软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(6):2878−2891 [doi: 10.13328/j.cnki.jos.006504]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

具有少量参与者的分层量子密钥分发协议*

闫晨红, 李志慧, 刘 璐, 韩召伟

(陕西师范大学 数学与统计学院, 陕西 西安 710119)

通信作者: 李志慧, E-mail: lizhihui@snnu.edu.cn

摘 要: 分层量子密钥分发在量子通信中有重要作用, 除了使用 EPR 与 GHZ 态可实现分层量子密钥分发, 非对称高维多粒子纠缠也为解决分层量子密钥分发提供了一种新思路, 这种方法在量子信道使用次数上比传统的使用二部链路的量子密钥分发更有效. 介绍了 3 用户在同构意义下的 5 种分层密钥结构, 并给出 4、5 用户的可分区分层密钥结构. 然后对于所介绍的各类分层密钥结构, 通过将上述两种方法进行对比, 得到实现各类密钥结构理想化密钥率最高的方案. 当量子网络用户大于 3 且密钥结构可分区时, 证明仅使用 EPR 与 GHZ 态就可实现各层理想化密钥率是 1, 并以 4、5 用户的可分区分层密钥结构为例展开说明.

关键词: 分层量子密钥分发; 非对称高维多粒子纠缠; 理想化密钥率; GHZ 态与 EPR 态

中图法分类号: TP309

中文引用格式: 闫晨红, 李志慧, 刘璐, 韩召伟. 具有少量参与者的分层量子密钥分发协议. 软件学报, 2023, 34(6): 2878–2891. http://www.jos.org.cn/1000-9825/6504.htm

英文引用格式: Yan CH, Li ZH, Liu L, Han ZW. Layered Quantum Key Distribution Protocol with a Small Number of Participants. Ruan Jian Xue Bao/Journal of Software, 2023, 34(6): 2878–2891 (in Chinese). http://www.jos.org.cn/1000-9825/6504.htm

Layered Quantum Key Distribution Protocol with a Small Number of Participants

YAN Chen-Hong, LI Zhi-Hui, LIU Lu, HAN Zhao-Wei

(School of Mathematics and Statistics, Shaanxi Normal University, Xi'an 710119, China)

Abstract: Layered key structure plays an important role in quantum communication, in addition to using EPR and GHZ states to achieve layered quantum key distribution, asymmetric high dimensional multi-particle entanglement also provides a new idea for solving layered quantum key distribution. This method is more efficient in the number of quantum channel uses than the conventional quantum key distribution using bipartite links. This study introduces five layered key structures for three users, and gives a partitionable key structure for 4 and 5 users. For the various layered key structures introduced in this study, the above two methods are compared to get the protocol with the highest idealized key rate of each key structure. When the quantum network has more than three users and the key structure can be partitioned, it is proved that the idealized key rate of each layer can be 1 by using the EPR and GHZ states. Finally, the partitionable key structure of four and five users is taken as an example to expand the description.

Key words: layered quantum key distribution; asymmetric high dimensional multi-particle entanglement; idealized key rate; GHZ and EPR states

1 介 绍

经典密码依赖于计算的高复杂度, 破解者在有限的时间内无法完成密钥破解, 以此达到保证通信安全的目的. 当计算能力提升到足够强大时, 依赖于计算复杂度的加密算法理论上都可能会被破解. Shanno 提出的"一次一密"加密方法[1]理论上可以实现无条件的安全, 但密钥在分发或协商的过程中存在被窃取的可能, 量子密钥分发

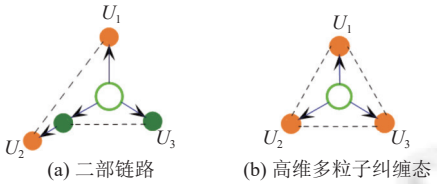
* 基金项目: 国家自然科学基金 (11671244)
收稿时间: 2021-08-11; 修改时间: 2021-09-03; 采用时间: 2021-10-11; jos 在线出版时间: 2022-12-16
CNKI 网络首发时间: 2022-12-19

© 中国科学院软件研究所 http://www.jos.org.cn

(QKD) 利用量子力学中的量子不可克隆定理[2]和量子纠缠的特性[3]来实现通信方共享一组随机密钥, 这为解决“一次一密”中的密钥分发问题提供一个有效途径, 因此量子通信技术得到了前所未有的重视和关注, QKD 也成为量子密码学的重要分支[4], 并且在应用方面也已经取得了很大的进展[5−7]. 量子密钥当前最普遍、最成熟的应用场景是利用量子密钥实现网络层加解密. 通过专用量子加解密设备和量子设备对接, 专用量子加解密设备可以直接从量子设备获取量子密钥, 从而对业务报文进行网络层加解密.

随着量子技术的不断发展, 单粒子和纠缠态作为量子信息的载体已经成为实现 QKD 的一种重要的量子资源. 比如, 1984 年, Bennett 等人[8]利用单光子的偏振态研发了世界上第一个 QKD 协议 (BB84 协议), 在该协议中, 两个用户通过交换单粒子来实现密钥的共享. 1991 年, 牛津大学的 Ekert[9]首次提出利用 Bell 态的纠缠特性构造 QKD 协议. 1992 年, Bennett 等人[10]又提出了使用非正交单光子比特来实现 QKD 协议 (B92 协议). 随后一系列基于单粒子态和纠缠态的 QKD 协议接连被提出[11−15], 协议的安全性也已经被详细分析[16−20].

然而大部分 QKD 协议都是双方间的密钥分发, 在实际的量子网络中, 经常要进行多个用户的密钥分发, 因此将 QKD 协议推广到多方是一个热门话题. 1995 年, Phoenix 等人[21]提出了第一个基于单粒子态的多用户量子密钥分发协议. 随后, 各式各样的基于单粒子、Bell 态和 GHZ 态等的多用户 QKD 协议也不断被提出[22−27]. 从这些协议中我们总结出多方 QKD 协议主要遵循以下两种不同路径: 从两方 QKD 链接建立多方密钥或者利用真正多粒子纠缠态的相关性建立多方密钥. 然而, 对于分层量子通信, 以上的多方 QKD 协议有两类不足: (1) 在单位时间内只能完成一层 (一个用户子集) 的密钥分发, 无法同时为不同的用户子集提供各自安全密钥, 导致各层理想密钥率不高; (2) 对比使用高维多粒子纠缠实现 QKD 协议, 以上方案在一个单位时间内所需量子发送源较多. 为解决这两种不足, 分层量子通信充分利用了纠缠结构, 仅使用单个量子态源就可以为不同的参与方子集提供安全密钥. 这种方法在量子信道使用数量上比传统的使用二部链路的量子密钥分配更高效. 例如图 1 展示了 3 用户分别使用传统二部链路 (图 1(a)) 与高维多粒子纠缠态 (图 1(b)) 两种方法实现 3 用户共享密钥所需的量子信道数. 图中黑色箭头表示量子信道的使用情况, 图 1(a) 中量子信道的使用个数为 4, 图 1(b) 中量子信道的使用个数为 3. 除此之外在两方通信中, 虽然违反 Bell 不等式的双粒子纠缠足以保证完全设备无关的安全性[28,29], 但由于需要严格的技术要求支撑 (比如极高的检测和耦合效率等) 这类方案在实践中很难实现. 所以使用高维多粒子纠缠来实现分层 QKD 不仅在量子信道的使用次数上优于传统方法, 而且具有实际操作性.



(a) 二部链路 (b) 高维多粒子纠缠态

图 1 使用二部链路与高维多粒子纠缠态实现 3 方密钥共享所需量子信道数

目前大量文献说明量子态维数对 QKD 协议的密钥率有很大的影响[30−32], 它可以显著改善协议对抗噪声以及其他潜在的安全泄漏的能力[33,34]. 除此之外基于多粒子纠缠的协议也可以从网络编码中获益[35], 因此纠缠粒子的数目也对 QKD 效率有极大影响. Lanyon 等人[36,37]的实验增加了纠缠粒子的数量, 但每个粒子都只存在于 2 维空间中. 2013 年 Huber 等人[38]的实验首次展示了粒子数和维数都大于 2 的多光子纠缠态的产生, 并发现在高维状态下多粒子纠缠态表现出非对称结构的性质. 随后, 学者们产生了大量制备高维多粒子纠缠的技术, 同时测量高维量子态的实验方法也在迅速成熟[39−41]. 高维多粒子纠缠所表现出的非对称性对提高分层密钥结构的量子通信效率也有重要意义. 基于这一思想, 2016 年 Malik 等人[41]将非对称三粒子纠缠态 $|\Psi_{332}\rangle$ 应用到分层量子通信协议, $|\Psi_{332}\rangle$ 的前两个光子的局部维数是 3, 第 3 个光子的局部维数是 2, 此方案使双方在与第三方已经共享一层密钥的基础上同时共享另一层安全信息, 但方案的理想化密钥率并不完美. 2018 年 Pivoluska 等人[42]使用非对称高维多粒子纠缠态 $|\Psi_{442}\rangle$ 实现 Malik 等人在文献 [41] 的 3 用户密钥结构, 此方案的各层理想化密钥率均可达到 1. 在这种分层量子通信协议成为现实之前, 还需要探索实现各类分层密钥结构理想化密钥率最高的方法以及完成相关高维多粒子

© 中国科学院软件研究所 http://www.jos.org.cn

纠缠态的制备. 为了实现高维量子通信, Liu 等人[43]从 2016 年开始采用光子的路径自由度编码, 制备出高保真度的 3 维纠缠态, 实现了制备 32 维量子纠缠态. 2017 年起, 他们将目标瞄准高维量子隐形传态, 通过实验结果表明, 量子隐形传态保真度达 59.6%, 以 7 个标准差超过了经典极限值 1/3, 证实了 3 维量子隐形传态过程的量子特性, 为构建高效的高维量子网络打下坚实基础.

