes Z_S$基测量结果以及TP对收到的单光子的$Z_P \otimes Z_S$基测量结果这三者未必能完全正确对应起来。其中，$i \in \{0,1,\cdots,N-1\}$。

对于TP–P_i–$P_{(i+1)\bmod N}$–TP环路，P_t可能会去尝试得到$K_{i((i+1)\bmod N)}$和$K_{T((i+1)\bmod N)}$，其中$t,i \in \{0,1,\cdots,N-1\}$且$t \neq i,(i+1)\bmod N$。此时，$P_t$对于TP–$P_i$–$P_{(i+1)\bmod N}$–TP环路而言不是扮演参与者的角色，因此$P_t$发起的任何攻击都会在步骤4被TP检测到。

对于TP–P_i–$P_{(i+1)\bmod N}$–TP环路，除P_i和$P_{(i+1)\bmod N}$外的2个或2个以上半量子参与者也可能联合起来去尝试得到$K_{i((i+1)\bmod N)}$和$K_{T((i+1)\bmod N)}$，但它们同样会被当成外部窃听者在步骤4被TP检测到。其中，$i \in \{0,1,\cdots,N-1\}$。

2.2.2　抗半忠诚TP发起的攻击的安全性

TP作为半忠诚第三方，可能会尝试去获取$K_{i((i+1)\bmod N)}$。TP以$Z_P \otimes Z_S$基制备S_i的所有单光子，但在步骤5中对它们仍公布制备基为“$Z_P \otimes X_S$”或“$X_P \otimes Z_S$”。TP的这种攻击策略可轻松通过步骤4的窃听检测，这是因为步骤4的窃听检测是由TP主导的。但是TP的这种攻击策略无法通过步骤5的窃听检测，这是因为TP在被P_i和$P_{(i+1)\bmod N}$要求公布初始制备态和测量结果前对P_i和$P_{(i+1)\bmod N}$的操作一无所知。

3　讨论

量子比特效率是评价量子通信协议性能的重要指标，被定义为[4]

$$\eta = \frac{\rho_k}{\rho_q + \rho_c} \tag{23}$$

其中，ρ_k是产生的经典密钥比特数目，ρ_q是消耗的量子比特数目，ρ_c是经典通信过程消耗的经典比特数目。这里忽略用于窃听检查的经典比特。

在本文的协议中，$K_{i((i+1)\bmod N)}$的长度为n bit，$K_{T((i+1)\bmod N)}$的长度也为n bit，其中$i \in \{0,1,\cdots,N-1\}$，因此有$\rho_k = nN + nN = 2nN$。TP在步骤1随机以$Z_P \otimes X_S$基或$X_P \otimes Z_S$基生成$8nN$个双自由度单光子，并将这些单光子分成N个序列，即$S_i = \{s_i^1, s_i^2, \cdots, s_i^{8n}\}$，其中$i \in \{0,1,\cdots,N-1\}$。TP将$S_i$的单光子一个接一个地发送给$P_i$，当收到$S_i$的单光子时，$P_i$对其随机执行CTRL操作或SITF操作后发送给$P_{(i+1)\bmod N}$；当收到来自$P_i$的单光子时，$P_{(i+1)\bmod N}$对其随机执行SIFT操作或酉操作（即$U_{PS}^{kl}$）后发送给TP，因此有$\rho_q = 8nN \times 2 + 4nN \times 2 + 4nN \times 2 = 32nN$。在步骤6中，对于TP–$P_i$–$P_{(i+1)\bmod N}$–TP环路中的$S_i$的剩余$4n$个单光子，$P_i$和$P_{(i+1)\bmod N}$分别公布施加的操作类型。TP对从$P_{(i+1)\bmod N}$收到的$S_i$_SIFT_$U$序列中的相应剩余单光子进行$Z_P \otimes Z_S$基测量，并公布自己对$S_i$中相应单光子的初始制备基；当TP以$Z_P \otimes X_S(X_P \otimes Z_S)$基制备$S_i$中的相应单光子时，TP再公布$Z_S(Z_P)$基测量结果；TP选择正确的测量基对从$P_{(i+1)\bmod N}$收到的$S_i$_CTRL_$U$序列中的相应剩余单光子进行测量，并公布自己对$S_i$中相应单光子的初始制备基，因此有$\rho_c = 4nN \times 2 + nN + nN + nN = 11nN$。不难得出本文的量子比特效率为$\eta = \dfrac{2nN}{32nN + 11nN} = \dfrac{2}{43}$。

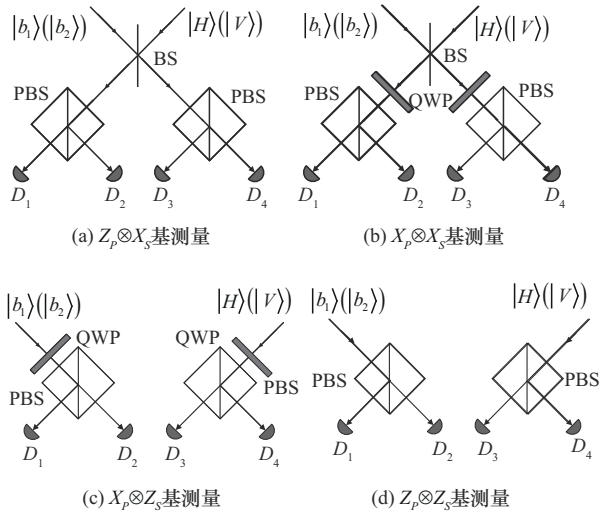
接下来，将本文协议与文献[18-22]中的MSQKD协议进行详细的比较，结果如表2所示。本文采用了双自由度的单光子，避免了量子纠缠态的使用，因此本文协议在量子资源方面优于文献[19-22]的协议；本文协议只要求量子参与者执行单光子测量，避免了进行量子纠缠态测量，因此本文协议在量子参与者的测量方面优于文献[19-21]的协议；本文协议不要求半量子参与者执行哈达玛操作，因此本文协议在半

