Modern Physics 现代物理, 2017, 7(6), 257-268
Published Online November 2017 in Hans. http://www.hanspub.org/journal/mp
https://doi.org/10.12677/mp.2017.76030

Hans汉斯

Security Analysis on Measurement-Device-Independent Quantum Key Distribution Protocol

Hongxin Li[1,2], Xiangbin Wang[1], Xin Liu[1], Yu Han[1], Bao Yan[1], Wei Wang[1]

[1]Luoyang Campus, Strategic Support Force Information Engineering University, Luoyang Henan
[2]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Henan
Email: lihongxin830@163.com

Received: Nov. 6th, 2017; accepted: Nov. 20th, 2017; published: Nov. 27th, 2017

Abstract

Quantum key distribution (QKD) has been paid much attention because of its theoretical unconditional security. However, in the actual system, QKD will be vulnerable to Quantum hackers because of non-perfection of equipment. The proposal of the measurement device independent (MDI) QKD provide a good solution to this problem. In this paper, we firstly introduce the latest research progress and implementation principles of the MDI-QKD protocol. And then, we summarize the advantages and disadvantages of the protocol in the practical application. Based on the analysis of the MDI-QKD improvement protocol, our research is mainly focused on the method of lifting scheme secure key generation rate and theoretical proof.

Keywords

Quantum Key Distribution, Measurement Device Independent, Side-Channel Attack, HSPS

测量设备无关量子密钥分发方案安全性研究

李宏欣[1,2]，王相宾[1]，刘　欣[1]，韩　宇[1]，闫　宝[12]，王　伟[1]

[1]战略支援部队信息工程大学洛阳校区，河南 洛阳
[2]数学工程与先进计算国家重点实验室，河南 郑州
Email: lihongxin830@163.com

收稿日期：2017年11月6日；录用日期：2017年11月20日；发布日期：2017年11月27日

文章引用：李宏欣，王相宾，刘欣，韩宇，闫宝，王伟. 测量设备无关量子密钥分发方案安全性研究[J]. 现代物理, 2017, 7(6): 257-268. DOI: 10.12677/mp.2017.76030

摘 要

量子密钥分发(quantum key distribution，简称QKD)因其具有理论上的无条件安全性而备受关注，但是在实际系统中，QKD会由于设备的非完美性而易受到量子黑客的攻击。测量设备无关(measurement device independent，简称MDI) QKD方案的提出，很好地解决了这一问题。本文首先介绍MDI-QKD协议的最新研究进展和实现原理，总结归纳了协议在实际应用中的优越性与不足，在分析MDI-QKD改进协议的基础上，重点研究提升方案安全密钥生成率的方法并进行理论证明。

关键词

量子密钥分发，测量设备无关，侧信道攻击，标记单光子源

1. 引言

QKD 是量子通信技术中实用化程度较高的应用之一，因其理论上的无条件安全性一直备受关注。1984 年 IBM 公司的 Charles H.Bennett 和蒙特利尔大学的 Gilles Brassard Bennett 提出第一个 QKD 协议即 BB84 协议，由于简单高效而被广泛使用。然而，在实际使用过程中，由于设备的不完美性，量子密钥系统还存在着较多的漏洞。被称为量子黑客的攻击者可以针对这些漏洞，实施诸如分束攻击、时移攻击、致盲攻击等来获取密钥信息。而在这中间，探测器遭到了最为频繁的攻击。

为解决上述问题，2006 年西班牙科学家 Antonio Acin 等人提出了设备无关(device indepenent，简称 DI) QKD 的思想。但 DI-QKD 要求接近一致的探测效率，其密钥生成率也较低，并不实用。2012 年加拿大多伦多大学的 Hoi-Kwong Lo 小组提出了一个创新的方案——MDI-QKD [1]。在 MDI-QKD 方案中，测量设备仅是用来在 Alice 和 Bob 间传递纠缠的，可以被当作是一个真正的黑盒子，进而使得 MDI-QKD 对所有针对探测系统的攻击免疫。

为了增加 MDI-QKD 协议在实际应用中的安全密钥传输距离并提高安全密钥生成率，国内外许多研究机构也不断对其进行改进。2013 年清华大学的王向斌小组提出了对 MDI-QKD 协议光源的改进方法[2]，在该方案中使用标记单光子源(HSPS)代替弱相干光源。同时各研究小组也在进一步探究在实际中是否存在一种最优的光源可以代替理想单光子光源。2013 年卡尔加里大学的概念性证明实验证明了 MDI-QKD 协议的非对称的方案[3]，2014 年空军工程大学信息与导航学院的东晨、赵尚弘和赵卫虎等[4]也对此问题进行了研究并得出结论说明 MDI-QKD 可应用于非对称信道。2014 年南京邮电大学的朱峰、王琴等人对当标记单光子源服从热分布时的 MDI-QKD 的优越性进行了证明。2014 年加拿大卡尔加里大学的 V.R.R. Valivarthi 等人提出了对 MDI-QKD 中探测器的改进[5]，他使用 id210 探测器代替目前广泛使用的 id200 探测器，进而提高探测效率。2014 年中科大的 Tang Y L 等人提出在 MDI-QKD 中使用 SNSPDs(超导纳米线单光子探测器)来降低普通探测器的暗记数，进而提高探测效率进而提高密钥生成率和安全密钥传输距离[6]。2014 年加拿大多伦多大学的 Lo 小组提出了在通信双方之间添加一个纠缠光子源的方法来提高 MDI-QKD 密钥传输距离[7]。2014 年中国科学技术大学的潘建伟小组设计了一个改进的 MDI-QKD 协议，并已经提高到了一个 75 MHz 的时钟率并将安全密钥传输距离提高到了 200 km [6]，该结果对于较为依赖