本文基于文献 [41,42] 的研究, 细化分析了 3 用户在图同构意义下的 5 种分层密钥结构, 以及 4、5 用户可分区分层密钥结构, 解决了少量用户在当前业内量子密钥使用场景单一且调度不够灵活的问题. 对于 3 用户量子网络, 我们构造出实现每种密钥结构的非对称高维多粒子纠缠态, 然后各用户对量子态进行局部测量并对测量结果进行特殊编码, 从而用户可以同时共享各层的多方密钥, 最终建立分层密钥分发协议. 我们也将其与使用 EPR 与 GHZ 态的分层量子密钥分发 (LQKD) 协议进行对比, 故对任意一个 3 用户的量子网络, 我们都可找到文中所例举的对应同构类型并且找到理想化密钥率最高的方案去实现 LQKD 协议. 对 4、5 等多用户而言, 虽然使用高维多粒子纠缠实现密钥分配在量子信道使用的数量以及协议对抗噪声和其他潜在的安全泄漏的能力具有优势, 但由于密钥结构层数可能过多, 而构造非对称高维多粒子纠缠态的各粒子维数随密钥层数指数扩大, 所以要达到各层密钥速率达到 1 的一般形式过于复杂. 我们证明了在可分区分层密钥结构下, 不用构造复杂的不对称高维多粒子纠缠态同样可高效实现 LQKD 协议, 并给出 4、5 用户可分区分层密钥结构的具体实现方案.

第 2 节介绍了本文所需的预备知识, 包括分层密钥结构、连通密钥结构与分区、纠缠态量子网络模型以及高维多粒子纠缠态的构造. 第 3 节给出 3 用户在同构意义下的 5 种分层密钥结构, 以及 4、5 用户可分区分层密钥结构. 第 4 节分析了 3、4、5 用户的各类分层密钥结构的理想化密钥率, 并得出在每种密钥结构下理想化密钥率最高的方案. 第 5 节对本文研究结果进行了总结.

2 预备知识

本节我们介绍了分层密钥结构并在此基础上介绍了连通密钥结构与分区.

2.1 分层密钥结构

在一个 n 用户的量子网络中, 设 $S=\{U_1,U_2,\ldots,U_n\}$ 为 n 个用户的集合, 在实际应用中我们除了需要两用户间可共享的双方密钥外, 还需要在人数大于 2 的用户子集中产生多方密钥.

定义 1. 给定一个 n 用户的量子网络, 将进行安全通信所需的各种类型密钥 (比如双方密钥以及多方密钥) 的集合称为分层密钥结构 K.

下面我们为了便于表达, 引入描述分层密钥结构 K 的一些相关参数, K 是所有用户 $S=\{U_1,U_2,\ldots,U_n\}$ 幂集的一个子集, 即 $K\subseteq P(S)$. 定义 E 为分层密钥结构的总层数, 且 $e\in\{1,2,\ldots,E\}$ 表示该分层密钥结构的某一层; r_e 表示第 e 层的理想化密钥率, r_e 的计算见第 4 节; t_i 表示用户 U_i 所属层的个数, 用数学语言描述为: $t_i=|\{e\in K|U_i\in e\}|$. 下面我们例举一个简单的分层密钥结构, 如图 2 所示, 这是一个 4 用户 6 层的分层密钥结构, 密钥层分别为: $\{U_1,U_2\},\{U_1,U_3\},\{U_1,U_4\},\{U_2,U_3\},\{U_2,U_4\},\{U_3,U_4\}$. 因为每层都有 2 个用户, 故 $t_1=t_2=t_3=t_4=2$.

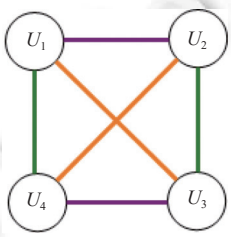


图 2 4 用户 6 层密钥结构

2.2 连通密钥结构与分区

分层密钥结构的类型众多, 然而为任意密钥结构找到可实现密钥率达到 1 的方案其构造比较复杂, 并且会涉

© 中国科学院软件研究所 http://www.jos.org.cn

及太多的参数. 下面我们介绍特殊的分层密钥结构——连通密钥结构与分区.

定义 2[44,45]. 每个分层密钥结构 K 可定义一个邻域图 G_K, 用户 U_i $(i=1,2,\ldots,n)$ 表示邻域图 G_K 中的顶点, 如果两个用户 U_i 和 U_j 在密钥结构 K 中共享一层, 则通过一条边将 U_i 和 U_j 连接. 在分层密钥结构 K 的邻域图 G_K 中, 如果任意两个顶点之间都存在连通路径, 那么称分层密钥结构 K 为连通密钥结构. 例如在图 2 所示的 4 用户 6 层密钥结构中, 由于任意两个用户之间都有连通的路径, 因此它是一个连通密钥结构.

若邻域图 G_K 的任意两个顶点之间不存在连通路径, 则密钥结构不连通. 例如在图 3 所示的 6 用户 2 层密钥结构中, 密钥层分别为: $\{U_1,U_2,U_3,U_4\},\{U_5,U_6\}$. 由于 U_1 和 U_5 之间不存在连通路径, U_1 和 U_6 之间也不存在连通路径, 该图中还有很多顶点之间不存在路径, 因此图 3 不是一个连通图.

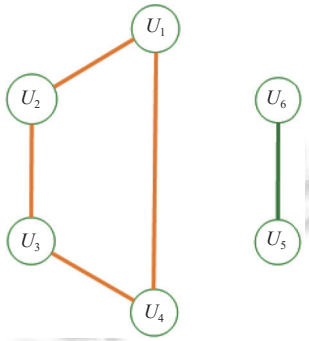


图 3 6 用户 2 层密钥结构

图 3 虽然不是一个连通图, 但它有多个连通子图, 比如 U_1,U_2,U_3 的顶点构成的子图是连通图, 故 U_1,U_2,U_3 构成一个连通子图, 我们把最大连通子图称为它的连通分量[44]. 由于 U_1,U_2,U_3,U_4 的顶点构成的子图就是该图的最大连通子图, 故 U_1,U_2,U_3,U_4 是图 3 的连通分量, 同理 U_5,U_6 也是图 3 的连通分量.

由于发送源可以同时向每个连通分量发送量子态, 故每个分层密钥结构 K 的连通分量可单独处理, 它们的密钥率不依赖于其他连通分量. 所以下文我们只讨论连通密钥结构, 即 t_i $(i=1,2,\ldots,n)$ 不全为 1 的情况.

定义 3. 在一个 n 用户的连通密钥结构 K 下, 设 P_i 是所有层的一个子集. 如果 P_i 中的各层用户之间是互斥的, 并且 P_i 所有层用户的并集等于 $S=\{U_1,U_2,\ldots,U_n\}$, 那么就称 P_i 是连通密钥结构 K 的一个分区, 由于每个连通密钥结构可能包含几个分区, 故用下标 i 来表示每个分区的指标集. 用数学语言可以将分区 P_i 描述为:

$$P_i=\left\{e_1,\ldots,e_a\in K\middle|\bigcup_a e_a=S,\forall a,b:e_a\cap e_b=\varnothing\right\}.$$

图 2 是一个 4 用户 6 层的连通密钥结构, 同时该分层密钥结构又可划分为 3 个分区, 分别为: $P_1=\{\{U_1,U_2\},\{U_3,U_4\}\},P_2=\{\{U_1,U_4\},\{U_2,U_3\}\},P_3=\{\{U_1,U_3\},\{U_2,U_4\}\}$.

2.3 纠缠态量子网络模型

由于密钥率取决于网络架构 (文献 [42] 所示), 本节我们构建纠缠态量子网络模型.

纠缠态分发模型: 在有 n 个用户的量子网络中, 每个用户 U_i $(i=1,2,\ldots,n)$ 可通过量子信道连接到纠缠发送源, 发送源可以向任何用户子集发送纠缠态, 并且每用户对 $\left(U_i,U_j\right)$ 共享一个安全的经典信道 (见图 4). 图 4 中绿色圆盘表示纠缠态发送源, 蓝色的箭头表示发送源通过量子信道发送给各个用户纠缠态粒子, 虚线表示两个用户之间通过一个可认证的经典信道进行通信.

利用上述纠缠态分发模型, 我们可通过以下两种方法实现 LQKD 协议.

方法 1: 文献 [42] 在分层密钥结构 K 下, 构造出可实现 K 的非对称高维多粒子纠缠态 $|\Psi_K\rangle$, 然后使用上述纠缠态分发模型实现 LQKD 协议.