表2 不同MSQKD协议的对比

协议	功能	量子资源	量子参与者的量子测量	半量子参与者是否执行量子测量	是否执行量子纠缠交换	半量子方是否使用延迟线	半量子方是否执行酉操作	半量子方是否执行哈达玛操作	半量子方是否拥有量子存储器
文献[18]	量子参与者与一群半量子参与者一起建立同一密钥	单光子	单光子测量	是	否	否	否	否	否
文献[19]	量子参与者与两群半量子参与者建立不同密钥	四粒子团簇态	单光子测量、Bell态测量和四粒子团簇态测量	是	否	否	否	否	否
文献[20]	量子参与者与一群半量子参与者一起建立同一密钥	超纠缠Bell态	单光子测量、超纠缠Bell态测量	是	否	否	否	否	否
文献[21]	量子参与者与每个半量子参与者建立不同密钥	多粒子GHZ态	单粒子测量和多粒子GHZ态测量	是	否	否	否	否	否
文献[22]	量子参与者帮助一个半量子参与者与一群其他半量子参与者一起建立同一密钥	图态	单光子测量	是	否	否	是	是	是
本文协议	量子参与者与每个半量子参与者建立不同密钥，同时帮助每2个相邻半量子参与者建立不同密钥	双自由度单光子	单光子测量	是	否	否	是	否	否

量子参与者执行哈达玛操作方面优于文献[22]的协议；本文协议不要求半量子参与者拥有量子存储器，因此本文协议在半量子参与者拥有量子存储器方面优于文献[22]的协议；在协议功能方面，只有本文协议可实现“量子参与者与每个半量子参与者建立不同密钥，同时又帮助每2个相邻半量子参与者建立不同密钥”的功能。

本文协议在实际执行时需要对具有极化和空模自由度的单光子进行制备、测量和施加酉操作。这些操作在目前的技术条件很容易，所以本文协议具有良好的实际可行性。具体而言，具有极化和空模自由度的单光子可按照如下方法制备[30-32]：处于Z_S基的单光子直接在对应的空模模式下制备；处于X_S基的单光子由对处于Z_S基的单光子施加50:50分束器（BS，beam splitter）来制备，即BS具有如下作用，$|b_1\rangle \to |s\rangle = \frac{1}{\sqrt{2}}\left(|b_1\rangle + |b_2\rangle\right)$，$|b_2\rangle \to |a\rangle = \frac{1}{\sqrt{2}}\left(|b_1\rangle - |b_2\rangle\right)$；处于$Z_P$基的单光子直接在对应的极化模式下制备；处于$X_P$基的单光子由对处于$Z_P$基的单光子施加$\frac{1}{4}$玻片（QWP，quarter wave plate）来制备，即QWP具有如下作用，$|H\rangle \to |S\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right)$，$|V\rangle \to |A\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right)$。具有极化和空模自由度的单光子可按照如图3所示的方法进行测量[30-32]。



(a) $Z_P \otimes X_S$基测量　(b) $X_P \otimes X_S$基测量

(c) $X_P \otimes Z_S$基测量　(d) $Z_P \otimes Z_S$基测量

图3　对具有极化和空模自由度的单光子进行的量子测量

4　仿真分析

本节使用IBM量子计算云平台Qiskit对$N = 3$时的本文协议进行仿真模拟以证明其正确性。每个仿真模拟实验都进行10 000次。为方便描述，仿真过程尽可能忽略窃听检测过程。

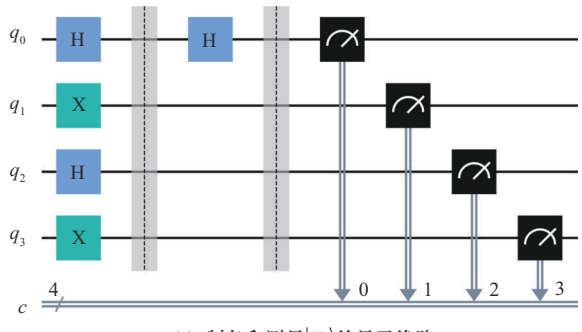
4.1　对量子态制备与测量的仿真分析

在本文协议的步骤1中，TP随机以$Z_P \otimes X_S$和$X_P \otimes Z_S$基制备双自由度单光子。不失一般性，假设TP制备$|Vs\rangle$，制备和测量$|Vs\rangle$的量子线路如图4(a)所示。在图4(a)中，第一条虚线的左侧表示量子态的制备，其中q_1和q_0代表初始量子态都为$|0\rangle$的2个量子比特，对q_1执行非门（即X门）且对q_0执行Hadamard门（即H门）即可产生$|Vs\rangle$，对q_3和q_2通过同样的方式制备$|Vs\rangle$；第一条虚线的右侧表示量子态的测量，对q_1和q_0这2条线路执行$Z_P \otimes X_S$基测量，对q_3和q_2这2条线路执行$Z_P \otimes Z_S$基测量，测量结果保存在寄存器c中。图4(a)的仿真结果如图4(b)所示。在图4(b)中，寄存器的后两位结果为10，说明$Z_P \otimes X_S$基测量结果始终为$|Vs\rangle$；寄存器的前两位结果为10和11的比例接近1:1，满足$Z_P \otimes Z_S$基测量的理论结果，说明$|Vs\rangle$经$Z_P \otimes Z_S$基测量后被随机坍缩为$|Vb_1\rangle$和$|Vb_2\rangle$。

