Applied Physics 应用物理, 2017, 7(8), 235-246
Published Online August 2017 in Hans. http://www.hanspub.org/journal/app
https://doi.org/10.12677/app.2017.78030

Hans汉斯

Quantum Channel Physical Security Detection Based on Photon Number Measurement

Jian Peng

School of Mathematics and Physics, North China Electric Power University, Beijing
Email: pjian@ncepu.edu.cn

Received: Aug. 16th, 2017; accepted: Aug. 19th, 2017; published: Aug. 24th, 2017

Abstract

The ideal single photon source and high performance single photon detectors are two key factors that restrict the key security and bit rate in quantum key distribution system. As a single photon source, the weak coherent pulse must contain fewer average photon number for the sake of security, thus the quantum bit rate cannot be raised to a high level. Superconducting transition edge sensor for single photon detection has been introduced. It is proposed that multi-port beam splitter combined with many APDs can be used to detect the photon number in weak coherent pulse in quantum key distribution system. The attack tactics of eavesdropper is analyzed, and based on photon number detection, it is proposed that the average photon number in weak coherent pulse can be improved, thus the quantum key bit rate can be improved.

Keywords

Quantum Key Distribution, Single Photon Detector, Key Security, Key Bit Rate

基于光子数测量的量子信道物理安全检测

彭　建

华北电力大学数理学院，北京
Email: pjian@ncepu.edu.cn

收稿日期：2017年8月16日；录用日期：2017年8月19日；发布日期：2017年8月24日

摘　要

理想的单光子源和高性能的单光子探测器是制约量子密钥分配系统中的密钥安全和码率的两个关键因素。

文章引用: 彭建. 基于光子数测量的量子信道物理安全检测[J]. 应用物理, 2017, 7(8): 235-246.
DOI: 10.12677/app.2017.78030

弱相干脉冲作为单光子源，为保证安全性，平均光子数必须少而限制了码率的提高。本文介绍了超导边沿传感器单光子探测器，提出了多端口分束器与多APD结合可用于量子密钥分配系统中检测弱相干脉冲中的光子数。对窃听者的攻击策略进行分析的基础上，基于光子数的检测，指出在保证安全性的前提条件下可以提高弱相干脉冲中的平均光子数，进而提高系统的量子密钥成码率。

关键词

量子密钥分配，单光子探测器，密钥安全性，密钥码率

1. 引言

量子密钥分配(QKD)是量子信息技术中最接近实用化的技术。与传统密钥的产生与分配不同，当今量子密钥的产生与分配是在专用的自由空间或是光纤信道中，基于量子力学的测不准原理、测量坍缩原理及量子不可克隆原理，按照一定的协议规范去操作携带量子信息的单光子，使发送方(Alice)与接收方(Bob)同时获得加密密钥与解密密钥，并可杜绝传统密钥在传送过程中失密的可能。原则上来说，如何安全、高效、方便地去实现量子密钥分配取决于协议规范。现存的协议规范基本的还是 BB84 协议、B92 协议和 EKert 协议三种。出于对具体的实验条件和安全性增强的考虑，发展出了很多新的协议[1]-[9]。当今量子密钥分配实验系统中[10] [11] [12] [13]，影响量子密钥安全和码率的关键因素有两个：一是尚未开发出理想的单光子源。虽然量子点单光子源的研究展示着很好的前景，但远未到实用化阶段，目前多是利用相干光源衰减到单光子水平，由于相干光源的光子数分布规律的限制，总会产生很多空脉冲和多光子脉冲，这就限制了码率，并为窃听者攻击留下了可能；二是实用化的单光子探测器(SPD)的探测速率与效率与期望值相差甚远，因而进一步地限制密钥的成码率。多光子脉冲的存在为窃听者(Eve)进行信息窃取提供了可能。但窃听者的存在，必将扰动光子数的分布。本文立足于现有的单光子探测器基于对光子数的检测，提出了一种检测窃听者对量子信道进行攻击的方法。

2. 单光子探测器对光子数的检测

目前，可对光子数进行探测的主要方法有两类：一类是基于现有的单光子探测器，将脉冲中的光子数进行分解，通过多端口探测器来探测光子数；另一类方法是采用某些超导薄膜在正常态与超导态温度转变边沿陡峭的电阻与温度变化关系做成超导转变边沿传感器(TES)来实现单光子探测。由于超导薄膜吸收不同数量的光子引起超导薄膜系统的温度变化不同，进而引起电阻变化的大小不同，最终引起偏置电路的电流变化不同而实现光子数的可分辨。