MDI-QKD 安全性的量子网络具有重要意义。

2015 年加拿大卡尔加里大学的量子科学技术研究所的 Raju Valivarthi 等人提出了更好的反馈机制，用以消除信道传输上的不足[8]。2015 年，南京邮电大学毛钱萍等提出了基于波分复用技术的 MDI-QKD 协议，在不增加系统传输设备的前提下，提高了系统的密钥生成率[9]。2016 年，中国科学技术大学的尹华磊等人使用最优化的四强度诱骗态方法进行了长距离 MDI-QDK 实验，利用超低损耗光纤的安全传输距离达到 404 km，创造了新的安全传输记录[10]。2016 年，空军工程大学的薛阳等人提出了一种基于修正相干态光源的 MDI-QKD 方案，相较于使用 HSPS 光源的系统，传输距离提高了 9% [11]。2017 年，空军工程大学的朱卓丹等人提出了一种基于预报相干光子对的 MDI-QKD 改进方案，降低了长距离量子密钥分发中由暗计数引起的误码率[12]。

近年来，研究人员也陆续提出了一些 MDI-QKD 的应用方案。2015 年，空军工程大学姬一鸣等提出了一种基于 MDI-QKD 的多用户接入网络，实现了量子密钥的安全共享[13]。同年，空军工程大学孙颖等人提出基于量子存储和纠缠光源的 MDI-QKD 网络，该方案弥补了直接预报量子存储方案的不足，通过分复用器和快速光开关实现单通道多用户的量子密钥分配网络[14]。2017 年，英国 Vigo 大学 Roberts 等人实现了一种新型的量子密钥分发方案，可以在常规 QKD 与 MDI-QKD 之间进行实时切换，同时提高了数字签名的效率[15]。2017 年，中国科学技术大学王超等人提出了 RFI-MDI-QKD 方案，可以运用于各种复杂的环境中，显著增强了测量设备无关量子密钥分发系统的安全性，在现实生活中有较好的前瞻性应用[16]。

本文首先介绍了 MDI-QKD 协议的相关内容，分析其优势与不足，并介绍相关的改进方案。最后，我们给出了一种使用 HPPS 光源的方案的改进，并说明何时能得到更高的秘钥生成率。

2. MDI-QKD 协议概述

2012 年，Lo 小组提出了 MDI-QKD 方案在抵御探测器的侧信道攻击方面取得了较好的成果。在 MDI-QKD 协议中，Alice 和 Bob 准备任意 BB84 偏振态的随机弱相干脉冲(weak coherent pulses，简称 WCPs)，并且将它们发送给一个处在中间位置的不可信的第三方 Charlie，Charlie 为了将接收到的信号变成 Bell 态会执行一个 Bell 态测量。Alice 和 Bob 可以应用诱骗态技术来估计增益和量子比特错误率(quantum bit error rate，简称 QBER)。

下面，我们将对 MDI-QKD 的具体协议流程、安全性分析、优越性和不足等进行分析。

2.1. MDI-QKD 协议流程

下面将对 MDI-QKD 协议的具体协议流程做出说明：

1) Alice 和 Bob 独立地制备弱相干光源(WCPs)。Alice 和 Bob 通过利用偏振调制器(Pol-M)来制备不同的 BB84 状态的随机 WCPs 并通过使用强度调制器(Decoy-IM)来生成诱骗态。完成以上操作后，Alice 和 Bob 将会通过信道独立地将自己的信号发送给一个处于中间位置的不可信第三方 Charlie。

2) 在测量过程中，Alice 和 Bob 发送的信号脉冲进入到一个 50:50 的分束器(BS)中进行干涉，之后分别进入两个偏振分束器(PBS)中将输入光子投射成水平的(H)或垂直的(V)偏振态。

3) Charlie 将执行一个 Bell 态测量用来将接收到的信号变成 Bell 态，该端的四个光子探测器用来探测结果。Bell 状态测量是否成功与两个探测器的测量结果有关。当测量设备不可信时，通过此过程 Alice 和 Bob 能够很好的屏蔽窃听者。他定义 Ψ^+ 为 D1H、D1V 或 D2H、D2V 同时响应的测量结果，其中 $\left|\Psi^+\right\rangle$ 可表示为：$\left|\Psi^+\right\rangle=\frac{1}{\sqrt{2}}\left(\left|HV\right\rangle+\left|VH\right\rangle\right)$；$\Psi^-$ 为 D1H、D2V 或 D2H、D1V 同时响应的测量结果，其中 $\left|\Psi^-\right\rangle$

可表示为：$\left|\Psi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|HV\right\rangle-\left|VH\right\rangle\right)$。Charlie 认为符合 Ψ^{+} 和 Ψ^{-} 的事件为成功的事件，其他均为失败的事件。待传输结束后，Charlie 广播他的测量结果。(如图 1 所示，D1H、D1V、D2H、D2V 为 Charlie 端的四个探测器)。

4) Alice 和 Bob 所需要的测量结果是 Ψ^{-}，其他的情况他们都视为是不需要的结果。如果 Alice 和 Bob 得到的结果为 Ψ^{-}，此次数据会被他们暂时保留，否则丢弃。通过经典信道下对比双方所选择的基，如果双方所选择的基相同他们将会保留此次数据。之后 Alice 和 Bob 其中的一个会任意选择一个比特进行翻转，当以上操作完成之后，这组数据就被称为原始密钥。当 Alice 和 Bob 得到了足够的原始密钥后，最终的安全密钥是用选择直线基时得到的密钥生成的，而选择对角基时得到的原始密钥则会作为测试比特用来检测错误概率，如果错误概率高于 QBER 门限值，说明在此次通信过程中存在窃听，那么就放弃此次结果，否则就在公共信道中进行纠错和私钥放大的过程进而提取安全的秘密密钥[17]。Alice 和 Bob 比特翻转选择情况如表 1 所示。