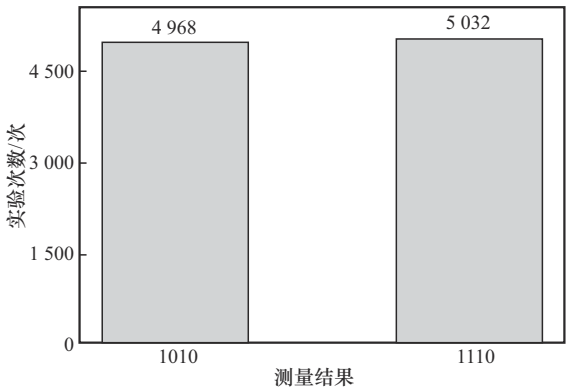
4.2　对协议关键步骤的仿真分析

在本文协议中，TP随机以$Z_P \otimes X_S$或$X_P \otimes Z_S$基制备初始单光子，然后将其发送给P_i；P_i对从TP收到的初始单光子随机执行CTRL操作或SIFT操作后将其发送给$P_{(i+1) \bmod 3}$；$P_{(i+1) \bmod 3}$对从P_i收到的单光子执行SIFT操作或酉操作后将其发送给TP。接下来对步骤6中生成$K_{i((i+1) \bmod 3)}$和$K_{T((i+1) \bmod 3)}$的仿真进行详细讨论。其中，$i \in \{0,1,2\}$。

首先讨论P_0、P_1和P_2都执行CTRL操作且P_1、P_2和P_0都选择酉操作的情况，相应的量子线路及其与仿真结果如图5所示。在图5(a)中，第一条虚线的左侧代表TP随机制备量子态$|Hs\rangle$、$|Ab_2\rangle$和$|Vs\rangle$（分别对应着q_5q_4、q_3q_2和q_1q_0）并将它们分别发送给P_0、P_1和P_2，然后P_0、P_1和P_2对从TP收到的单光子都执行CTRL操作后将其分别发送给P_1、P_2和P_0；第二条虚线的左侧代表P_1、P_2和P_0对收到的单光子都执行$U_P \otimes I_S$后将其发送给TP；第二条虚线和第三条虚线的右侧代表TP利用$Z_P \otimes X_S$基、$X_P \otimes Z_S$基和$Z_P \otimes X_S$基分别测量从P_1、P_2和P_0收到的单光子。在图5(b)中，按从左到右的顺序，仿真结果中第1~6位为TP的测量结

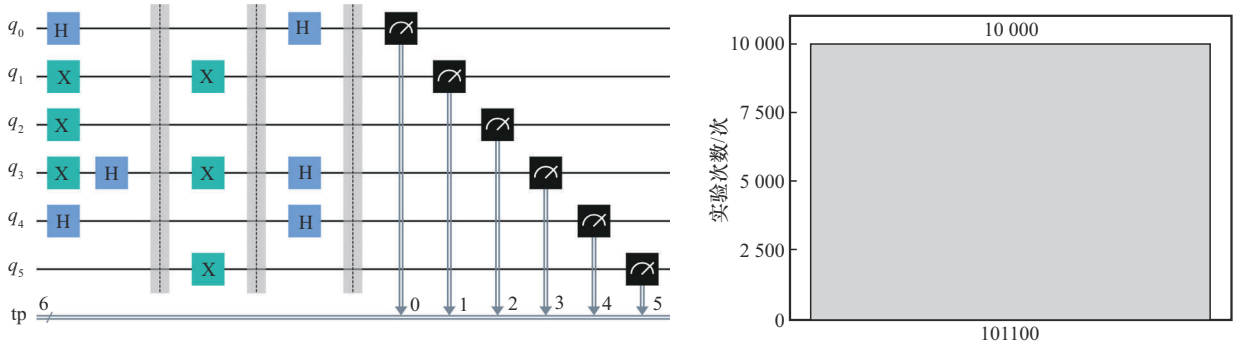


(a) 制备和测量$|Vs\rangle$的量子线路



(b) 制备和测量$|Vs\rangle$的仿真结果

图4　制备和测量$|Vs\rangle$的量子线路及其仿真结果



(a) P_0、P_1和P_2都选择CTRL操作且P_1、P_2和P_0都选择　　(b) 仿真结果

图5　P_0、P_1和P_2都执行CTRL操作且P_1、P_2和P_0都选择酉操作的量子线路及其仿真结果

果。这里用$r(j)$代表仿真结果第j位的值，其中$j\in\{1,2,\cdots,6\}$。不难发现，存在如下关系

$$\begin{aligned}&E(|H\rangle)\oplus E(U_P)=r(1)\\&E(|b_2\rangle)\oplus E(I_S)=r(4)\\&E(|V\rangle)\oplus E(U_P)=r(5)\end{aligned}\tag{24}$$

其中，$|H\rangle$、$|b_2\rangle$、$|V\rangle$为TP的部分初始制备态，U_P、I_S、U_P分别为P_1、P_2和P_0对$|H\rangle$、$|b_2\rangle$、$|V\rangle$执行的酉操作。TP会公布初始态的制备基，P_1、P_2和P_0可分别通过计算$K_{T_1}=E(U_P)=1$、$K_{T_2}=E(I_S)=0$和$K_{T_0}=E(U_P)=1$来生成密钥。TP通过计算$K_{T_1}=E(|H\rangle)\oplus r(1)=E(U_P)=1$、$K_{T_2}=E(|b_2\rangle)\oplus r(4)=E(I_S)=0$和$K_{T_0}=E(|V\rangle)\oplus r(5)=E(U_P)=1$来分别与$P_1$、$P_2$和$P_0$建立密钥。因此，这种情形的量子线路的仿真结果是符合协议的。