方法 2: 使用 $|EPR_d\rangle=\dfrac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle$ 与 $\left|GHZ_d^n\right\rangle_{U_1,\ldots,U_n}=\dfrac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\ldots i\rangle_{U_1,\ldots,U_n}$ 态 (其中 d 表示量子态的维数, n 表示

© 中国科学院软件研究所 http://www.jos.org.cn

粒子的个数) 实现 LQKD 协议.

1) 当某密钥层用户人数为 2, 使用 EPR 态可实现两用户间的密钥共享[4].

2) 当某密钥层用户人数大于 2, 使用不同维数的 GHZ 态, 直接在该层进行密钥分发[35].

为公平对比上述两种方法, 量子纠缠态分发的时隙需要保持一致, 我们允许纠缠态同时分布到互斥的用户集合. 除此之外, 在量子网络中, 需要限制每个用户局域测量的维数, 本文在用户局域测量方面的限制在与文献 [42] 相似.

注意: 当使用 EPR 与 GHZ 态实行 LQKD 协议时, 为了在维数方面的对比相对公平, EPR 与 GHZ 态的维数应与构造的非对称高维多粒子纠缠态的局部维数尽量保持一致.

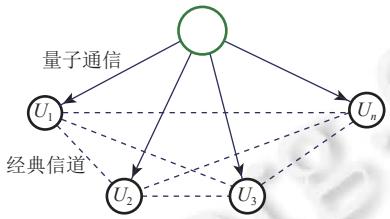


图 4 纠缠态分发模型

2.4 高维多粒子纠缠态的构造

假设给定一个分层密钥结构 K, 我们构造高维多粒子纠缠态 $|\Psi_K\rangle$ 用于 K 的实现. 该构造是基于在高维空间下, 根据每层用户的数量, 由 GHZ 和 EPR 态做张量积来构造每层的纠缠量子态, 最后将每层所构造出的量子态叠加得到 $|\Psi_K\rangle$. 下面给出具体步骤.

1) 首先对于第 e 层的第 i 个用户, 记用户 U_i 所持有的量子比特记为 u_i^e.

2) 对于每一层 $e\in K$, 我们定义态 $|\Psi_e\rangle:=\dfrac{1}{\sqrt{2}}\left(\otimes_i|0\rangle_{U_i}+\otimes_i|1\rangle_{U_i}\right)$, 其中下标 U_i 在第 e 层的用户.

3) 定义 $|\Psi_K\rangle:=\otimes_{e=1}^{E}|\Psi_e\rangle$.

4) 每个用户 U_i 将其 t_i 个量子比特 $\left\{u_i^e\right\}$ 编码到 $d_i=2^{t_i}$ 维的高维量子态寄存器 R_i 中, 方法是将二进制的量子比特字符串转化为数字.

5) 最后产生的态 $|\Psi_K\rangle$ 是 2^E 个被重新编码的量子态的相等叠加.

从高维多粒子态 $|\Psi_K\rangle$ 的构造方法过程中, 我们可以得到每个用户 U_i 所拥有的量子态的各粒子维数与其所在层的个数 t_i 息息相关, 每一个量子位的维数为 2^{t_i}.

3 用户数为 3、4、5 的分层密钥结构

本节我们在同构意义下给出用户数为 3 的分层密钥结构, 并给出 4、5 用户的可分区分层密钥结构.

3.1 3 用户的分层密钥结构

由每个分层密钥结构都可定义一个邻域图, 在 3 用户的量子网络中, 若两个密钥结构具有相同数量的层数, 且每层用户数相等, 由图同构[44,45]的概念可知, 这两个密钥结构的邻域图是同构的.

在同构意义下, 3 用户的分层密钥结构共有 5 种, 如表 1 所示, 我们规定分层密钥结构的表示形式为 $[n(a_1,a_2,\ldots,a_k)]$, 其中 n 表示量子网络的用户总数, a_k 表示第 k 层用户的个数.

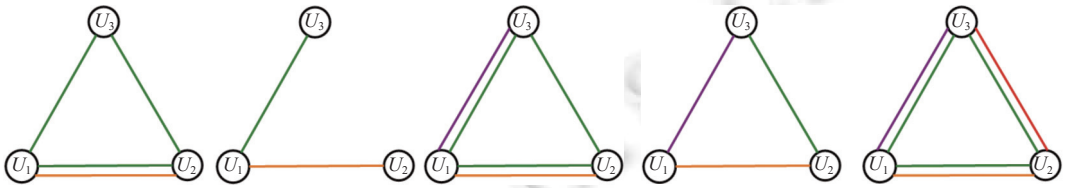
3 用户各分层密钥结构示意图见图 5, 其中图 5(a) 表示 [3(3,2)] 在同构意义下的示意图, [3(3,2)] 包含的分层密钥结构有: $\{\{U_1,U_2,U_3\},\{U_1,U_2\}\}$, $\{\{U_1,U_2,U_3\},\{U_1,U_3\}\}$, $\{\{U_1,U_2,U_3\},\{U_2,U_3\}\}$. 图 5(b) 表示 [3(2,2)] 在同构意义下的示意图, [3(2,2)] 包含的分层密钥结构有: $\{\{U_1,U_2\},\{U_1,U_3\}\}$, $\{\{U_1,U_2\},\{U_2,U_3\}\}$, $\{\{U_1,U_3\},\{U_2,U_3\}\}$. 图 5(c) 表示 [3(3,2,2)] 在同构意义下的示意图, [3(3,2,2)] 包含的分层密钥结构有: $\{\{U_1,U_2,U_3\},\{U_1,U_2\},\{U_1,U_3\}\}$, $\{\{U_1,U_2,U_3\},\{U_1,U_2\},\{U_2,U_3\}\}$, $\{\{U_1,U_2,U_3\},\{U_1,U_3\},\{U_2,U_3\}\}$. 图 5(d) 表示 [3(2,2,2)] 在同构意义下的示意图, 此

© 中国科学院软件研究所 http://www.jos.org.cn

类型的密钥结构只有$\{U_1,U_2\},\{U_1,U_3\},\{U_2,U_3\}$. 图 5(e) 表示[3(3,2,2,2)]在同构意义下的示意图, 此类型的密钥结构只有$\{U_1,U_2\},\{U_1,U_3\},\{U_2,U_3\},\{U_1,U_2,U_3\}$.

表 1　在同构意义下 3 用户的分层密钥结构

密钥层数	类型	分层密钥结构	表示形式
2	1	$\{U_1,U_2\},\{U_1,U_2,U_3\}$	[3(2,3)]
	2	$\{U_1,U_2\},\{U_1,U_3\}$	[3(2,2)]
3	3	$\{U_1,U_2\},\{U_1,U_3\},\{U_1,U_2,U_3\}$	[3(2,2,3)]
	4	$\{U_1,U_2\},\{U_1,U_3\},\{U_2,U_3\}$	[3(2,2,2)]
4	5	$\{U_1,U_2\},\{U_1,U_3\},\{U_2,U_3\},\{U_1,U_2,U_3\}$	[3(2,2,2,3)]



(a) [3(3,2)]　(b) [3(2,2)]　(c) [3(3,2,2)]　(d) [3(2,2,2)]　(e) [3(3,2,2,2)]

图 5　3 用户的 5 种类型分层密钥结构

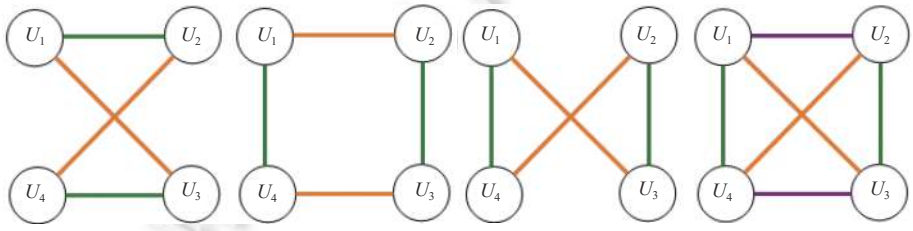
3.2　4 用户可分区分层密钥结构

4 用户可分区分层密钥结构一共有 4 种, 可分为两种类型, 如表 2 所示. 我们定义m分区分层密钥结构的表示形式为$\left[n\left(a_1^1,a_2^1,\ldots,a_k^1\right)\left(a_1^2,a_2^2,\ldots,a_k^2\right)\ldots\left(a_1^m,a_2^m,\ldots,a_k^m\right)\right]$, 其中$n$表示量子网络的用户总数, a_k^m表示第m分区的第k层用户的数目, 若每个分区的层结构相似且单层用户数相等, 则分层密钥结构的表示形式可记作$\left[n\left(a_1,a_2,\ldots,a_k\right)_v\right]$, 其中$v$表示相似分区结构的个数.