图 1 展示的是用钛(Ti)做成超导薄膜的 TES 单光子探测器的光学照片，其中存在有两种不同尺寸的 4 个 TES 单光子探测器[14]。其制作的工艺流程是首先在覆盖有一定厚度氮化硅(SiN)的硅(Si)衬底上，通过电子束蒸发或磁控溅射的方式生长一层几十纳米厚的单层或双层超导薄膜，一般单元素超导薄膜除了钛(Ti)薄膜之外还有有钨(W)薄膜、铪(Hf)薄膜等，这几种超导薄膜的超导转变温度 Tc 分别在 100、390 和 128 mK 附近。也可以制作出 Ti/Au 或 Ti/Pd 等复合双层薄膜，这时可以利用近邻效应，通过改变 Au 或 Pd 等正常金属层的厚度来改变 Tc 值[15]。为了提高 Au 或 Pd 与 SiN/Si 衬底之间的黏合性，在生长 Au

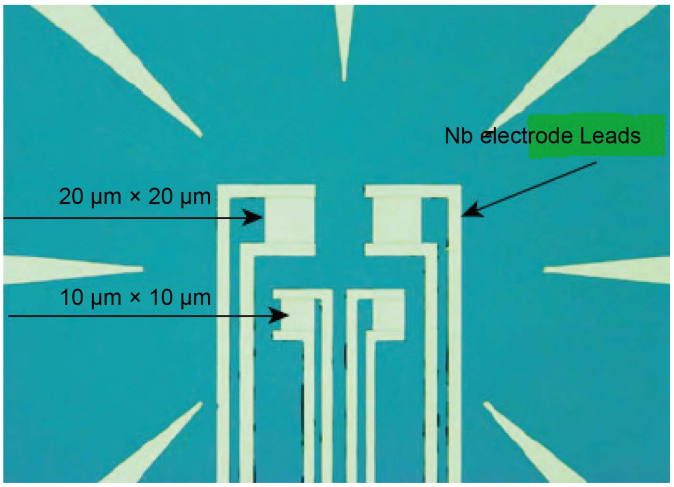

Figure 1. The photo of the Ti TES single photon detector
图 1. Ti TES 单光子探测器光学照片[14]

或 Pd 正常金属层之前，一般先沉积一层厚度为 10~15 nm 的 Ti 薄膜，再在其上生长正常的 Au 或 Pd 薄膜，最后生长出厚度约几十纳米的超导 Ti 薄膜层。为了使不同金属薄膜层之间保持干净良好的界面，制备 Ti/Au 或 Ti/Pd 双层薄膜的三次薄膜生长过程必须确保在同一真空环境中完成。待薄膜生长完毕之后，做一次光刻，针对不同薄膜层，通过专门的刻蚀方法完成整个薄膜的图形化，形成具有特定尺寸的 TES。制备 TES 所需的超导引线和和芯片周围的焊盘一般采用超导铌(Nb)或铝(Al)材料，二者的 Tc 值分别为 9.5 和 1.1 K，因而在探测器几百 mK 的工作温度下是完全超导的。制作工艺上，引线和焊盘通常为同一层，一般采用溅射方法生长，厚度在 100~150 nm 之间，最后使用剥离技术完成图形化。每个 TES 由两根超导 Nb 引线实现电连接，其中叉指结构的作用是方便光学对准。

TES 探测器的灵敏度取决于超导薄膜的热容 Ce。为了达到单光子能量探测水平并具备光子数分辨能力，TES 超导薄膜的热容 Ce 须尽可能小，薄膜超导转变区域内 R-T 曲线变化应尽可能陡(超导转变温度变化宽度 ΔTc 尽可能小)，而且探测器的热噪声和读出电子学系统噪声水平要尽可能低。因此，超导 TES 单光子探测器中 TES 的尺寸不能太大，通常在 20 μm × 20 μm 左右，ΔTc 在 1.0 mK 量级，Tc 值也即探测器的工作温度一般在几百 mK 温度范围内。