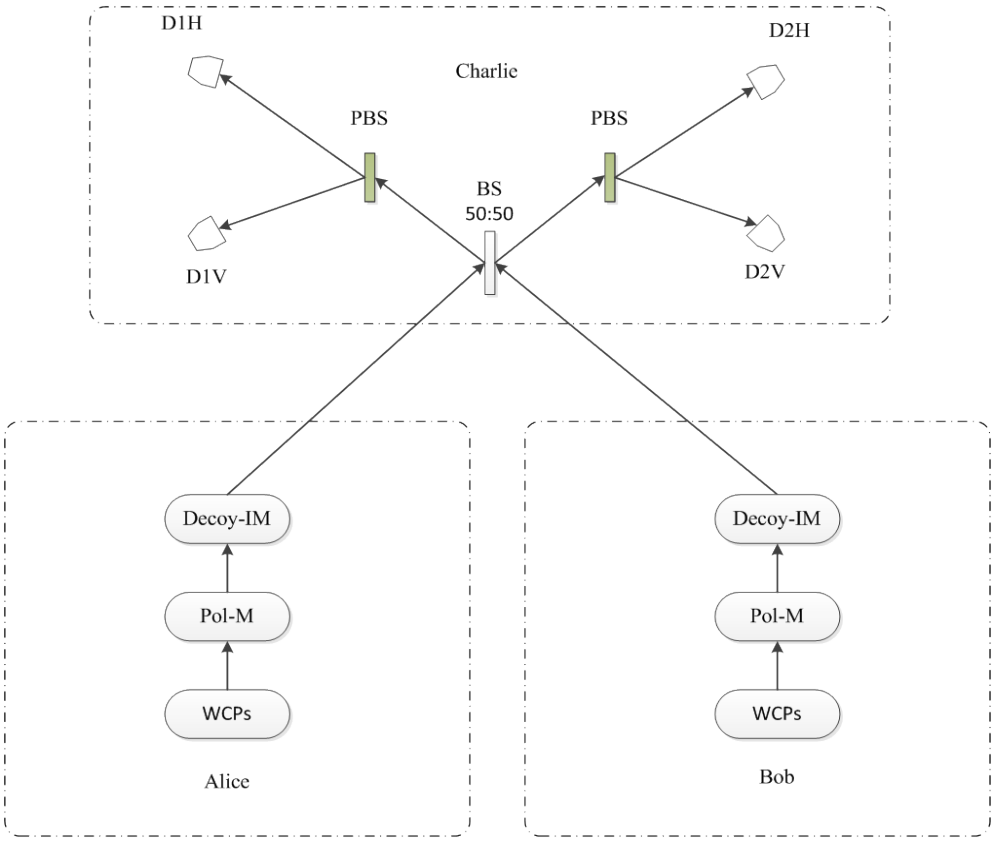

Figure 1. Progress of MDI-QKD protocol
图 1. MDI-QKD 协议流程图

Table 1. Bit flip choices of Alice and Bob
表 1. Alice 和 Bob 比特翻转选择

Alice 和 Bob	Ψ^{-}	Ψ^{+}
直线基	比特翻转	比特翻转
对角基	比特翻转	——

2.2. MDI-QKD 协议安全性分析

在 MDI-QKD 中，直线基(rectilinear basis，简称 *rect*)用作密钥生成基，而对角基(diagonal basis，简称 *diag*)仅用于测试。下面我们将对 MDI-QKD 协议的安全密钥生成率进行分析：

当 QKD 系统使用非完美器件时，其安全性已被 Gottesman，Lo，Lütkenhaus 和 Preskill 等四人(GLLP) [18]证明，Hwang 于 2003 年首次提出了诱骗态的思想[19]。结合 GLLP 协议和诱骗态的思想，我们可以得到密钥生成率公式：

$$R = Q_{rect}^{1,1}\left[1 - H\left(e_{diag}^{1,1}\right)\right] - Q_{rect} f\left(E_{rect}\right) H\left(E_{rect}\right)$$

在 MDI-QKD 中使用弱相干光源(WCPs)代替理想的单光子源，弱相干光源服从泊松分布，其分布形式如下：

$$P_n\left(x\right) = e^{-x}\frac{x^n}{n!}$$

首先考虑增益 $Q_{rect}^{i,j}$：

$$Q_{rect}^{i,j} = \sum_{n=0}^{\infty} e^{-\mu_i}\frac{\mu_i^n}{n!} Y_n^{j;rect},$$

其中

$$Y_{n;rect}^{j} = \sum_{m=0}^{\infty} e^{-\mu_j}\frac{\mu_j^m}{m!} Y_{rect}^{n,m}.$$

i 和 j 分别代表 Alice 和 Bob 所选择的不同的诱骗态。

然后考虑误码率 QBER $E_{rect}^{i,j}$：

$$Q_{rect}^{i,j} E_{rect}^{i,j} = \sum_{n=0}^{\infty} e^{-\mu_i}\frac{\mu_i^n}{n!} W_{n;rect}^{j},$$

其中

$$W_{n;rect}^{j} = \sum_{m=0}^{\infty} e^{-\mu_j}\frac{\mu_j^m}{m!} Y_{rect}^{n,m} e_{rect}^{n,m}.$$

因而，当 Alice 和 Bob 发送单光子即 $m=1, n=1$ 时，可以得到：

$$Q_{rect}^{1,1} = \mu_A \mu_B e^{-(\mu_A+\mu_B)} Y_{rect}^{1,1}$$

在实验中，增益是可以由实验测得的，因而由以上公式可以得出，为了提高 MDI-QKD 系统的密钥生成率，我们只需提高单光子生成率 $Y_{rect}^{1,1}$ 和降低单光子误码率 $e_{diag}^{1,1}$。