表 2　4 用户可分区分层密钥结构

密钥层数与分区	类型	分层密钥结构	表示形式
2分区4层	1	$\{\{U_1,U_2\},\{U_3,U_4\}\},\{\{U_1,U_3\},\{U_2,U_4\}\}$ $\{\{U_1,U_4\},\{U_2,U_3\}\},\{\{U_1,U_2\},\{U_3,U_4\}\}$ $\{\{U_1,U_4\},\{U_2,U_3\}\},\{\{U_1,U_3\},\{U_2,U_4\}\}$	$[4(2,2)_2]$
3分区6层	2	$\{\{U_1,U_2\},\{U_3,U_4\}\},\{\{U_1,U_4\},\{U_2,U_3\}\},\{\{U_1,U_3\},\{U_2,U_4\}\}$	$[4(2,2)_3]$

4 用户可分区分层密钥结构的示意图见图 6, 2 分区结构$[4(2,2)_2]$包含的分层密钥结构类型有$\{\{U_1,U_2\},\{U_3,U_4\}\},\{\{U_1,U_3\},\{U_2,U_4\}\}$, $\{\{U_1,U_4\},\{U_2,U_3\}\},\{\{U_1,U_2\},\{U_3,U_4\}\}$, $\{\{U_1,U_4\},\{U_2,U_3\}\},\{\{U_1,U_3\},\{U_2,U_4\}\}$, 分别对应图 6(a), 图 6(b), 图 6(c). 3 分区结构$[4(2,2)_3]$包含的分层密钥结构类型只有 $\{\{U_1,U_2\},\{U_3,U_4\}\},\{\{U_1,U_4\},\{U_2,U_3\}\},\{\{U_1,U_3\},\{U_2,U_4\}\}$, 如图 6(d) 所示.



(a) 2 分区结构 1　(b) 2 分区结构 2　(c) 2 分区结构 3　(d) 3 分区结构

图 6　4 用户的可分区分层密钥结构

© 中国科学院软件研究所 http://www.jos.org.cn

3.3 5 用户的可分区分层密钥结构

由于 5 用户的[5(3,2)]分层密钥结构有$C_5^3=10$种, 故 5 用户的 2 分区分层密钥结构有$C_{10}^2=45$种, 取其中一种为例: $\{\{U_1,U_2,U_3\},\{U_4,U_5\}\},\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, 这个分层密钥结构有 2 个分区, 共有两个 3 用户层, 两个 2 用户层, 5 用户其他可分区分层密钥结构可类似得到, 见表 3.

表 3 同构意义下 5 用户的分层密钥结构

密钥层数	类型	分层密钥结构	表示形式
2分区4层	1	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$	$[5(3,2)_2]$
3分区6层	2	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$	$[5(3,2)_3]$
4分区8层	3	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$	$[5(3,2)_4]$
5分区10层	4	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$, $\{\{U_1,U_3,U_5\},\{U_2,U_4\}\}$	$[5(3,2)_5]$
6分区12层	5	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$, $\{\{U_1,U_3,U_5\},\{U_2,U_4\}\}$, $\{\{U_1,U_4,U_5\},\{U_2,U_3\}\}$	$[5(3,2)_6]$
7分区14层	6	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$, $\{\{U_1,U_3,U_5\},\{U_2,U_4\}\}$, $\{\{U_1,U_4,U_5\},\{U_2,U_3\}\}$, $\{\{U_2,U_3,U_4\},\{U_1,U_5\}\}$	$[5(3,2)_7]$
8分区16层	7	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$, $\{\{U_1,U_3,U_5\},\{U_2,U_4\}\}$, $\{\{U_1,U_4,U_5\},\{U_2,U_3\}\}$, $\{\{U_2,U_3,U_4\},\{U_1,U_5\}\}$, $\{\{U_2,U_4,U_5\},\{U_1,U_3\}\}$	$[5(3,2)_8]$
9分区18层	8	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$, $\{\{U_1,U_3,U_5\},\{U_2,U_4\}\}$, $\{\{U_1,U_4,U_5\},\{U_2,U_3\}\}$, $\{\{U_2,U_3,U_4\},\{U_1,U_5\}\}$, $\{\{U_2,U_4,U_5\},\{U_1,U_3\}\}$, $\{\{U_2,U_3,U_5\},\{U_1,U_4\}\}$	$[5(3,2)_9]$
10分区20层	9	$\{\{U_1,U_2,U_3\},\{U_4,U_5\}\}$, $\{\{U_1,U_2,U_4\},\{U_3,U_5\}\}$, $\{\{U_1,U_2,U_5\},\{U_3,U_4\}\}$, $\{\{U_1,U_3,U_4\},\{U_2,U_5\}\}$, $\{\{U_1,U_3,U_5\},\{U_2,U_4\}\}$, $\{\{U_1,U_4,U_5\},\{U_2,U_3\}\}$, $\{\{U_2,U_3,U_4\},\{U_1,U_5\}\}$, $\{\{U_2,U_4,U_5\},\{U_1,U_3\}\}$, $\{\{U_2,U_3,U_5\},\{U_1,U_4\}\}$, $\{\{U_3,U_4,U_5\},\{U_1,U_2\}\}$	$[5(3,2)_{10}]$

4 各类分层密钥结构的密钥率

本节给出理想化密钥率的定义, 并使用第 2.3 节所述方法 1 与方法 2 实现各类分层密钥结构, 得到理想化密钥率最高的方案. 我们证明在可分区分层密钥结构下, 仅使用 EPR 与 GHZ 态就可实现各层理想化密钥率是 1, 最后以 4、5 用户可分区分层密钥结构举例进行说明.

4.1 分层密钥结构的理想化密钥率

在量子密钥分发中密钥率是参与者所能获得的最大安全信息量, 比如在 BB84 协议中, 密钥率则为双 Alice 和 Bob 之间的信息量减去其中可能被窃听者 Eve 窃取的信息量, 这个过程也被称为保密增强, 经过保密增强后得到的密钥信息对于窃听者则是完全保密的. 通常协商过程不能完全提取出 Alice 和 Bob 之间的互信息, 因此用一个协商效率因子 β 来表征提取度, 其中 $\beta\in[0,1]$. 反向协商密钥率为:

$$\begin{cases} R=\beta I(A:B)-S(E:B), \text{集体攻击} \\ R=\beta I(A:B)-I(E:B), \text{个体攻击} \end{cases}.$$

正向协商密钥率为:

$$\begin{cases} R=\beta I(A:B)-S(E:A), \text{集体攻击} \\ R=\beta I(A:B)-I(E:A), \text{个体攻击} \end{cases},$$

其中, $I(A:B)$ 表示 Alice 和 Bob 之间的经典香农信息量, 而 Eve 根据不同的攻击方式获得不同的信息量. $S(E:B)$ 和 $S(E:A)$ 分别表示在反向协商和正向协商的情况下, 集体攻击 Eve 获得的信息量, $I(E:B)$ 和 $I(E:A)$ 分别表示在反

© 中国科学院软件研究所 http://www.jos.org.cn

向协商和正向协商的情况下, 个体攻击 Eve 获得的信息量. 所谓反向协商就是指 Alice 和 Bob 在协商的过程中以 Bob 的信息作为参考来提取密钥, 正向协商则为以 Alice 的信息作为参考[46]. 只要密钥率 $R>0$, 则说明可以提取出对 Eve 完全保密的信息, 即协议在此攻击下是安全的.

对于多方的密钥率的具体计算比较复杂, 详细的计算推导过程见参考文献 [35], 可得到多方密钥率的计算公式:

$$R=\left(1-\frac{Q_Z}{2}-Q_X\right)\log_2\left(1-\frac{Q_Z}{2}-Q_X\right)+\left(Q_X-\frac{Q_Z}{2}\right)\log_2\left(Q_X-\frac{Q_Z}{2}\right)+(1-Q_Z)(1-\log_2(1-Q_Z))-h\left(\max_{1\leqslant i\leqslant N-1}Q_{AB_i}\right).$$

该公式中的参数是从测量数据中获得的, 并取决于参与方的数量. 由于密钥率中涉及太多参数, 计算起来繁琐, 理想化的密钥率可以直接反映实现密钥结构的不同量子态的信息携带效率如何, 忽略了测试轮在协议的参数估计部分的需要以及噪声的干扰. 我们研究针对各类分层密钥结构, 找到使得各层密钥率最高的方法, 若理想化密钥率高, 则它的密钥率也是在各类方法中最高的, 下面我们给出理想化密钥率的定义.

定义 4. 在一个分层密钥结构下, 在测量轮阶段只使用密钥轮测量 (即计算基测量) 且不考虑噪声干扰的情况下, 称在每一个时隙第 e 层产生密钥比特的数目为第 e 层的理想化密钥率, 记作 r_e.

针对第 3 节构造出的所有分层密钥结构, 我们将第 2.3 节中的方法 1 与方法 2 进行对比, 得到各分层密钥结构理想化密钥率最高的方案.

4.2 方法 1: 构造高维多粒子纠缠态实现 LQKD 的密钥率

针对表 1 中 3 用户分层密钥结构 $[3(3,2)]$, $[3(2,2)]$, 我们使用方法 1 可达到各层理想密钥率为 1, 对分层密钥结构 $[3(3,2,2)]$, 方法 1 各层理想化密钥率高于方法 2, 表 4 是 3 用户各密钥结构使用两种方法的理想化密钥率对比, 下面介绍具体实施方案. 使用方法 1 实现 3 用户分层密钥结构 $[3(3,2)]$ 的密钥分发具体步骤如下.