图 2 为超导 TES 探测器的工作原理图。当有 n 个能量为 E_0 的光子同时被超导薄膜吸收时，产生的总能量 $E_{ph} = nE_0$ 会引起 TES 的电子系统温度 Te 出现微小的变化量 $\Delta T = E_{ph}/Ce$，进而引起 TES 的电阻产生 ΔR 的变化量，图 2(a)给出的是 1 个(1 ph)和 2 个光子(2 ph)被吸收后 TES 阻值变化示意图。TES 采用的是恒压偏置，如图 2(b)所示，ΔR 的变化量引起 TES 所在支路的电流变化量 ΔI 被与 TES 串联的高灵敏超导量子干涉放大器(SQUID)读出。不同数目光子被吸收时，被探测到的响应信号 ΔI 也不相同。图 2(c)显示的是对应吸收 1 和 2 个光子后 ΔI 的响应曲线。在一定的能量范围内，ΔI 的幅度值与被吸收的光子数目成正比，这样就实现了具有光子数分辨能力的探测。

超导 TES 单光子探测器的典型测试系统如图 3 所示[17]，其中包括 TES 的偏置和读出电路，以及光脉冲产生和耦合系统。探测器芯片通常被固定在制冷机的 mK 温区上，使芯片的衬底温度等于 mK 温区的温度。R_b 是处于低温下与 TES 支路并联的电阻，阻值通常在 mΩ 量级，远小于 TES 在工作点处的阻值 R_{TES}。TES 工作时所需要的电压偏置由室温电流源提供的偏置电流 I_b 流过 R_b 来实现，此时 TES 两端的电压约为 $V_b = I_b \cdot R_b$。流过 TES 的电流是通过一个输入线圈 L_{in} 与其串联、工作在磁通锁定环路(flux-locked loop, FLL)的 SQUID 来读出的。单个光子引起的 TES 阻值变化量 ΔR 是非常小的，为了准确

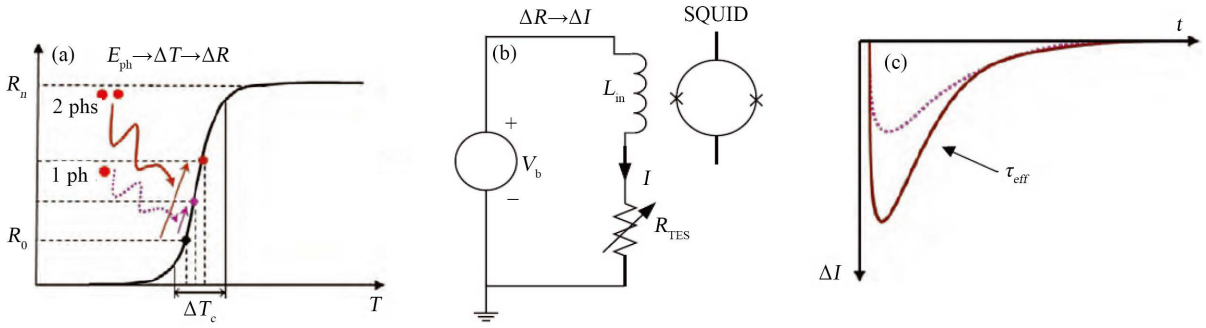

Figure 2. The working principle diagram of the superconducting TES single photon detector [16]. (a). Changes of TES resistance after absorbing 1 and 2 photons; (b) Measurement of TES branch current by voltage bias; (c) The TES branch responds to the current pulse after absorbing 1 and 2 photons

图 2. 超导 TES 单光子探测器工作原理图[16]。(a) 吸收 1 个和 2 个光子后的 TES 阻值变化示意图；(b) 电压偏置测量 TES 支路电流；(c) 吸收 1 个和 2 个光子后 TES 支路的响应电流脉冲