理想的 QKD 系统具有信息论安全性。然而，QKD 系统的非完美性能被窃听者利用进而在未经合法使用者 Alice 和 Bob 同意的情况下获得密钥信息。其中比较受关注的是单光子探测器，因为单光子探测器易受到侧信道攻击。

MDI-QKD 协议的安全性证明基于 EPR (Einstein, Podolsy, Rosen) QKD 协议[20]和诱骗态的方法。MDI-QKD 协议对于针对探测器攻击具有免疫性，例如通过远距离控制，Charlie 端探测器响应仅允许窃听者知道 Alice 和 Bob 已经建立的相关的秘密密钥比特，但是不泄露他们的比特值。因此，通过利用探测器弱点而实施的所有的侧信道攻击将会被消除，MDI-QKD 协议能够很好的执行。

2.3. MDI-QKD 协议的优越性与不足

2.3.1. MDI-QKD 协议的优越性

MDI-QKD 协议在实际应用中，相比于其他的 QKD 协议在安全密钥生成率和密钥安全传输距离方面具有明显的优势[1] [21]。

1) 与使用 WCP 的传统的 QKD 方案相比：

① MDI-QKD 具有可以弱化所有的探测器侧信道攻击的优势，因而其具有非常好的安全性。

② 它也有能力将 QKD 方案中所使用的常见的激光二极管的传输距离扩展到两倍。

③ 它比标准的安全性证明如 ILM 和 GLLP 具有更好的安全性的优点且它的思想也可以实施于低探测效率的标准探测器和高噪信道中(能够容忍超过 40 dB 的光学损失)，进而可以提高密钥传输的距离。

2) 与 DI-QKD 相比

① MDI-QKD 探测效率高并且在高噪声信道中也能安全地生成密钥。

② MDI-QKD 不依赖于任何理想的设备并在抵御探测器侧信道攻击方面取得了较好的结果。

③ 它还具有相当高的密钥生成率，它的密钥生成率高于标准安全性证明中使用纠缠对时的生成率，且在数量级上高于全设备无关 QKD 的密钥生成率。

MDI-QKD 协议的思想可以在以下几个方面进行推广[1]：

1) 它也能应用到 Alice 和 Bob 使用纠缠光子对作为光源的情况。

2) 即使 Alice 和 Bob 的制备过程并不完美，它也可以正确实现。

3) 在实际的应用中所需要的诱骗态的数量是有限的。在这一点上它与在实验中广泛使用的标准的有限诱骗态 QKD 协议相似。

4) MDI-QKD 协议在没有精确的数据分析的情况下也可以工作。

5) 它也可服务于其他的 QKD 协议。

2.3.2. MDI-QKD 协议的不足

1) MDI-QKD 协议具有一个无法被忽略的缺点就是它需要假设 Alice 和 Bob 拥有几乎完美的量子态制备，即在 MDI-QKD 的理想模型中要求使用单光子光源。但在实际中这种每次只发送一个光子的单光子光源基本上是不存在的。因而在标准 MDI-QKD 协议中，使用 WCPs 代替单光子光源，这样的代替一定程度上可以解决单光子光源的问题，但我们知道弱相干光源至少有两个缺点[2]：一是真空脉冲很多，二是多光子概率大。前者因为暗记数会使得在长距离传输中发生大量的比特翻转错误而限制了量子密码的传输距离，后者会导致密钥生成率降低。

2) 在标准的 MDI-QKD 协议中假设使用的是对称信道，但在实际应用中，非对称信道比对称信道更加常见，因而在非对称信道中 MDI-QKD 协议是否依然适用也是一个值得研究的问题。此外，对于理想的 MDI-QKD 协议而言，光子在光纤中传输时应保持连续的传输时间，且在传输过程中纠缠量子位的偏振态不能发生改变。但在实际中以上两点都不会被满足。在实际传输中，信号的损耗既会增加密钥错误率又限制了 MDI-QKD 协议的最大传输距离。

3) 在实现中，脉冲形状不匹配、时间跳动、强度偏振器消光比有限、两个激光间的频率不匹配、偏振不匹配、BS 不对称、错误确定平均光子数的数量、SPD (探测器)具有暗记数和由于数据大小有限而带来的统计波动等问题都会使得 MDI-QKD 协议在实现上不理想。

3. MDI-QKD 协议的改进方法研究

为了提高 MDI-QKD 协议的安全传输距离并提高密钥生成率，现有的研究成果主要针对下述几个改

进方向进行：

1) 信道：将 MDI-QKD 协议应用于非对称信道中并加强其反馈机制。

2) 探测器：使用 id210 探测器或超导纳米线单光子探测器。

3) 光源：用标记单光子源代替弱相干光源。

目前针对 MDI-QKD 在实际应用中的不足，已有下述改进方法，用以提高密钥生成率和安全传输距离。

3.1. 对信道的改进——加强反馈机制

非对称 MDI-QKD 是指在实际应用中 Alice 到 Charlie 和 Bob 到 Charlie 的两条信道具有不相同的传输距离的 MDI-QKD 协议。2013 年卡尔加里大学的概念性证明实验证明了这个非对称的方案[3]。在这个实验中，在短臂的一端添加合适长度的光纤以平衡双方的传输距离从而实现 MDI-QKD 协议。因为在系统中引进了附加的损失，所以还不确定这个方案是否是最佳的方案。主要的问题是在非对称的情况下如何选择最佳的强度。