1) 量子态的构造: 对第 1 层 $\{U_1,U_2\}$, 我们构造出量子态 $|\Psi_1\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{U_1,U_2}+|11\rangle_{U_1,U_2}\right)$; 对第 2 层 $\{U_1,U_2,U_3\}$, 我们构造出量子态 $|\Psi_2\rangle=\frac{1}{\sqrt{2}}\left(|000\rangle_{U_1,U_2,U_3}+|111\rangle_{U_1,U_2,U_3}\right)$. 最后将 $|\Psi_1\rangle$ 和 $|\Psi_2\rangle$ 做张量积得到量子态 $|\Psi_{442}\rangle$:

$$\begin{aligned}|\Psi_{442}\rangle&=|\Psi_1\rangle\otimes|\Psi_2\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{U_1,U_2}+|11\rangle_{U_1,U_2}\right)\otimes\frac{1}{\sqrt{2}}\left(|000\rangle_{U_1,U_2,U_3}+|111\rangle_{U_1,U_2,U_3}\right)\\&=\frac{1}{2}\left(|0\rangle_{U_1}|0\rangle_{U_1}|0\rangle_{U_2}|0\rangle_{U_2}|0\rangle_{U_3}+|0\rangle_{U_1}|1\rangle_{U_1}|0\rangle_{U_2}|1\rangle_{U_2}|1\rangle_{U_3}+|1\rangle_{U_1}|0\rangle_{U_1}|1\rangle_{U_2}|0\rangle_{U_2}|0\rangle_{U_3}+|1\rangle_{U_1}|1\rangle_{U_1}|1\rangle_{U_2}|1\rangle_{U_2}|1\rangle_{U_3}\right).\end{aligned}$$

用 U_i^e 表示用户 U_i 在第 e 层所持有的量子比特, U_1 通过将二进制重写为数字的方法, 将其两个量子比特 U_1^1,U_1^2 编码到 $2^2=4$ 维的高维量子寄存器 R_1 (将 $|0\rangle|0\rangle$ 编码成 $|0\rangle$, $|0\rangle|1\rangle$ 编码成 $|1\rangle$, $|1\rangle|0\rangle$ 编码成 $|2\rangle$, 将 $|1\rangle|1\rangle$ 编码成 $|3\rangle$). U_2 也按照这个编码方式将其 2 个量子比特 U_1^1,U_1^2 编码到 $2^2=4$ 维的高维量子寄存器 R_2 中. U_3 将其 1 个量子比特 U_3^2 编码到 $2^1=2$ 维的高维量子寄存器 R_3 中. 产生的状态 $|\Psi_{442}\rangle$ 是寄存器 R_j 的 $2^2=4$ 个量子态的相等叠加:

$$|\Psi_{442}\rangle_{U_1U_2U_3}=\frac{1}{\sqrt{2}}\left(|000\rangle_{U_1U_2U_3}+|111\rangle_{U_1U_2U_3}+|220\rangle_{U_1U_2U_3}+|331\rangle_{U_1U_2U_3}\right),$$

其中, $|\Psi_{442}\rangle$ 表示该量子态的第 1, 2 个粒子在 4 维空间中, 第 3 个粒子在 3 维空间中. 下标 $U_1U_2U_3$ 表示 $|\Psi_{442}\rangle$ 的前两个粒子分发给 U_1 和 U_2, 第 3 个粒子分发给 U_3.

2) 测量: 用户 U_1、U_2 和 U_3 分别对量子态 $|\Psi_{442}\rangle$ 进行局域测量后, 3 个用户的测量结果会呈现出特有的相关性: U_1 和 U_2 的结果 $00,11,22,33$ 是完全相关的, 而 U_3 的测量结果 (0 或 1) 与 U_1 和 U_2 的测量结果是独立的.

3) 密钥生成: U_1 和 U_2 可以根据其测量结果对字符串 k_{123} 和 k_{12} 进行编码:

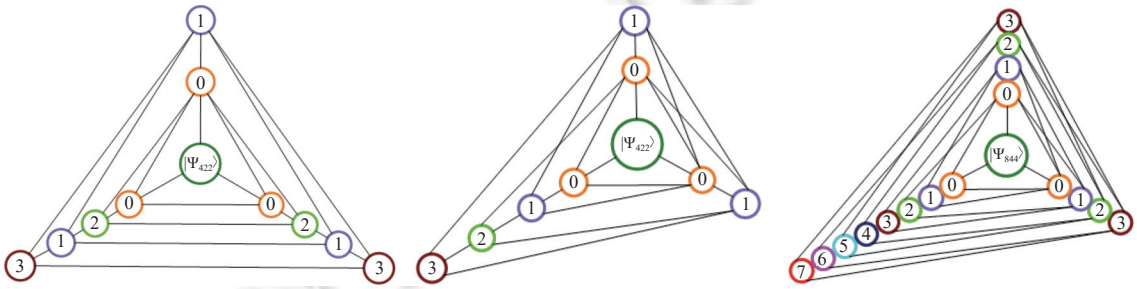
$$k_{123}=\begin{cases}0, & \text{当测量结果是0或2}\\1, & \text{当测量结果是1或3}\end{cases},\quad k_{12}=\begin{cases}0, & \text{当测量结果是0或1}\\1, & \text{当测量结果是2或3}\end{cases}.$$

通过编码我们可以得到 k_{123} 与 U_3 的测量结果完全相关, 由此达到 k_{123} 共享于 U_1、U_2 和 U_3, 又因为无论 U_3 的测量结果是 0 或 1 中的任意一个, k_{12} 的值是 0 或 1 的概率都是 1/2, 所以 k_{12} 与 U_3 的测量结果完全独立, k_{12} 只共享于 U_1、U_2 之间. 图 7(a) 表示使用量子态 $|\Psi_{442}\rangle$ 实现分层密钥结构 $[3(2,3)]$ 的示意图, 其中各层的理想化密钥率见表 4.

© 中国科学院软件研究所 http://www.jos.org.cn

表 4　3 用户量子网络中各分层密钥结构的理想化密钥率对比

分层密钥结构	理想化密钥率	密钥结构与实现方法			
		k_{12}	k_{13}	k_{23}	k_{123}
[3(3,2)]	方法1: 构造 $\|\Psi_{442}\rangle$	1	—	—	1
	方法2: 使用 $\|EPR_4\rangle$ 与 $\|GHZ_2\rangle$	1	—	—	1/2
[3(2,2)]	方法1: 构造 $\|\Psi_{422}\rangle$	1	1	—	—
	方法2: 使用 $\|EPR_2\rangle$ 与 $\|EPR_4\rangle$	1	1/2	—	—
[3(2,2,3)]	方法1: 构造 $\|\Psi_{844}\rangle$	1	1	—	1/2
	方法2: 使用 $\|EPR_4\rangle$ $\|EPR_8\rangle$ $\|GHZ_4\rangle$	1	1	—	1/3
[3(2,2,2)]	方法1: 构造 $\|\Psi_{444}\rangle$	1/2	1/2	1/2	—
	方法2: 使用 $\|EPR_4\rangle$ 与 $\|GHZ_4\rangle$	1/2	1/2	1	—
[3(2,2,2,3)]	方法1: 构造 $\|\Psi_{888}\rangle$	1/2	1/2	1/2	1/2
	方法2: 使用 $\|EPR_8\rangle$ 与 $\|GHZ_8\rangle$	1/2	1/2	1/2	3/2



(a) 使用量子态 $|\Psi_{422}\rangle$ 实现分层密钥结构 [3(3,2)]　(b) 使用量子态 $|\Psi_{422}\rangle$ 实现分层密钥结构 [3(2,2)]　(c) 使用量子态 $|\Psi_{422}\rangle$ 实现分层密钥结构 [3(3,2,2)]

图 7　使用高维多粒子纠缠实现 LQKD

4) 在对原始密钥进行参数估计和后处理之后, 可以使用密钥字符串对所有 3 个用户之间的消息进行一次性填充 (OTP) 加密[35].

在密钥结构 [3(2,2)] 下使用类似的方法可构造非对称高维多粒子 $|\Psi_{422}\rangle=\frac{1}{2}(|000\rangle+|101\rangle+|210\rangle+|311\rangle)$, 并采用如下编码方式 (各层理想密钥率见表 4):

$$k_{12}=\begin{cases}0, & \text{当测量结果是0或1}\\ 1, & \text{当测量结果是2或3}\end{cases},\quad k_{13}=\begin{cases}0, & \text{当测量结果是0或2}\\ 1, & \text{当测量结果是1或3}\end{cases}.$$

使用类似的方法构造非对称高维多粒子纠缠态 $|\Psi_{844}\rangle=\frac{1}{2\sqrt{2}}(|000\rangle+|101\rangle+|210\rangle+|311\rangle+|422\rangle+|523\rangle+|632\rangle+|733\rangle)$ 实现密钥结构 [3(3,2,2)], 采用的编码方式如下 (各层理想密钥率见表 4):

$$k_{12}=\begin{cases}0, & \text{当测量结果是0或1}\\ 1, & \text{当测量结果是2或3}\\ 2, & \text{当测量结果是4或5}\\ 3, & \text{当测量结果是6或7}\end{cases},\quad k_{13}=\begin{cases}0, & \text{当测量结果是0或2}\\ 1, & \text{当测量结果是1或3}\\ 2, & \text{当测量结果是4或6}\\ 3, & \text{当测量结果是5或7}\end{cases}.$$

图 7(a) 表示使用量子态 $|\Psi_{442}\rangle$ 实现分层密钥结构 [3(3,2)] 的示意图, 图 7(b) 表示使用量子态 $|\Psi_{422}\rangle$ 实现分层密钥结构 [3(2,2)] 的示意图, 图 7(c) 表示使用量子态 $|\Psi_{844}\rangle$ 实现分层密钥结构 [3(3,2,2)] 的示意图.