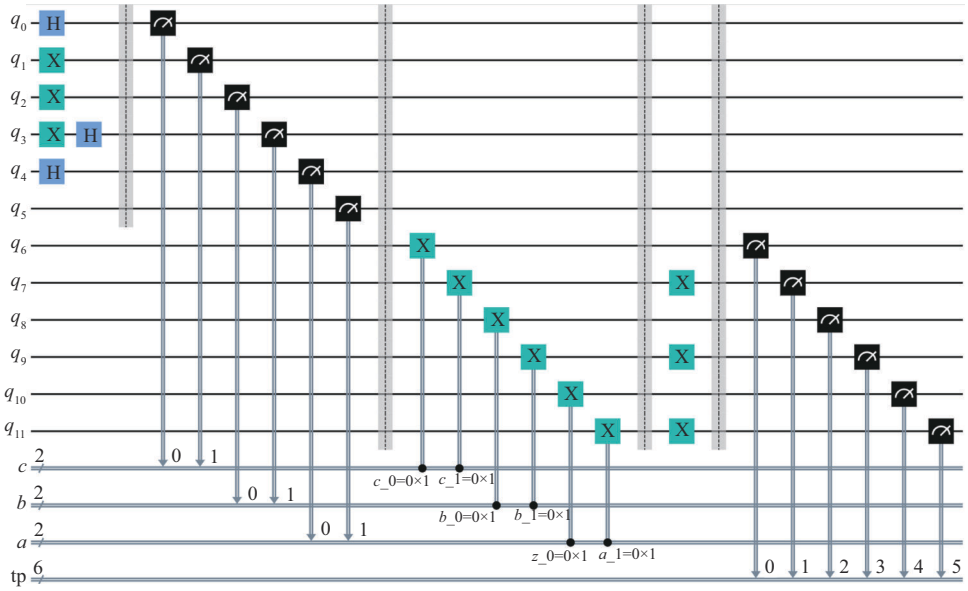
接下来讨论P_0、P_1和P_2都执行SIFT操作且P_1、P_2和P_0都选择酉操作的情况。相应的量子线路及其仿真结果如图6所示。在图6(a)中，第一条虚线的左侧代表TP随机制备量子态$|Hs\rangle$、$|Ab_2\rangle$和$|Vs\rangle$（分别对应着q_5q_4、q_3q_2和q_1q_0）并将它们分别发送给P_0、P_1和P_2；第二条虚线的左侧代表P_0、P_1和P_2对从TP收到的单光子都执行SIFT操作时以$Z_P\otimes Z_S$基测量它们，并将测量结果分别存储到寄存器a、b和c中；第三条虚线左侧代表P_0、P_1和P_2分别根据寄存器a、b和c存储的测量结果重新生成处于相同量子态的新单光子（分别对应着$q_{11}q_{10}$、q_9q_8和q_7q_6）并分别发送给P_1、P_2和P_0；第四条虚线左侧代表P_1、P_2和P_0对收到的单光子都执行$U_P\otimes I_S$后将其发送给TP；第四条虚线右侧代表TP对从P_1、P_2和P_0收到的单光子都进行$Z_P\otimes Z_S$基测量并将测量结果都保存在寄存器tp中。在图6(b)中，按从左到右的顺序，每种仿真结果中第1~6位是TP的测量结果，第7~12位是P_0、P_1和P_2执行SIFT操作的测量结果。这里用$r(j)$代表仿真结果第j位的值，其中$j\in\{1,2,\cdots,12\}$。不难发现，存在如下关系

$$\begin{aligned}&r(7)r(8)r(9)r(10)r(11)r(12)\oplus(101010)=\\&\qquad r(1)r(2)r(3)r(4)r(5)r(6)\end{aligned}\tag{25}$$

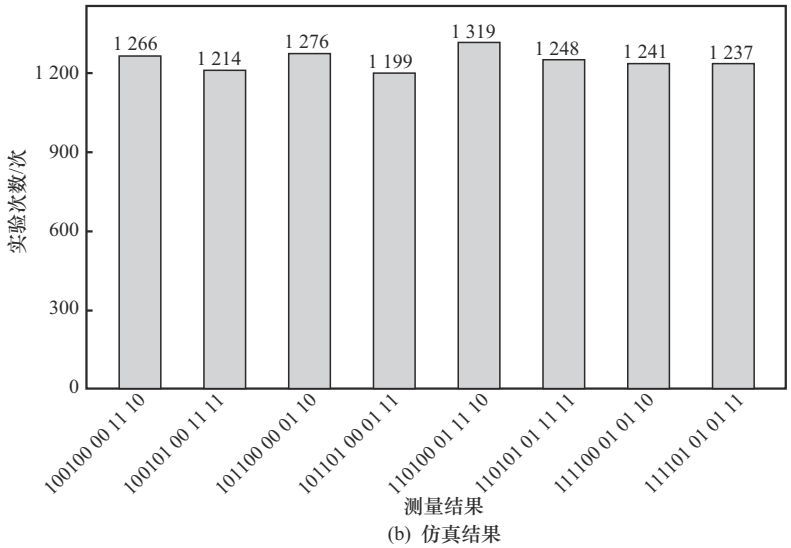
其中，101010对应于P_1、P_2和P_0分别执行的$U_P\otimes I_S$。TP会公布$r(2)$、$r(3)$和$r(6)$的值，P_1可通过计算$r(2)\oplus 0=r(8)$与P_0建立密钥$K_{01}=r(8)$，P_2可通过计算$r(3)\oplus 1=r(9)$与P_1建立密钥$K_{12}=r(9)$，P_0可通过计算$r(6)\oplus 0=r(12)$与P_2建立密钥$K_{02}=r(12)$。因此，这种情形的量子线路的仿真结果是符合协议的。

4.3　对Eve发起的测量-重发攻击的仿真分析

本节以4.2节中P_0、P_1和P_2都执行CTRL操作且P_1、P_2和P_0都选择酉操作的情况为例分析Eve发起的测量-重发攻击，相应的量子线路如图7(a)所示。根据图7(a)，Eve以$Z_P\otimes Z_S$基测量P_0、P_1和P_2执行CTRL操作时发送出去的量子态并将测量结果存储在寄存器eve中，然后重新生成处于相同态的新单光子并分别发送给P_1、P_2和P_0；P_1、P_2和P_0对收到的单光子都执行$U_P\otimes I_S$后将其发送给TP；最后，TP以制备基对收到的单光子进行量子测量。如果没有Eve存在，仿真结果应如图7(b)所示，即TP的测量结果都应为101100。然而，图7(b)的64种测量结果中只有8种