对于非对称信道，MDI-QKD 系统密钥生成率与信道传输损耗间有何种关系，距离比率对单光子误码率及量子密钥生成率有何影响是值得研究的问题。

2014 年空军工程大学信息与导航学院的东晨、赵尚宏和赵卫虎等[4]对非对称信道的 MDI-QKD 进行了研究得出结论说明 MDI-QKD 可应用于非对称信道，但信道的不匹配度越高，为安全地提取密钥而可容忍的传输损耗下降得越快，密钥安全传输距离越低。为了提高非对称信道下 MDI-QKD 的密钥生成率，可以采取调解信号光强度的方法。

信号在传输中发生的损耗会增加密钥错误率并限制 MDI-QKD 协议的最大传输距离。理想的 MDI-QKD 协议既要求光子在光纤中传输时保持连续的传输时间，又要求在传输过程中纠缠量子位的偏振态不发生改变。但由于实现上的动态属性导致这两点都不能被满足。

为了更好地实现 MDI-QKD 协议，2015 年加拿大卡尔加里大学量子科学技术研究所的 Raju Valivarthi 等人提出了更好的反馈机制，用以消除信道传输上的不足。MDI-QKD 协议在实现上主要的技术挑战是要求两个独立的的光源通过两个独立的光纤进行光子 BSM。这个测量要求输入的光子是完全独立的，且光子间要有足够的时间、极化和光谱重叠。在该改进方案中，主要针对时间重叠、极化重叠和光谱重叠这三个方面进行技术上的改进。

3.2. 对探测器的改进——使用新型高效探测器

为了提高 MDI-QKD 的密钥传输距离，我们可以对其所使用的探测器进行改进，进而可以提高密钥生成率。目前在 QKD 系统中广泛使用的探测器是 id200 探测器。这会使得最小的闲置时间大约在一微秒左右，最大的门率是 1MHz。这限制了 QKD 系统中的最大的光子探测率和密钥生成率。2014 年 V.R.R. Valivarthi 等人提出了使用 id210 探测器代替 id200 探测器的方法来解决这个问题。此外，探测器的暗计数也会影响探测器的探测效率，2014 年 Tang Y L 等人提出在 MDI-QKD 中使用 SNSPDs (超导纳米线单光子探测器)来降低普通探测器的暗记数，进而提高探测效率进而提高密钥生成率和安全密钥传输距离。

3.3. 对光源的改进——标记单光子源

在一个 $\chi^{(2)}$ 的非线性光学晶体(如参量下转换 PDC)中，标记单光子源 HSPS 通过非线性的光学交互产生[22]。激光泵通过非线性光学晶体时一次产生具有两个光子的纠缠对，其中一个光子的探测结果可以预测另一个光子是否到达，控制另一个探测器的开启时间。

通常，人们利用参量下转换 PDC 的过程来制备纠缠光子对，可以得到双模光场[23] [24]：

$$|\psi\rangle_{TS}=\sum_{n=0}^{\infty}\sqrt{P_n}\,|n\rangle_T\,|n\rangle_S$$

$$P_n(x)=\frac{x^n}{(1+x)^{n+1}},(\Delta t_c\gg\Delta t)$$

$$P_n(x)=e^{-x}\frac{x^n}{n!},(\Delta t_c\ll\Delta t)$$

其中，$|n\rangle$代表一个n光子的状态，x代表一个模式的强度(平均光子数)。模式T (闲频光模式)由 Alice 或 Bob 一方的探测器探测，而模式S (信号光模式)则会发送给不可信第三方 Charlie。输出的两种模式的光子数分布相同，且探测器的时间窗口Δt和光子的相干时间Δt_c的关系决定了其具体服从于哪一种分布形式。如果光子的相干时间Δt_c远大于探测器的的时间窗口Δt，则两种模式的光子数将服从热分布；反之，如果在光子的相干时间Δt_c内，则两种模式的光子数将服从于泊松分布。

在 HSPS 输出的两种模式中，光子数是高度相关的。通过这一特性即可完成标记单光子源的实现。应用诱骗态的方法，可以对这个改进协议的单光子信号状态的增益$Q_{rect}^{1,1}$和误码率$e_{diag}^{1,1}$进行估计。通过这样的方法就可以大大减少长距离量子密钥分发过程中暗计数的影响，从而可以增加量子密钥分发的安全传输距离。

此外，也可以使用奇相干光源等其他的光源来代替弱相干光源，但是是否存在一种效率最高的最好的光源，目前还没有定论。

前面我们提到标记单光子源(HSPS)其具体服从的分布的形式与探测器的时间窗口Δt和光子的相干时间Δt_c的关系有关，其既可以服从泊松分布，也可以服从热分布。当标记单光子源(HSPS)服从于不同的分布和使用不同的探测器时，密钥成码率的大小也会存在显著地差别。已有证明当标记单光子源处于热分布时，MDI-QKD 协议的单光子密钥生成率$Y_{1,1}$的下限要高于使用 WCPs 的 MDI-QKD 协议，而误码率$e_{1,1}$的上限要低于使用 WCPs 的 MDI-QKD 协议[25]，但对于当标记单光子源处于泊松分布时并没有给出证明。

在此，本文就该点提出改进与创新：

1) 针对上面提到的基于 HSPS 的 MDI-QKD 协议，本文提出改进方向——调整探测器的时间窗口Δt和光子的相干时间Δt_c的关系使标记单光子源服从泊松分布，通过这样的方法可以提高密钥生成率。

2) 对于上述提出的改进方向对其进行理论上的证明。

一般来说，泊松分布要优于热分布。泊松分布中的多光子脉冲数目要少于热分布，因而当标记单光子源服从泊松分布时会产生更高的密钥生成率。同时，参量下转换(PDC)产生的纠缠光子对与 MDI-QKD 结合可以证明 MDI-QKD 也能应用到 Alice 和 Bob 使用纠缠光子对作为光源的情况的这一假设。