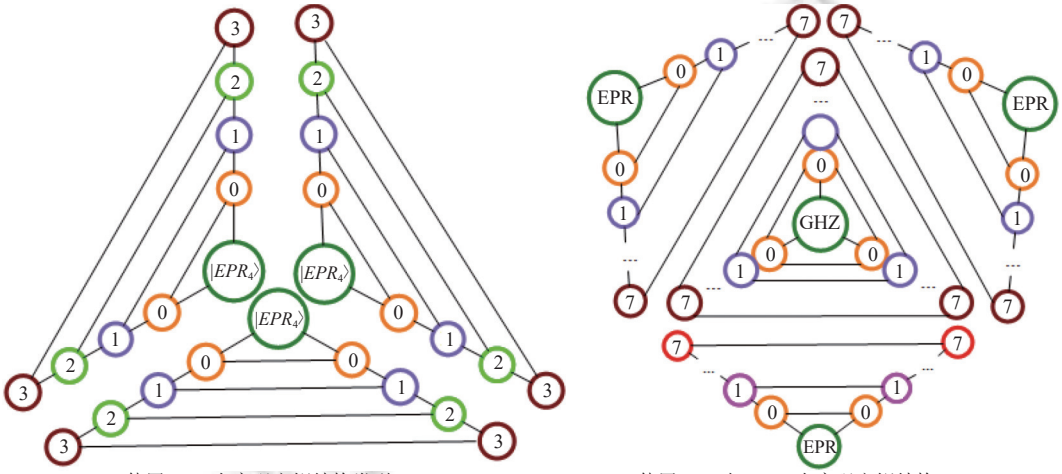
4.3　方法 2: 使用 EPR 与 GHZ 态实现 LQKD 的密钥率

针对表 1 中 3 用户分层密钥结构 [3(2,2,2)] 与 [3(2,2,2,3)], 使用方法 2 可使各层理想化密钥率高于方法 1, 针对表 2 与表 3 中 4、5 用户可分区分层密钥结构, 使用方法 2 可达到各层理想化密钥率是 1, 下面介绍实现的方法.

© 中国科学院软件研究所 http://www.jos.org.cn

4.3.1 实现方法

对密钥结构[3(2,2,2)], 使用方法 1 构造出的量子态为$|\Psi_{444}\rangle=\frac{1}{2\sqrt{2}}(|000\rangle+|011\rangle+|102\rangle+|113\rangle+|220\rangle+|231\rangle+|322\rangle+|333\rangle)$, 为了对比的公平性, 我们将$U_1$、$U_2$和$U_3$的局部维数固定为 4, 由于$U_1$和$U_2$可以执行四执系统测量[42], 他们可以使用给定的时隙使用$|EPR_4\rangle=\frac{1}{2}(|00\rangle+|11\rangle+|22\rangle+|33\rangle)$运行四执量子密钥分发协议, 在每个时隙可得到 2 个共享比特, 达到理想速率为 2. 所以当发送源分别以概率p、q、$1-p-q$发送 4 维 EPR 对$|EPR_4\rangle=\frac{1}{2}(|00\rangle+|11\rangle+|22\rangle+|33\rangle)$给$\{U_1,U_2\}$、$\{U_1,U_3\}$、$\{U_2,U_3\}$时, 各层理想化密钥率为: $[\{1,2\},2q],[\{1,3\},2p],[\{2,3\},2(1-p-q)]$, 图 8(a) 表示使用 EPR 态实现密钥结构类型[3(2,2,2)]的示意图.



(a) 使用 EPR 态实现密钥结构类型 [3(2,2,2)] (b) 使用 EPR 与 GHZ 态实现密钥结构 [3(2,2,2,3)]

图 8 使用 EPR 与 GHZ 态实现 LQKD 协议

在方法 2 中, 当$p=\frac{1}{4}$, $q=\frac{1}{4}$时, 各层理想化密钥率为$\left[\{1,2\},\frac{1}{2}\right],\left[\{1,3\},\frac{1}{2}\right],[\{2,3\},1]$, 由表 4 的对比可知方法 2 在$\{U_2,U_3\}$层的理想化密钥率大于方法 1, 故方法 2 更高效.

对密钥结构[3(2,2,2,3)], 使用方法 1 构造出的量子态为$|\Psi_{888}\rangle=\frac{1}{4}\{|000\rangle+|011\rangle+|102\rangle+|113\rangle+|220\rangle+|231\rangle+|322\rangle+|333\rangle+|444\rangle+|455\rangle+|546\rangle+|557\rangle+|664\rangle+|675\rangle+|766\rangle+|777\rangle\}$, 同样为了对比的公平性, 我们将$U_1$、$U_2$和$U_3$的局部维数固定为 8. 因此, 为了实现给定的密钥结构, 发送源分别以概率p、q、s发送 8 维 EPR 对$|EPR_8\rangle=\frac{1}{2\sqrt{2}}(|00\rangle+|11\rangle+|22\rangle+|33\rangle+|44\rangle+|55\rangle+|66\rangle+|77\rangle)$给$\{U_1,U_2\}$、$\{U_1,U_3\}$、$\{U_2,U_3\}$,并以概率$1-p-q-s$发送一个 8 维 3 粒子 GHZ 态$\left|GHZ_8^3\right\rangle=\frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle+|222\rangle+|333\rangle+|444\rangle+|555\rangle+|666\rangle+|777\rangle)$给$\{U_1,U_2,U_3\}$, 这使得$U_1$和$U_2$之间的二部密钥$k_{12}$的理想化密钥率$r_{12}=3p$. 在此设置中, U_1和U_3之间的k_{13}的理想化密钥率为$r_{13}=3q$, U_2和U_3之间k_{23}的理想化密钥率为$r_{23}=3s$, U_1、U_2和U_3之间k_{123}的理想化密钥率为$r_{123}=3(1-p-q-s)$, 图 8(b) 表示使用 EPR 与 GHZ 态实现密钥结构[3(2,2,2,3)]的示意图.

在密钥结构类型[3(2,2,2,3)]下, 用户使用方法 1、2 所处空间维数都是 8 维, 当$p=q=s=\frac{1}{6}$时, 方法 2 的各层理想密钥率为$\left[\{1,2\},\frac{1}{2}\right],\left[\{1,3\},\frac{1}{2}\right]\left[\{2,3\},\frac{1}{2}\right]\left[\{1,2,3\},\frac{3}{2}\right]$, 由表 4 对比可知, 方法 2 在$\{U_1,U_2,U_3\}$层中的理想密钥率高于方法 1, 故方法 2 更高效.

4.3.2 对 4、5 用户可分区分层密钥结构的实现

对 4、5 用户而言, 由于密钥结构层数可能过多, 而构造高维多粒子纠缠态的各粒子维数随密钥层数指数扩大, 所以要达到各层密钥速率是 1 的一般形式过于复杂. 下面我们证明在可分区分层密钥结构下, 不用构造复杂的

© 中国科学院软件研究所 http://www.jos.org.cn

不对称高维多粒子纠缠态就可使得各层理想化密钥率达到 1.

定理 1. 只有在可分区的连通密钥结构下, 使用 EPR 和 GHZ 态可达到每层平均速率为 1.

证明: 在 n 个用户的量子网络中, 假设该分层密钥结构具有 t 分区, 每个用户正好属于 t 个层, 因此有 $t_i = t$ $(i = 1,2,\ldots,n)$. 由于各分区 P_i 中的用户是互斥的, 故发送源可以同时发送 2^t 维 EPR 或 GHZ 态到分区 P_i 中的每一层, 导致每一层理想化密钥率为 t. 这正好消耗发送源 t 个时间间隔去遍历所有的分区 P_i, 故每层的平均速率是 1.

接下来我们证明在不可分区结构下, 使用 EPR 和 GHZ 态不能达到每层平均速率为 1. 我们可转化为证明其逆否命题. 为了在每层实现理想化密钥率为 1, 首先计算在每个时间间隙中需要产生的密钥数量. 每个用户 U_i 使用全维测量可在每一轮中产生总共 t_i 个密钥位. 为了充分实现信息携带的潜力, 用户 U_i 在一轮中需要在他的某一层共享一个 2^{t_i} 维 GHZ 态或 EPR 态. 这意味着用户 U_i 的所有相邻用户 $\{U_j\}$ 可得到 $t_j = t_i$, 否则他们既不能在 2^{t_i} 维的空间进行测量, 也不能在给定的回合中生成足够的密钥. 在每一轮中, 只有当他的每一层都属于一个分区, 每个用户才能在他的某一层中共享一个密钥, 达到理想化密钥率是 1. 所以该连通密钥结构是一个可分区结构. 除此之外, 每个用户都有 $t_j = t_i$, 为了获得每一层的速率 1, 每个用户正好需要 t_i 轮去遍历他所在的层. 这意味着密钥结构可分解为 t_i 个分区. 因此我们证明在不可分区的结构下, 使用 EPR 和 GHZ 态不能达到每层平均速率为 1.

定理 2. 在可分区的连通密钥结构下, 当每层用户的数量为 2 时, 单使用 EPR 态, 就可达每层平均速率为 1.