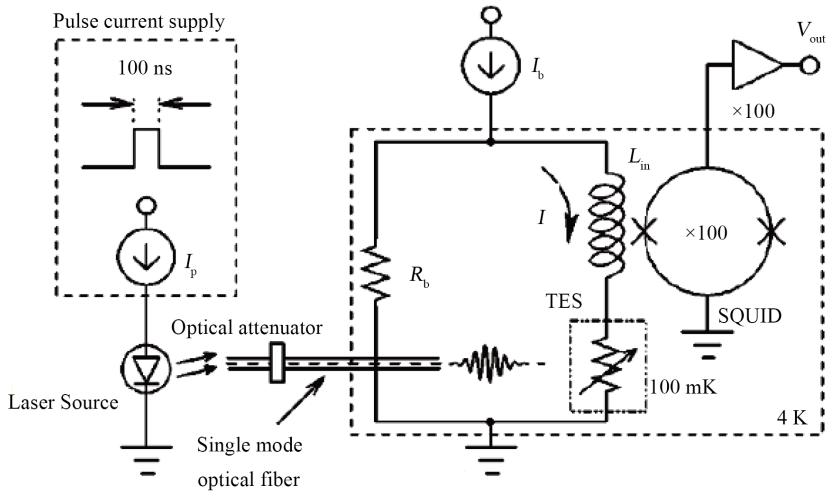

Figure 3. Typical test system for the superconducting TES single photon detector

图 3. 超导 TES 单光子探测器的典型测试系统[17]

探测到因电阻变化引起的电流变化量 ΔI，采用铌钛(NbTi)合金超导线来实现电阻 R_b、SQUID 输入线圈 L_{in} 以及 TES 构成的整个环路的电连接。通过单模光纤将光脉冲从室温的发生系统导入至 mK 温区下的探测器，光纤末端与探测器的距离一般保持在 100 μm 左右。

世界上有很多研究小组研发出了 TES 单光子探测器[14] [18]。进一步通过集成光学谐振腔并提高光纤与探测器之间的光耦合效率的办法，目前的超导 TES 单光子探测器的系统探测效率在多个波长下已接近 100%。对 1550 nm 的光纤量子通信波段，光子的能量分辨已达到 0.2 eV 以下，并表现出多至 29 个光子态的分辨能力。相较于 APD 单光子探测器，超导 TES 单光子探测器的突出优点在于极低的暗计数率(典型值在几个赫兹以下)、很高的探测效率、可分辨光子数及可实现光子能量的分辨。但其响应速度以及时间抖动等特性仍存在不足，目前最快的超导 TES 单光子探测器的响应时间在 300 ns 左右，最小的时间抖动在 20 ns 左右。TES 单光子探测器使用的最大问题则是在于必须在极低温下工作，制冷系统体积庞大，使用成本高昂，因此很难用于实用的量子密钥分配系统中。

在实用的光纤通信 1310 nm 与 1550 nm 波段，为了有效地进行单光子探测，普遍采用的是带隙渐变的吸收区与倍增区分离结构的雪崩二极管(SAGM-APD)，其结构如图 4 所示[19] [20]。综合考虑带隙结构、暗噪声大小、工作温度和晶体缺陷等因素，通常选用 III-V 族化合物半导体(InGaAs)作为吸收区材料。重