下面，本文将对上述改进方向进行理论上的证明：

本文将估计当标记单光子源(HSPS)服从泊松分布时 MDI-QKD 协议的单光子密钥生成率$Y_{1,1}$和误码率$e_{1,1}$，并证明其优于使用 WCPs 的 MDI-QKD 协议。

$$q_0^v=d_v$$

$$q_n^v=1-(1-d_v)(1-\eta_v)$$

其中v代表 Alice 或 Bob，d_v是探测效率，η_v是 Alice 或 Bob 端的暗记数(由探测器内部的暗计数率和其他的环境噪声所引起的，比如来自时序脉冲的杂散光没有被完全过滤掉[26])。q_n^v代表发出n个光子时 Alice 或 Bob 端探测器触发的概率。

分别用$Y_{m,n}^W$、$S_{m,n}^W$和$e_{m,n}^W$分别代表密钥生成率、增益和误码率。其中m和n分别代表 Alice 和 Bob 端发射的光子数，W (Z/X)代表 Alice 和 Bob 所选择的基，一般来说，用直线基Z作为密钥生成基，对

角基 X 作为错误测试基。Alice 和 Bob 可以在三个强度 0、μ、μ' $(0<\mu<\mu')$中随机的改变发出的光脉冲的强度，设 Alice 和 Bob 端发射的光脉冲的强度分别为 x 和 y，则他们的密度矩阵可表示为：

$$\begin{aligned}\rho_{xy}&=\left(\sum_0^\infty q_n P_n(x)|n\rangle\langle n|\right)\otimes\left(\sum_0^\infty q_n P_n(y)|n\rangle\langle n|\right)\\&=\left(\sum_0^\infty q_n \mathrm{e}^{-x}\frac{x^n}{n!}|n\rangle\langle n|\right)\otimes\left(\sum_0^\infty q_n \mathrm{e}^{-y}\frac{y^n}{n!}|n\rangle\langle n|\right)\end{aligned}$$

由此，我们可以得到：

$$\begin{aligned}S_{xy}=&\tilde{S}_{00}+\eta_A\eta_B x e^{-x} y e^{-y} Y_{11}+\eta_A x e^{-x}\sum_{n=2}^{\infty}\left[1-(1-\eta_B)^n\right]e^{-y}\frac{y}{n!}Y_{1n}\\&+\eta_B y e^{-y}\sum_{m=2}^{\infty}\left[1-(1-\eta_A)^n\right]e^{-x}\frac{x}{m!}Y_{m1}\\&+\sum_{m=2,n=2}^{\infty}e^{-x}\frac{x}{m!}e^{-y}\frac{y}{n!}\left[1-(1-\eta_A)^n\right]\left[1-(1-\eta_B)^n\right]Y_{mn}\end{aligned}$$

其中，$\tilde{S}_{00}=S_{x0}+S_{0y}-S_{00}$。因为 $S_{m,n}^{W}$ 可以通过实验测得，因而 S_{xy} 是一个已知量。

下面，我们将用 $S_{\mu,\mu}$ 和 $S_{\mu',\mu'}$ 来估计 Y_{11}。

当 Alice 和 Bob 同时发送强度为 μ 或 μ' 的脉冲时，有如下等式成立：

$$\begin{aligned}S_{\mu\mu}=&\tilde{S}_{00}+\eta_A\eta_B\mu e^{-\mu}\mu e^{-\mu}Y_{11}+\eta_A\mu e^{-\mu}\sum_{n=2}^{\infty}\left[1-(1-\eta_B)^n\right]e^{-\mu}\frac{\mu}{n!}Y_{1n}\\&+\eta_B\mu e^{-\mu}\sum_{m=2}^{\infty}\left[1-(1-\eta_A)^n\right]e^{-\mu}\frac{\mu}{m!}Y_{m1}\\&+\sum_{m=2,n=2}^{\infty}e^{-\mu}\frac{\mu}{m!}e^{-\mu}\frac{\mu}{n!}\left[1-(1-\eta_A)^n\right]\left[1-(1-\eta_B)^n\right]Y_{mn}\end{aligned}$$

$$\begin{aligned}S_{\mu'\mu'}=&\tilde{S}_{00}+\eta_A\eta_B\mu e^{-\mu'}\mu e^{-\mu'}Y_{11}+\eta_A\mu' e^{-\mu'}\sum_{n=2}^{\infty}\left[1-(1-\eta_B)^n\right]e^{-\mu'}\frac{\mu'}{n!}Y_{1n}\\&+\eta_B\mu' e^{-\mu'}\sum_{m=2}^{\infty}\left[1-(1-\eta_A)^n\right]e^{-\mu'}\frac{\mu'}{m!}Y_{m1}\\&+\sum_{m=2,n=2}^{\infty}e^{-\mu}\frac{\mu}{m!}e^{-\mu''}\frac{\mu'}{n!}\left[1-(1-\eta_A)^n\right]\left[1-(1-\eta_B)^n\right]Y_{mn}\end{aligned}$$

令 $k=\dfrac{(1-\eta_A)(1-\eta_B)^2}{\eta_A\left[1-(1-\eta_B)^2\right]}\left(\dfrac{\mu'}{\mu}\right)^3 e^{2\mu-2\mu'}$，

则 $Y_{11}=\dfrac{k\left(S_{\mu,\mu}-\tilde{S}_{00}\right)-\left(S_{\mu',\mu'}-\tilde{S}'_{00}\right)+\Gamma}{\left[k\eta_A\eta_B\mu^2e^{-2\mu}-(1-\eta_A)(1-\eta_B)\mu'^2e^{-2\mu'}\right]}$，

$$\Gamma=\sum_{n=2}^{\infty}\left\{(1-\eta_A)\mu' e^{-2\mu'}(1-\eta_B)^n\frac{\mu'^n}{n!}-k\eta_A\mu e^{-2\mu}\left[1-(1-\eta_B)^n\right]\frac{\mu^n}{n!}\right\}Y_{1n}$$