证明: 使用 EPR 实现每层理想密钥率是 1 需要限制每层的用户的数量为 2. 当每一层用户数量大于 2 时, 对某些用户来说需要共享两个 EPR 对, 如图 9 所示, 使用 EPR 态完成 6 用户之间密钥分发 (发送源分别将 5 个对 EPR 态分发给用户 $\{U_1,U_2\}$、$\{U_2,U_3\}$、$\{U_3,U_4\}$、$\{U_4,U_5\}$、$\{U_5,U_6\}$, 其中 U_1 和 U_6 分别与其相邻用户共享一个 EPR 对, 其余用户共享两个 EPR 对. 为共享多方密钥, 用户 U_1 在本地生成一个随机字符串, 并通过一次一密的方式将其发送给 U_2. 之后每个用户 U_i 在从用户 U_{i-1} 接收到密钥后, 将其秘密发送给用户 U_{i+1}, 最后所有用户共享新的密钥). 因此, 当某层用户的数量大于 2 时, 为达到每层平均速率为 1, 对一些用户来说每轮所需的比特数超过 t_i. 这表明, 即使密钥结构是可分区的, 且所有用户在每一轮中随机生成 t 比特双方密钥, 但有一些用户需要产生超过 t 比特的双方密钥, 以便他们在多用户层中一共可以共享 t_i 比特. 所以只有当每层用户的数量为 2 时, 单使用 EPR 态, 可达到每层平均速率为 1.

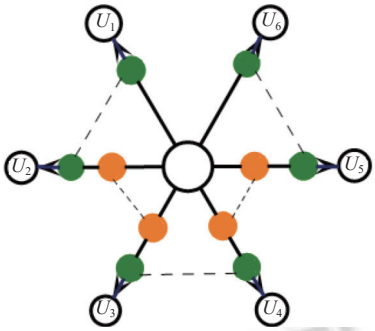
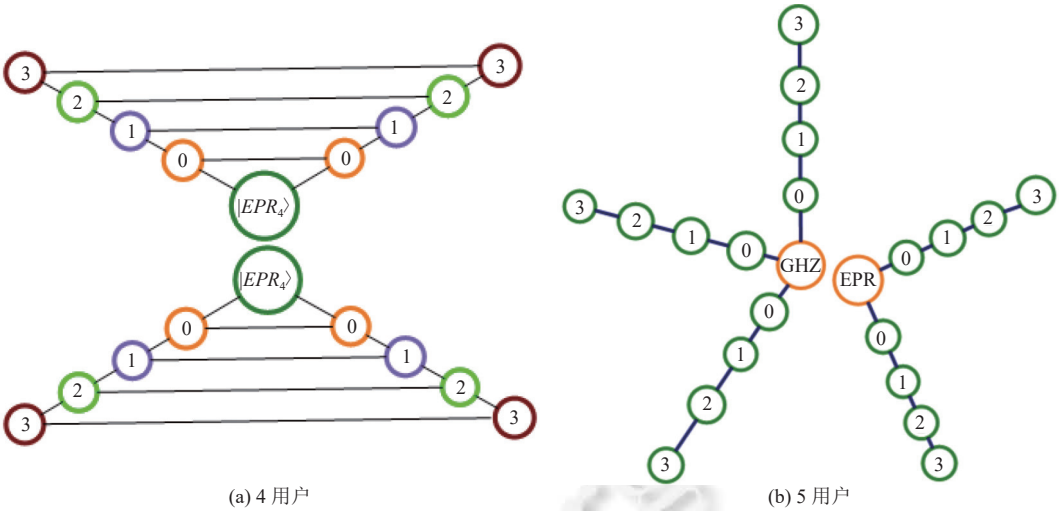


图 9 使用 EPR 对共享多方密钥所需信道数

对于 4 用户可分区分层密钥结构 $[4(2,2)_2]$, 由于各分区中的用户互斥, 故 4 维的 EPR 对可以同时分布到这两个分区, 如果每个分发轮发生的概率 $\frac{1}{2}$, 那么每一层的平均密钥速率是 1, 图 10(a) 为分区的量子态分布图. 同理可分析 3 分区分离结构 $[4(2,2)_3]$, 每层人数也只有 2 人, 由定理 2 可知, 仅使用 EPR 态就可对此密钥结构以理想速率 1 进行实现, 8 维 EPR 态并行分布到这 3 个分区, 如果每个分发轮发生的概率 $\frac{1}{3}$, 那么每一层的平均密钥速率是 1.

对 5 用户可分区分层密钥结构 $[5(3,2)_2]$, 此结构有两个 3 用户层, 两个 2 用户层, 由定理 1、2 知, 使用 GHZ 与 EPR 态可对此密钥结构以理想速率 1 进行实现. 由于每个分区用户集是互斥的, 所以一个 4 维的 3 粒子 GHZ 态与 4 维 EPR 态可以并行分布到每个分区, 如图 10(b) 所示. 如果每个分发轮发生的概率 $\frac{1}{2}$, 那么每一层的平均密钥速率是 1. 更多分区的 5 用户密钥结构分析与二分区类似, 每个分区的量子态分发与图 10(b) 类似.

© 中国科学院软件研究所 http://www.jos.org.cn



(a) 4 用户 (b) 5 用户

图 10 使用 EPR 与 GHZ 态实现 4、5 用户可分区分层密钥结构

注意: 为了达到每层密钥速率是 1, EPR 态或 GHZ 态的维数 L 与分区的个数 M 密切相关, $L=2^M$.

5 结 论

本文在同构意义下给出 3 用户的分层密钥结构, 并给出 4、5 用户的可分区分层密钥结构. 实现这些分层密钥结构类型的方法有两种, 方法 1 是构造非对称高维多粒子纠缠态来实现分层密钥结构, 方法 2 是使用 EPR 与 GHZ 态来实现分层密钥结构. 针对各类分层密钥结构, 我们通过对比方法 1 和方法 2 的理想化密钥率, 得到在分层密钥结构类型 $[3(2,3)]$, $[3(2,2)]$, $[3(2,2,3)]$ 下, 使用方法 1 的理想化密钥率高于方法 2, 其中方法 1 可使得结构 $[3(2,3)]$ 与 $[3(2,2)]$ 的各层理想化密钥率达 1, 且结构 $[3(2,2,3)]$ 中的 3 用户层的理想化密钥率 ($k^1_{123}=\frac{1}{2}$) 高于方法 2 ($k^2_{123}=\frac{1}{2}$); 在分层密钥结构类型 $[3(2,2,2)]$, $[3(2,2,2,3)]$ 下, 使用方法 2 的理想化密钥率高于方法 1, 其中在结构 $[3(2,2,2)]$ 下, 方法 2 在 $\{U_2,U_3\}$ 层的理想化密钥率 ($k^2_{23}=1$) 高于方法 1 ($k^1_{23}=\frac{1}{2}$), 在结构 $[3(2,2,2,3)]$ 下, 方法 2 在 $\{U_1,U_2,U_3\}$ 层的理想化密钥率 ($k^2_{123}=\frac{3}{2}$) 高于方法 1 ($k^1_{123}=\frac{1}{2}$). 最后我们证明在可分区分层密钥结构下, 仅使用 EPR 和 GHZ 就能实现每层的密钥达到 1, 并给出 4、5 用户可分区分层密钥结构的具体实现方案, 对 4 用户可分区分层密钥结构来说, 仅使用 EPR 态就可使得每层平均理想密钥速率达到 1, 而 5 用户的可分区分层密钥结构需要 EPR 态与 GHZ 态共同实现协议, 使得每层平均理想密钥速率达到 1.

如果高维多粒子纠缠态的产生变得更加可靠, 这就有可能大大简化网络体系结构, 因为单一源就足以完成各种任务. 我们明确地展示了高维多粒子纠缠在量子密钥分发方面的应用, 也希望可以鼓励物理光学实验室以可控方式和适当速率可靠地制备高维多粒子纠缠源, 在制备高维多粒子纠缠做出更大突破. 这种不对称高维多粒子纠缠态成为量子纠缠实验研究的一个新方向, 也为今后复杂的多层次量子网络的研究提供了一种新思路.