(a) P_0、P_1和P_2都选择SIFT操作且P_1、P_2和P_0都选择酉操作的量子线路



(b) 仿真结果

图6　P_0、P_1和P_2都执行CTRL操作且P_1、P_2和P_0都选择酉操作的量子线路及其仿真结果

为101100，因此Eve的测量−重发攻击无疑会被检测到。

5　所提出的半量子密钥分配网络协议的应用

5.1　应用于半量子求和

半量子求和[33-37]旨在不泄露半量子参与者隐秘数据的前提下计算出这些隐秘数据的求和。接下来将本文协议应用到半量子求和中。

半量子参与者P_i的二进制秘密序列为M_i，其中$i\in\{0,1,\cdots,N-1\}$。$P_0,P_1,\cdots,P_{N-1}$想要在半忠诚量子第三方TP的帮助下计算出$M_0,M_1,\cdots,M_{N-1}$的模2和，但不能将$M_0,M_1,\cdots,M_{N-1}$泄露给持有者之外的其他人。可利用下述协议来实现这一目标。

步骤1~6同1.2节的步骤1~6。

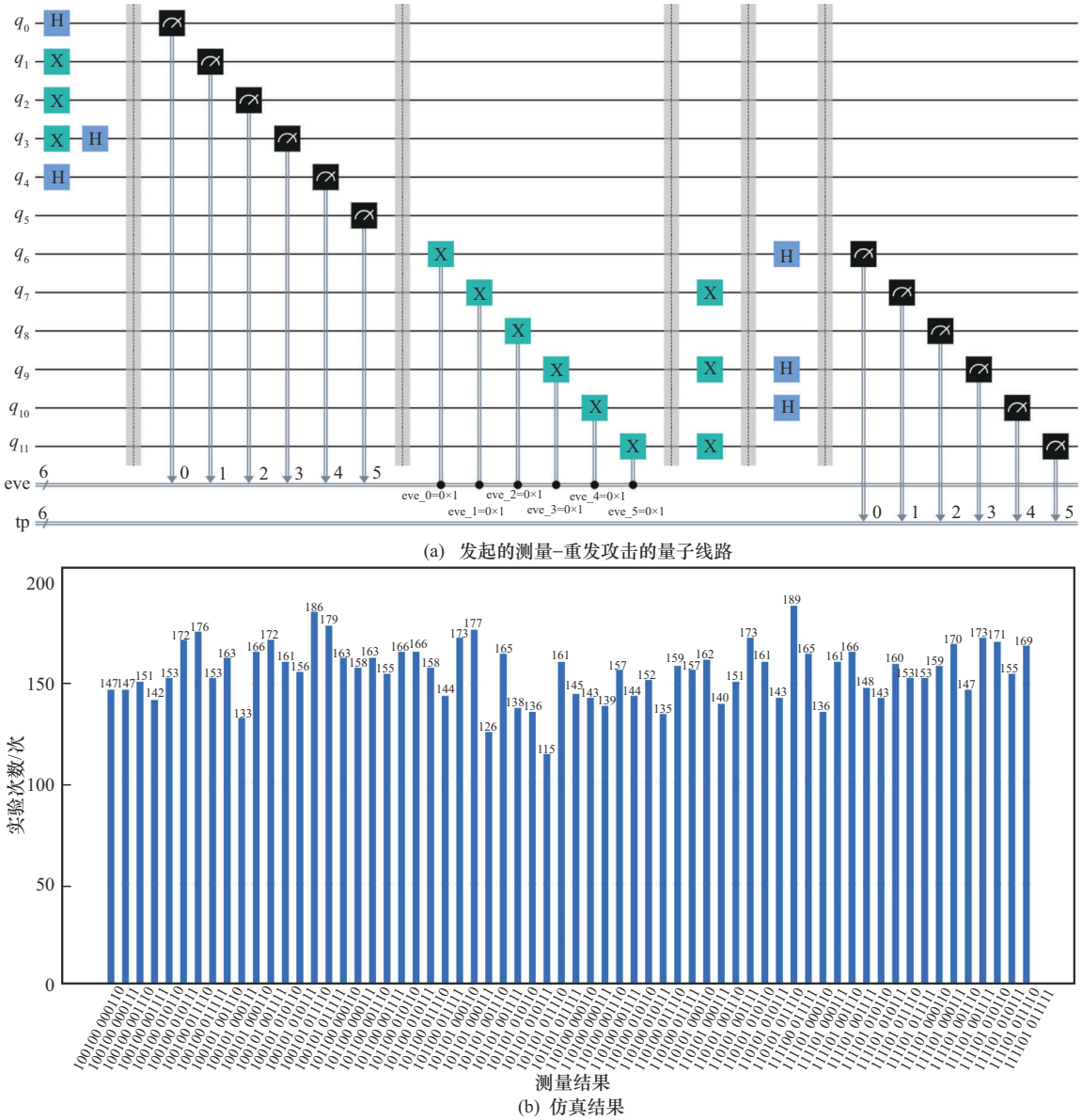
步骤7　P_i计算

$$R_i=M_i\oplus K_{Ti}\oplus K_{i((i+1)\bmod N)}\oplus K_{((i-1)\bmod N)i} \tag{26}$$

并通过认证的经典信道将R_i发送给TP，其中$i\in\{0,1,\cdots,N-1\}$。TP计算

$$\begin{aligned}&R=R_0\oplus R_1\oplus\cdots\oplus R_{N-1}\oplus\\&K_{T0}\oplus K_{T1}\oplus\cdots\oplus K_{T(N-1)}=\\&(M_0\oplus K_{T0}\oplus K_{01}\oplus K_{(N-1)0})\oplus\\&(M_1\oplus K_{T1}\oplus K_{12}\oplus K_{01})\oplus\cdots\oplus\\&(M_{N-1}\oplus K_{T(N-1)}\oplus K_{(N-1)0}\oplus K_{(N-2)(N-1)})\oplus\\&K_{T0}\oplus K_{T1}\oplus\cdots\oplus K_{T(N-1)}=\\&M_0\oplus M_2\oplus\cdots\oplus M_{N-1}\end{aligned} \tag{27}$$