其中，

$$+\sum_{m=2}^{\infty}\left\{(1-\eta_B)\mu' e^{-2\mu'}(1-\eta_A)^m\frac{\mu'^m}{m!}-k\eta_B\mu e^{-2\mu}\left[1-(1-\eta_A)^m\right]\frac{\mu^m}{m!}\right\}Y_{m1}$$

且 $\tilde{S}'_{00}$

$$+\sum_{m=2,n=2}^{\infty}\left\{(1-\eta_A)^m(1-\eta_B)^n e^{-2\mu'}\frac{\mu'^m}{m!}\frac{\mu'^n}{n!}-k\left[1-(1-\eta_A)^m\right]\left[1-(1-\eta_B)^n\right]e^{-2\mu}\frac{\mu^m}{m!}\frac{\mu^n}{n!}\right\}Y_{mn}$$

表示 Alice 和 Bob 端探测器没有触发时 Alice 和 Bob 都没有发送光子的概率。

由 $0<\mu<\mu'$ 可以得出 $k\eta_A\eta_B\mu^2e^{-2\mu}-(1-\eta_A)(1-\eta_B)\mu'^2e^{-2\mu'}\le 0$； $\Gamma\le 0$。

因而将得到 Y_{11} 的下限：

$$Y_{11}>Y_{11}^L\equiv\frac{k\left(S_{\mu,\mu}-\tilde{S}_{00}\right)-\left(S_{\mu',\mu'}-\tilde{S}'_{00}\right)}{\left[k\eta_A\eta_B\mu^2e^{-2\mu}-(1-\eta_A)(1-\eta_B)\mu'^2e^{-2\mu'}\right]}.$$

进而可以得到所有成功的事件中单光子脉冲的计数率： $S_{11}=\eta_A\eta_B\mu'^2e^{-2\mu'}Y_{11}$。

当 Alice 和 Bob 得到了足够的原始密钥后，他们用选择直线基 Z 时得到的密钥来生成最终的安全密钥，用选择对角基 X 时得到的原始密钥作为测试比特来检测错误概率(比特翻转错误率为 $E_{\mu\mu}$)，可以得到 e_{11}：

$$e_{11}^X\le\frac{E_{\mu\mu}^XS_{\mu\mu}^X-E_{\mu0}^XS_{\mu0}^X-E_{0\mu}^XS_{0\mu}^X+E_{00}^XS_{00}^X}{S_{11}^X}.$$

结合 GLLP 协议和诱骗态的方法我们可以得出当 HSPS 服从泊松分布时 MDI-QKD 协议的密钥生成率公式(其中 $H(x)=-x\log_2(x)-(1-x)\log_2(1-x)$， $P(x)$ 为光源服从的分布函数， $f(x)$ 为纠错函数，通常令 $f(x)=1.16$)：

$$R\ge\eta_A\eta_BP^2(\mu')Y_{11}^Z\left[1-H\left(e_{11}^X\right)\right]-S_{\mu'\mu'}^Zf\left(E_{\mu'\mu'}^Z\right)H\left(E_{\mu'\mu'}^Z\right).$$

当标记单光子源服从热分布时，其密钥生成率公式为：

$$R\ge\eta_A\eta_B\frac{\mu'^2}{(1+\mu')^4}Y_{11}^Z\left[1-H\left(e_{11}^X\right)\right]-S_{\mu'\mu'}^Zf\left(E_{\mu'\mu'}^Z\right)H\left(E_{\mu'\mu'}^Z\right).$$

当标记单光子源服从泊松分布时，其密钥生成率公式为：

$$R\ge\eta_A\eta_B\mu'^2e^{-2\mu'}Y_{11}^Z\left[1-H\left(e_{11}^X\right)\right]-S_{\mu'\mu'}^Zf\left(E_{\mu'\mu'}^Z\right)H\left(E_{\mu'\mu'}^Z\right).$$

对于标记单光子源(HSPS)而言，当其服从于泊松分布时，它的单光子概率高于 WCPs 的单光子概率，从而导致它的信号脉冲强度 μ' 要高于 WCPs 的信号强度，因而它具有更高的密钥生成率 R。

HSPS 分别服从于泊松分布与热分布的情况比较来看，泊松分布时具有比热分布更高的单光子比率，从而使得泊松分布时 HSPS 具有更高的密钥生成率 R。

当然我们也可以对探测器进行改进如上文提到的 id210 探测器和超导纳米线单光子探测器等。而对于目前广泛使用的探测器而言，光子数解析探测器的探测效率要高于阈值探测器。当对探测器进行改进后，探测效率 η_A 和 η_B 会增大，进而会增大密钥生成率 R。

2016 年，空军工程大学薛阳等人提出可以使用修正相干态光源(MCS)来优化发送端光源的光子数分布，提高了 MDI-QKD 系统的传输性能。相较于使用 HSPS 光源的方案，MCS 光源有更大的传输极限距离和更低的误比特率。其使用的全局估计方法能够提高参数估计的效率，也值得借鉴。

4. 总结与展望

本文对MDI-QKD协议进行了研究，具体分析了其协议流程，对MDI-QKD协议进行了安全性分析并总结其优越性与不足。自2012年MDI-QKD协议被Lo提出以来，它相比于其他QKD协议的优点就非常显著，它能够弱化所有的探测器侧信道攻击的优势，因而在理论上具有很强的安全性。此外，它因能够提高安全密钥传输距离与密钥生成率而受到了国内外研究机构的关注与研究。为了提高其安全密钥生成率与增加安全传输距离，各研究机构针对其实现上的不足提出了改进的方案。本文分析研究了MDI-QKD的