References:

[1] Shannon CE. Communication theory of secrecy systems. The Bell System Technical Journal, 1949, 28(4): 656–715. [doi: 10.1002/j.1538-7305.1949.tb00928.x]

[2] Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature, 1982, 299(5886): 802–803. [doi: 10.1038/299802a0]

[3] Coffman V, Kundu J, Wootters WK. Distributed entanglement. Physical Review A, 2000, 61(5): 052306. [doi: 10.1103/PhysRevA.61.052306]

[4] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Reviews of Modern Physics, 2002, 74(1): 145–195. [doi: 10.1103/revmodphys.74.145]

[5] Gobby C, Yuan ZL, Shields AJ. Quantum key distribution over 122 km of standard telecom fiber. Applied Physics Letters, 2004, 84(19):

© 中国科学院软件研究所 http://www.jos.org.cn

3762–3764. [doi: 10.1063/1.1738173]

[6] Wang XB, Yu ZW, Hu XL. Twin-field quantum key distribution with large misalignment error. Physical Review A, 2018, 98(6): 062323. [doi: 10.1103/PhysRevA.98.062323]

[7] Liu CJ, Zhu CH, Liu X, Nie M, Yang H, Pei CX. Multicarrier multiplexing continuous-variable quantum key distribution at Terahertz bands under indoor environment and in inter-satellite links communication. IEEE Photonics Journal, 2021, 13(4): 7600113. [doi: 10.1109/JPHOT.2021.3098717]

[8] Bennett CH, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. Theoretical Computer Science, 2014, 560(Pt 1): 7–11. [doi: 10.1016/j.tcs.2014.05.025]

[9] Ekert AK. Quantum cryptography based on Bell's theorem. Physical Review Letters, 1991, 67(6): 661–663. [doi: 10.1103/PhysRevLett.67.661]

[10] Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters, 1992, 68(21): 3121–3124. [doi: 10.1103/PhysRevLett.68.3121]

[11] Bruß D. Optimal eavesdropping in quantum cryptography with six states. Physical Review Letters, 1998, 81(14): 3018–3021. [doi: 10.1103/PhysRevLett.81.3018]

[12] Daoud M, Ez-Zahraouy H. Three-dimensional quantum key distribution in the presence of severeral eavesdroppers. Physica Scripta, 2011, 84(4): 045018. [doi: 10.1088/0031-8949/84/04/045018]

[13] Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. Physical Review Letters, 2012, 108(13): 130503. [doi: 10.1103/PhysRevLett.108.130503]

[14] Vazirani U, Vidick T. Fully device-independent quantum key distribution. Physical Review Letters, 2014, 113(14): 140501. [doi: 10.1103/PhysRevLett.113.140501]

[15] Cao Y, Li YH, Yang KX, Jiang YF, Li SL, Hu XL, Abulizi M, Li CL, Zhang WJ, Sun QC, Liu WY, Jiang X, Liao SK, Ren JG, Li H, You LX, Wang Z, Yin J, Lu CY, Wang XB, Zhang Q, Peng CZ, Pan JW. Long-distance free-space measurement-device-independent quantum key distribution. Physical Review Letters, 2020, 125(26): 260503. [doi: 10.1103/PhysRevLett.125.260503]

[16] Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283(5410): 2050–2056. [doi: 10.1126/science.283.5410.2050]

[17] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters, 2000, 85(2): 441–444. [doi: 10.1103/PhysRevLett.85.441]

[18] Mayers D. Unconditional security in quantum cryptography. Journal of the ACM, 2001, 48(3): 351–406. [doi: 10.1145/382780.382781]

[19] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Reviews of Modern Physics, 2009, 81(3): 1301–1350. [doi: 10.1103/revmodphys.81.1301]

[20] Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de finetti reduction. Physical Review Letters, 2017, 118(20): 200501. [doi: 10.1103/PhysRevLett.118.200501]

[21] Phoenix SJD, Barnett SM, Townsend PD, Blow KJ. Multi-user quantum cryptography on optical networks. Journal of Modern Optics, 1995, 42(6): 1155–1163. [doi: 10.1080/09500349514551001]

[22] Guo Y, Shi RH, Zeng GH. Secure networking quantum key distribution schemes with Greenberger-Horne-Zeilinger states. Physica Scripta, 2010, 81(4): 045006. [doi: 10.1088/0031-8949/81/04/045006]

[23] Li CY, Zhou HY, Wang Y, Deng GF. Secure quantum key distribution network with Bell states and local unitary operations. Chinese Physics Letters, 2005, 22(5): 1049–1052. [doi: 10.1088/0256-307X/22/5/006]

[24] Xue P, Li CF, Guo GC. Conditional efficient multiuser quantum cryptography network. Physical Review A, 2002, 65(2): 022317. [doi: 10.1103/PhysRevA.65.022317]

[25] Gao F, Guo FZ, Wen QY, Zhu FC. On the information-splitting essence of two types of quantum key distribution protocols. Physics Letters A, 2006, 355(3): 172–175. [doi: 10.1016/j.physleta.2006.02.027]

[26] Chen K, Lo HK. Conference key agreement and quantum sharing of classical secrets with noisy GHZ states. In: Proc. of the 2005 Int'l Symp. on Information Theory. Adelaide: IEEE, 2005. 1607–1611. [doi: 10.1109/isit.2005.1523616]

[27] Fu Y, Yin HL, Chen TY, Chen ZB. Long-distance measurement-device-independent multiparty quantum communication. Physical Review Letters, 2015, 114(9): 090501. [doi: 10.1103/PhysRevLett.114.090501]

[28] Masanes L, Pironio S, Acín A. Secure device-independent quantum key distribution with causally independent measurement devices. Nature Communications, 2011, 2: 238. [doi: 10.1038/ncomms1244]

[29] Pironio S, Acín A, Brunner N, Gisin H, Massar S, Scarani V. Device-independent quantum key distribution secure against collective attacks. New Journal of Physics, 2009, 11(4): 045021. [doi: 10.1088/1367-2630/11/4/045021]

© 中国科学院软件研究所 http://www.jos.org.cn

[30] Krenn M, Malik M, Erhard M, Zeilinger A. Orbital angular momentum of photons and the entanglement of Laguerre-Gaussian modes. Philosophical Trans. of the Royal Society A: Mathematical, Physical, and Engineering Sciences, 2017, 375(2087): 20150442. [doi: 10.1098/rsta.2015.0442]

[31] Mafu M, Dudley A, Goyal S, Giovannini D, Mclaren M, Padgett MJ, Konrad T, Petruccione F, Lütkenhaus N, Forbes A. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. Physical Review A, 2013, 88(3): 032305. [doi: 10.1103/PhysRevA.88.032305]

[32] Mirhosseini M, Magaña-Loaiza OS, O'Sullivan MN, Rodenburg B, Malik M, Lavery MPJ, Padgett MJ, Gauthier DJ, Boyd RW. High-dimensional quantum cryptography with twisted light. New Journal of Physics, 2015, 17(3): 033033. [doi: 10.1088/1367-2630/17/3/033033]

[33] Vértesi T, Pironio S, Brunner N. Closing the detection loophole in Bell experiments using qudits. Physical Review Letters, 2010, 104(6): 060401. [doi: 10.1103/PhysRevLett.104.060401]

[34] Huber M, Pawłowski M. Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement. Physical Review A, 2013, 88(3): 032309. [doi: 10.1103/PhysRevA.88.032309]

[35] Epping M, Kampermann H, Macchiavello C, Bruß D. Multi-partite entanglement can speed up quantum key distribution in networks. New Journal of Physics, 2017, 19(9): 093012. [doi: 10.1088/1367-2630/aa8487]

[36] Lanyon BP, Zwerger M, Jurcevic P, Hempel C, Dür W, Briegel HJ , Blatt R, Roos CF. Experimental violation of multipartite Bell inequalities with trapped ions. Physical Review Letters, 2014, 112(10): 100403. [doi: 10.1103/PhysRevLett.112.100403]

[37] Yao XC, Wang TX, Xu P, Lu H, Pan GS, Bao XH, Peng CZ, Lu CY, Chen YA, Pan JW. Observation of eight-photon entanglement. Nature Photonics, 2012, 6(4): 225–228. [doi: 10.1038/nphoton.2011.354]

[38] Huber M, De Vicente JI. Structure of multidimensional entanglement in multipartite systems. Physical Review Letters, 2013, 110(3): 030501. [doi: 10.1103/PhysRevLett.110.030501]

[39] Krenn M, Malik M, Fickler R, Lapkiewicz R, Zeilinger A. Automated search for new quantum experiments. Physical Review Letters, 2016, 116(9): 090405. [doi: 10.1103/PhysRevLett.116.090405]

[40] Hiesmayr BC, De Dood MJA, Löffler W. Observation of four-photon orbital angular momentum entanglement. Physical Review Letters, 2016, 116(7): 073601. [doi: 10.1103/PhysRevLett.116.073601]

[41] Malik M, Erhard M, Huber M, Krenn M, Fickler R, Zeilinger A. Multi-photon entanglement in high dimensions. Nature Photonics, 2016, 10(4): 248–252. [doi: 10.1038/nphoton.2016.12]

[42] Pivoluska M, Huber M, Malik M. Layered quantum key distribution. Physical Review A, 2018, 97(3): 032312. [doi: 10.1103/PhysRevA.97.032312]

[43] Liu BH, Hu XM, Chen JS, Huang YF, Han YJ, Li CF, Guo GC, Cabello A. Nonlocality from local contextuality. Physical Review Letters, 2016, 117: 220402. [doi: 10.1103/PhysRevLett.117.220402]

[44] Diestel R. Graph Theory. 5th ed., Berlin: Springer, 2017. 2–27. [doi: 10.1007/978-3-662-53622-3]

[45] McKay BD. Graph isomorphism. In: Kao MY, ed. Encyclopedia of Algorithms. New York: Springer, 2016. 875–879. [doi: 10.1007/978-1-4939-2864-4_172]

[46] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R, Grangier P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. Journal of Physics B: Atomic, Molecular, and Optical Physics, 2009, 42(11): 114014. [doi: 10.1088/0953-4075/42/11/114014]

闫晨红(1997－), 女, 硕士生, 主要研究领域为量子密码学.

刘璐(1996－), 女, 硕士生, 主要研究领域为量子密码学.

李志慧(1966－), 女, 教授, 博士生导师, 主要研究领域为量子密码学, 密码学.

韩召伟(1981－), 男, 副教授, 主要研究领域为量子密码学, 量子计算, 量子逻辑.

© 中国科学院软件研究所 http://www.jos.org.cn