并向$P_0,P_1,\cdots,P_{N-1}$公布R。



(a)　发起的测量−重发攻击的量子线路

(b)　仿真结果

图 7　Eve 发起的测量−重发攻击的量子线路及其仿真结果

5.2　应用于半量子隐私比较

半量子隐私比较[38-45]旨在不泄露半量子参与者隐秘数据的前提下比较这些隐秘数据的相等性或大小关系。接下来将本文协议应用到半量子隐私比较中。

1) 应用于半量子隐私相等性比较

半量子参与者 P_i 的二进制秘密序列为 M_i，其中 $i \in \{0,1,\cdots,N-1\}$。P_i 和 $P_{(i+1)\bmod N}$ 想要在半忠诚量子第三方 TP 的帮助下判断出 M_i 和 $M_{(i+1)\bmod N}$ 是否相等，但不能将 M_i 和 $M_{(i+1)\bmod N}$ 泄露给持有者之外的其他人。可利用下述协议来实现这一目标。

步骤 1~6 同 1.2 节的步骤 1~6。

步骤 7　P_i 计算

$$R_i = M_i \oplus K_{Ti} \oplus K_{i((i+1)\bmod N)} \tag{28}$$

$P_{(i+1)\bmod N}$ 计算

$$R_{(i+1)\bmod N} = M_{(i+1)\bmod N} \oplus K_{T((i+1)\bmod N)} \oplus K_{i((i+1)\bmod N)} \tag{29}$$

随后，P_i 和 $P_{(i+1)\bmod N}$ 分别将 R_i 和 $R_{(i+1)\bmod N}$ 通过认证的经典信道发送给 TP。TP 计算

$$\begin{aligned} R = R_i \oplus R_{(i+1)\bmod N} \oplus K_{Ti} \oplus K_{T((i+1)\bmod N)} = \\ \left(M_i \oplus K_{Ti} \oplus K_{i((i+1)\bmod N)}\right) \oplus \\ \left(M_{(i+1)\bmod N} \oplus K_{T((i+1)\bmod N)} \oplus K_{i((i+1)\bmod N)}\right) \oplus \\ K_{Ti} \oplus K_{T((i+1)\bmod N)} = M_i \oplus M_{(i+1)\bmod N} \end{aligned} \tag{30}$$

并向P_i和$P_{(i+1)\bmod N}$公布R。如果R是一串全零序列，P_i和$P_{(i+1)\bmod N}$将认为M_i和$M_{(i+1)\bmod N}$相等；否则，P_i和$P_{(i+1)\bmod N}$将认为M_i和$M_{(i+1)\bmod N}$不相等。

2) 应用于半量子隐私大小比较

半量子参与者P_i的秘密整数为M_i，其中$M_i \in \{0,1,\cdots,h\}$，$i \in \{0,1,\cdots,N-1\}$且$h=\dfrac{d-1}{2}$。P_i和P_j想要在半忠诚量子第三方TP的帮助下判断出M_i和M_j的大小关系，但不能将M_i和M_j泄露给持有者之外的其他人，其中$i,j \in \{0,1,\cdots,N-1\}$且$i \neq j$。可利用下述协议来实现这一目标。其中，$\oplus$与$\ominus$分别代表模$d$和与模$d$减。

步骤1~6同1.2节的步骤1~6。

步骤7　K_{Ti}、$K_{T((i+1)\bmod N)}$和$K_{i((i+1)\bmod N)}$的每$\lceil \mathrm{lb}(d) \rceil$个比特分别被转化为一个$d$进制数，从而形成新密钥序列$K'_{Ti}$、$K'_{T((i+1)\bmod N)}$和$K'_{i((i+1)\bmod N)}$，其中$\lceil\ \rceil$代表向上取整。$P_i$计算

$$R_i = M_i \oplus K'_{Ti} \oplus K'_{i((i+1)\bmod N)} \tag{31}$$

$P_{(i+1)\bmod N}$计算

$$R_{(i+1)\bmod N} = M_{(i+1)\bmod N} \oplus K'_{T((i+1)\bmod N)} \oplus K'_{i((i+1)\bmod N)} \tag{32}$$

然后，P_i和$P_{(i+1)\bmod N}$分别将R_i和$R_{(i+1)\bmod N}$通过认证的经典信道发送给TP。TP计算

$$\begin{aligned} &R_{i((i+1)\bmod N)} = R_i \ominus R_{(i+1)\bmod N} \ominus K'_{Ti} \oplus K'_{T((i+1)\bmod N)} = \\ &\left(M_i \oplus K'_{Ti} \oplus K'_{i((i+1)\bmod N)}\right) \ominus \left(M_{(i+1)\bmod N} \oplus K'_{T((i+1)\bmod N)} \oplus K'_{i((i+1)\bmod N)}\right) \ominus K'_{Ti} \oplus K'_{T((i+1)\bmod N)} = \\ &M_i \ominus M_{(i+1)\bmod N} \end{aligned} \tag{33}$$

当$i<j$时，TP计算

$$\begin{aligned} &R_{ij} = R_{i(i+1)} \oplus R_{(i+1)(i+2)} \oplus \cdots \oplus R_{(j-1)j} = \\ &(M_i \ominus M_{i+1}) \oplus (M_{i+1} \ominus M_{i+2}) \oplus \cdots \oplus (M_{j-1} \ominus M_j) = \\ &M_i \ominus M_j \end{aligned} \tag{34}$$