若干改进协议并针对基于标记单光子源的MDI-QKD协议这一改进方法提出了一个改进方向，进而对这一改进方向进行理论上的推导，证明当使用标记单光子源(HSPS)来代替弱相干光源且其服从于泊松分布时会产生更高的密钥生成率。

基金项目

国家高科技研究和发展项目(863 项目) (2011AA010803)；
国家自然科学基金项目(U1204602)；
数学工程与先进计算国家重点实验室开放课题项目(2013A14)。

参考文献 (References)

[1] Lo, H.K., Curty, M. and Qi, B. (2012) Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, **108**, Article ID: 103503. https://doi.org/10.1103/PhysRevLett.108.130503

[2] Wang, Q. and Wang, X.B. (2013) An Efficient Implementation of the Decoy-State Measurement-Device-Independent Quantum Key Distribution with Heralded Single-Photon Sources. *Physical Review A*, **88**, Article ID: 052332. https://doi.org/10.1103/PhysRevA.88.052332

[3] Rubenok, J.A., Slater, P., Chan, I., *et al*. (2013) Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Physical Review Letters*, **111**, Article ID: 130501. https://doi.org/10.1103/PhysRevLett.111.130501

[4] 东晨, 赵尚宏, 赵卫虎, 等. 非对称信道传输效率的测量设备无关量子密钥分配研究[J]. 物理学报, 2014, 63(3): 28-32.

[5] Valivarthi, V.R.R., Chan, P., Lucio-Martinez, I., *et al*. (2014) Measurement-Device Independent Quantum Key Distribution with id210 Detectors. *Quantum Science and Technology*.

[6] Tang, Y.L., Yin, H.L., Chen, S.J., *et al*. (2014) Measurement-Device-Independent Quantum Key Distribution over 200km. *Physical Review Letters*, **113**, Article ID: 190501. https://doi.org/10.1103/PhysRevLett.113.190501

[7] Abruzzo, S., Kampermann, H. and Bruß, D. (2013) Long-Distance Measurement-Device-Independent Quantum Key Distribution Without Quantum Memories. *Applied Physics Letters*, **103**, Article ID: 061101.

[8] Valivarthi, R., Lucio-Martinez, I., Chan, P., *et al*. (2015) Measurement-Device-Independent Quantum Key Distribution: From Idea towards Application. *Journal of Modern Optics*, 62, 1141-1150. https://doi.org/10.1080/09500340.2015.1021725

[9] 毛钱萍, 赵生妹, 王乐, 等. 基于波分复用技术的测量设备无关量子密钥分发[J]. 量子电子学报, 2017, 34(1): 47-49.

[10] 尹华磊, 刘慧, 陈腾云. 超过 404km 的测量设备无关量子密钥分发实验[J]. 信息安全研究, 2017, 3(1): 75-78.

[11] 薛阳, 马丽华, 石磊, 魏家华, 罗均文. 基于修正相干态光源的 MDI-QKD 全局估计性能分析[J]. 量子电子学报, 2014, 34(4): 447-449.

[12] 朱卓丹, 赵尚弘, 苏力华, 王星宇. 预报相干光子对的测量设备无关量子密钥分发协议研究[J]. 激光与光电子学进展, 2017, 54(12): 122703.

[13] 姬一鸣, 李云霞, 石磊, 蒙文, 崔树民, 许振华. 基于 MDI-QKD 的多用户接入组网方案研究[J]. 光网络, 2015(11): 10-11.

[14] 孙颖, 赵尚弘, 东晨. 基于量子存储和纠缠光源的测量设备无关量子密钥分配网络[J]. 光学学报, 2016, 36(3): 037001.

[15] Roberts, G.L., Lucamarini, M., Yuan, Z.L. (2017) Experimental Measurement-Device-Independent Quantum Digital Signatures. *Physical Review A*, **8**.

[16] Wang, C., Guo, GC. and Wang, S. (2017) Measurement-Device-Independent Quantum Key Distribution Robust against Environmental Disturbances. *Optica*, **4**, 1016.

[17] 颜龙, 孙豪, 赵生妹. 应用诱骗态的光子轨道角动量测量设备无关量子密钥分发协议的研究[J]. 信号处理, 2014, 30(11): 1276-1277.

[18] Gottesman, D., Lo, H.K., Lütkenhaus, N., *et al*. (20040 Security of Quantum Key Distribution with Imperfect Devices. *Quantum information & computation*, **5**, 325-360.

[19] Hwang, W.Y. (2003) Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Re-*

view Letters, **91**, Article ID: 057901.

[20] Inamori, H. (2002) Security of Practical Time-Reversed EPR Quantum Key Distribution. *Algorithmica*, **34**, 340-365.

[21] Feihu Xu, Bing Qi, Zhongfa Liao, and Hoi-Kwong Lo. Practical aspects of measurement-device-independent quantum key distribution[J]. *New Journal of Physics*, 2013, 15(6): 061101.

[22] Castelletto, S.A. and Scholten, R.E. (2008) Heralded Single Photon Sources: A Route towards Quantum Communication Technology and Photon Standards. *The European Physical Journal Applied Physics*, **41**, 181-194.

[23] Yurke, B. and Potasek. M. (1987) Obtainment of Thermal Noise from a Pure Quantum State. *Physical Review A*, **36**, 3464.

[24] Lu'tkenhaus, N. (2000) Security against Individual Attacks for Realistic Quantum Key Distribution. *Physical Review A*, **61**, Article ID: 052304.

[25] 朱峰, 王琴. 基于指示单光子源的量子密钥分配协议[J]. 光学学报, 2014(6): 266-271.

[26] 罗军. 诱骗态量子密钥分配协议的研究[D]: [硕士学位论文]. 哈尔滨: 哈尔滨工业大学, 2011.