当$i>j$时，TP计算

$$\begin{aligned} &R_{ji} = R_{j(j+1)} \oplus R_{(j+1)(j+2)} \oplus \cdots \oplus R_{(i-1)i} = \\ &(M_j \ominus M_{j+1}) \oplus (M_{j+1} \ominus M_{j+2}) \oplus \cdots \oplus (M_{i-1} \ominus M_i) = \\ &M_j \ominus M_i \end{aligned} \tag{35}$$

其中，$i,j \in \{0,1,\cdots,N-1\}$且$i \neq j$。

根据式(34)和式(35)可知，如果$R_{ij}=0$，则有$M_i=M_j$；如果$0<R_{ij} \leqslant h$，则有$M_i>M_j$；如果$h<R_{ij} \leqslant 2h$，则有$M_i<M_j$。其中，$i,j \in \{0,1,\cdots,N-1\}$且$i \neq j$。最后，TP向$P_i$和$P_j$公布$M_i$和$M_j$的大小关系。

5.3　应用于半量子秘密共享

半量子秘密共享[46-50]旨在实现“量子参与者的隐秘数据被多个半量子参与者共享且只有当这些半量子参与者一起合作时才能恢复出量子参与者的隐秘数据”这一功能。接下来将本文协议应用到半量子秘密共享中。

量子TP的二进制秘密序列为M_{TP}。TP计划让半量子$P_0,P_1,\cdots,P_{N-1}$共享M_{TP}。可利用下述协议来实现这一目标。

步骤1~6同1.2节的步骤1~6。

步骤7　TP计算

$$R = M_{TP} \oplus K_{T0} \oplus K_{T1} \oplus \cdots \oplus K_{T(N-1)} \tag{36}$$

并向$P_0,P_1,\cdots,P_{N-1}$公布R。显然，只有当$P_0,P_1,\cdots,P_{N-1}$一起合作时才能获取M_{TP}。

6　结束语

本文采用具有极化和空模自由度的单光子作为量子资源设计了一种新颖的半量子密钥分配网络协议，实现“量子参与者与每个半量子参与者建立不同密钥，同时又帮助每2个相邻半量子参与者建立不同密钥”的功能。该协议无须量子纠缠态、量子纠缠交换操作、量子延迟线以及哈达玛操作，而且只需进行单光子测量。

本文协议假设量子信道是无噪声的且量子设备是理想的，如何设计基于双自由度单光子的适用于含噪量子信道的半量子密钥分配网络协议、基于双自由度单光子的量子设备无关的半量子密钥分配网络协议值得进一步研究。另外，本文仅将所设计的协议应用于半量子求和、半量子隐私比较和半量子秘密共享上，如何进一步拓展所设计的协议的应用范围，如将其应用于量子匿名投票、量子区块链等领域，也值得进一步研究。

参考文献：

[1] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Piscataway: IEEE Press, 1984: 175-179.

[2] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters, 1991, 67(6): 661-663.

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

[4] CABELLO A. Quantum key distribution in the holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635-5638.

[5] HWANG W Y. Quantum key distribution with high loss: toward global secure communication[J]. Physical Review Letters, 2003, 91(5): 057901.

[6] LI X H, DENG F G, ZHOU H Y. Efficient quantum key distribution over a collective noise channel[J]. Physical Review A, 2008, 78(2): 022321.

[7] ZHANG C M, SONG X T, TREEVIRIYANUPAB P, et al. Delayed error verification in quantum key distribution[J]. Chinese Science Bulletin, 2014, 59(23): 2825-2828.

[8] SCARANI V, ACÍN A, RIBORDY G, et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations[J]. Physical Review Letters, 2004, 92(5): 057901.

[9] BOYER M, KENIGSBERG D, MOR T. Quantum key distribution with classical bob[J]. Physical Review Letters, 2007, 99(14): 140501.

[10] BOYER M, GELLES R, KENIGSBERG D, et al. Semiquantum key distribution[J]. Physical Review A, 2009, 79(3): 032341.

[11] NIE Y Y, LI Y H, WANG Z S. Semi-quantum information splitting using GHZ-type states[J]. Quantum Information Processing, 2013, 12(1): 437-448.

[12] ZOU X F, QIU D W, LI L Z, et al. Semiquantum-key distribution using less than four quantum states[J]. Physical Review A, 2009, 79(5): 052312.

[13] WANG J, ZHANG S, ZHANG Q, et al. Semiquantum key distribution using entangled states[J]. Chinese Physics Letters, 2011, 28(10): 100301.

[14] ZOU X F, QIU D W, ZHANG S Y, et al. Semiquantum key distribution without invoking the classical party's measurement capability[J]. Quantum Information Processing, 2015, 14(8): 2981-2996.

[15] YE T Y, LI H K, HU J L. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom[J]. International Journal of Theoretical Physics, 2020, 59(9): 2807-2815.

[16] YE T Y, GENG M J, XU T J, et al. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom[J]. Quantum Information Processing, 2022, 21 (4): 123.

[17] XU T J, YE T Y. A novel two-party semiquantum key distribution protocol based on GHZ-like states[J]. Scientia Sinica Physica, Mechanica & Astronomica, 2022, 52(12): 120312.

[18] ZHANG X Z, GONG W G, TAN Y G, et al. Quantum key distribution series network protocol with *M*-classical Bobs[J]. Chinese Physics B, 2009, 18(6): 2143-2148.

[19] ZHOU N R, ZHU K N, ZOU X F. Multi-party semi-quantum key distribution protocol with four-particle cluster states[J]. Annalen der Physik, 2019, 531(8): 1800520.

[20] TIAN Y, LI J, YE C Q, et al. Multi-party semi-quantum key distribution protocol based on hyperentangled Bell states[J]. Frontiers in Physics, 2022, 10: 1023443.

[21] PAN H M. Multi-party semiquantum key distribution with multi-qubit GHZ states[J]. Quantum Information Processing, 2024, 23(2): 50.

[22] TSAI C W, WANG C H. Multi-party quantum key distribution protocol in quantum network[J]. EPJ Quantum Technology, 2024, 11(1): 63.

[23] LIU D, CHEN J L, JIANG W. High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom[J]. International Journal of Theoretical Physics, 2012, 51(9): 2923-2929.

[24] YANG Y G, XIA J, JIA X, et al. Comment on quantum private comparison protocols with a semi-honest third party[J]. Quantum Information Processing, 2013, 12(2): 877-885.

[25] CAI Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons[J]. Physics Letters A, 2006, 351(1/2): 23-25.

[26] GISIN N, RIBORDY G, TITTEL W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

[27] DENG F G, ZHOU P, LI X H, et al. Robustness of two-way quantum communication protocols against Trojan horse attack[J]. arXiv Preprint, arXiv: 0508168, 2005.

[28] LI X H, DENG F G, ZHOU H Y. Improving the security of secure direct communication based on the secret transmitting order of particles[J]. Physical Review A, 2006, 74(5): 054302.

[29] GAO F, QIN S, WEN Q, et al. A simple participant attack on the Bradler-Dusek protocol[J]. Quantum Information and Computation, 2007, 7(4): 329-334.

[30] CHEN Z B, PAN J W, ZHANG Y D, et al. All-versus-nothing violation of local realism for two entangled photons[J]. Physical Review Letters, 2003, 90(16): 160408.

[31] YANG T, ZHANG Q, ZHANG J, et al. All-versus-nothing violation of local realism by two-photon, four-dimensional entanglement[J]. Physical Review Letters, 2005, 95(24): 240406.

[32] ZENG H, DU M M, ZHONG W, et al. High-capacity device-independent quantum secure direct communication based on hyper-encoding[J]. Fundamental Research, 2024, 4(4): 851-857.

[33] ZHANG C, HUANG Q, LONG Y X, et al. Secure three-party semi-quantum summation using single photons[J]. International Journal of Theoretical Physics, 2021, 60(9): 3478-3487.

[34] YE T Y, XU T J, GENG M J, et al. Two-party secure semiquantum summation against the collective-dephasing noise[J]. Quantum Information Processing, 2022, 21(3): 118.

[35] HU J L, YE T Y. Three-party secure semiquantum summation without entanglement among quantum user and classical users[J]. International Journal of Theoretical Physics, 2022, 61(6): 170.

[36] LIAN J Y, YE T Y. Hybrid protocols for multi-party semiquantum private comparison, multiplication and summation without a pre-shared key based on d-dimensional single-particle states[J]. EPJ Quantum Technology, 2024, 11(1): 17.

[37] YE C Q, LI J, CHEN X B, et al. Semi-quantum secure multiparty summation and its applications to anonymous auction and ranking[J]. Advanced Quantum Technologies, 2024, 7(3): 2300347.

[38] CHOU W H, HWANG T, GU J. Semi-quantum private comparison protocol under an almost-dishonest third party[J]. arXiv Preprint, arXiv: 1607.07961, 2016.

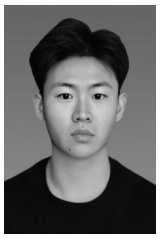
[39] LANG Y F. Semi-quantum private comparison using single photons[J].

International Journal of Theoretical Physics, 2018, 57(10): 3048-3055.
[40] LIN P H, HWANG T, TSAI C W. Efficient semi-quantum private comparison using single photons[J]. Quantum Information Processing, 2019, 18(7): 207.
[41] LIAN J Y, LI X, YE T Y. Multi-party semiquantum private comparison of size relationship with d-dimensional Bell states[J]. EPJ Quantum Technology, 2023, 10(1): 10.
[42] XU X, LIAN J Y, YE T Y. Semiquantum private comparison via cavity QED[J]. Quantum Information Processing, 2024, 23(5): 174.
[43] GENG M J, LI X, YE T Y. Semiquantum private comparison based on Bell states without quantum measurements from the classical user[J]. Laser Physics Letters, 2024, 21(10): 105205.
[44] GONG L H, LI M L, CAO H, et al. Novel semi-quantum private comparison protocol with Bell states[J]. Laser Physics Letters, 2024, 21(5): 055209.
[45] GONG L H, YE Z J, LIU C, et al. One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations[J]. Laser Physics Letters, 2024, 21(3): 035207.
[46] LI Q, CHAN W H, LONG D Y. Semiquantum secret sharing using entangled states[J]. Physical Review A, 2010, 82(2): 022303.
[47] TIAN Y, BIAN G Q, CHANG J Y, et al. A semi-quantum secret-sharing protocol with a high channel capacity[J]. Entropy, 2023, 25 (5): 742.
[48] XING D, WANG Y F, DOU Z, et al. Efficient semi-quantum secret sharing protocol using single particles[J]. Chinese Physics B, 2023, 32 (7): 070308.
[49] YOUNES M A, ZEBBOUDJ S, GHARBI A. A lightweight and efficient multiparty semi-quantum secret sharing protocol using entangled states for sharing specific bit[J]. International Journal of Theoretical Physics, 2024, 63(11): 292.
[50] LI J, YE C Q. Multi-party semi-quantum secret sharing protocol based on measure-flip and reflect operations[J]. Laser Physics Letters, 2024, 21(7): 075201.

[作者简介]

叶天语（1982– ），男，浙江温州人，博士，浙江工商大学教授、硕士生导师，主要研究方向为量子信息、量子计算、量子与半量子密码等。

叶腾琦（1998– ），男，浙江台州人，浙江工商大学硕士生，主要研究方向为量子密码学。



马鹏辉（2001– ），男，山东德州人，浙江工商大学硕士生，主要研究方向为量子密码学、量子计算。

李霞（1988– ），女，山东聊城人，博士，浙江工商大学讲师，主要研究方向为量子信息、量子计算、量子与半量子密码等。