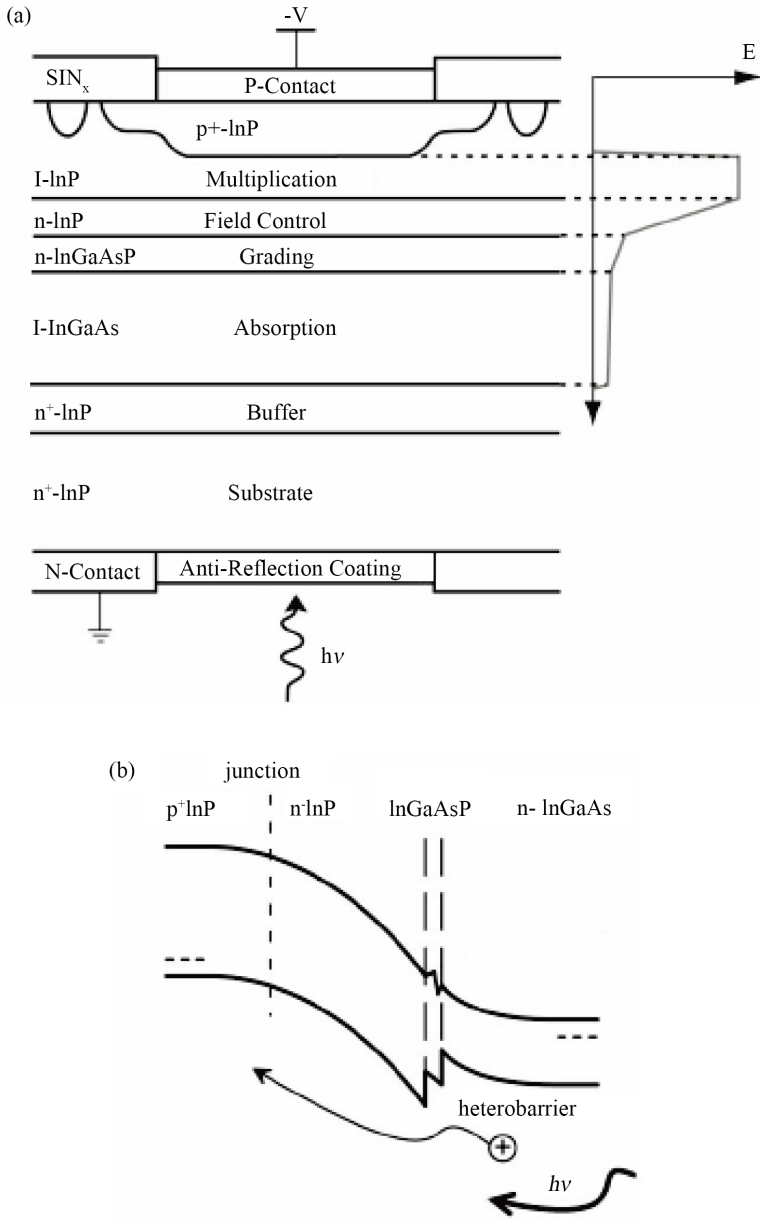

Figure 4. Sectional drawing of SAGM-APD and energy band diagram of InGaAs/InP material
图 4. InGaAs/InP 材料的 SAGM 型 APD 的截面图和能带图

掺杂的 n^+-InP 作为衬底和缓冲层，由于其具有宽的带隙(EG = 1.35 eV)，因而波长大于 900 nm 的红外波段的光可以接近透明通过。非掺杂的 I-InGaAs 作为吸收层，其带隙约为 0.73 eV，对波长小于 1700 nm 的红外波段的光具有很好的吸收特性，可在此充分吸收。本征 I-InP 层作为倍增层，可在其中建立很高的电场，雪崩倍增过程就发生在其中。n-InP 作为电场控制层，当反向偏压很大时，倍增区可扩展到其中，与拉通型 APD 的 π 区的作用相似，起到控制倍增区电场的作用。由于 InGaAs 和 InP 带隙相差很大，能带在此发生突变，因而光生空穴容易在它们的界面发生陷落，出现电荷的堆积，影响器件的量子效率和响应速度。为了解决此问题，往往在 n-InP 和 i-InGaAs 层之间加上两层掺杂浓度不同，厚度约为 1~2 μm 的 InGaAsP 材料。

作为单光子探测器的核心部分——雪崩二极管(APD)必须以“盖革”模式工作[19] [20] [21]，这是通过性能优越的抑制电路来实现的。最早应用的是无源抑制电路，以后又出现了主动抑制电路和门模电路以及它们之间的组合。在量子密钥分配系统中，携带量子信息的光子到达的时间一般是准确知道的，因此普遍采用的是门模抑制电路。图 5 即为工作于门控“盖革”模式的单光子探测器示意图，其右上图表示的是加在 APD 上的反向电压时序图。其工作的门控时间通常为 1~100 ns，而为了抑制后脉冲，其不工作的死时间通常为 1~10 μs。

很显然，工作于“盖革”模式的 APD 型单光子探测器是不足以直接检测到达接收端的某一脉冲所包含的光子数的。1999 年 Kim 等人提出了基于光学参量下转换产生的双光子光程的不同，因而在高灵敏度、响应区域大的可见光光子计数仪中产生的响应脉冲幅值与脉宽的不同来区分单光子与双光子。但这种方法只可以用于双光子检测，且暗计数率比较高[22] [23] [24]。山西大学何博等人研究了单光子探测器对微弱激光脉冲的暂态响应，利用不同光子数的响应时间不同的特性去实现光子数的分辨测量[25]。技术上也可将包含多个光子的弱光脉冲经 N 通道分流变为时间独立的 N 个单光子脉冲，耦合进入 N 个探测器，实现一定程度上的光子数区分[26] [27] [28] [29]。

作者在文献[29]中从解决 QKD 系统码率过低的角度出发，提出了充分利用“单 APD”探测器处于沉寂状态的时隙窗口的方案。为此设计了多端口分束器与多 APD 结合构成各端口时分工作模式的探测器来代替 QKD 系统中的每一单光子探测器，如图 6 所示。它通过一对称的 N 端口光纤分束器(耦合器)与光纤

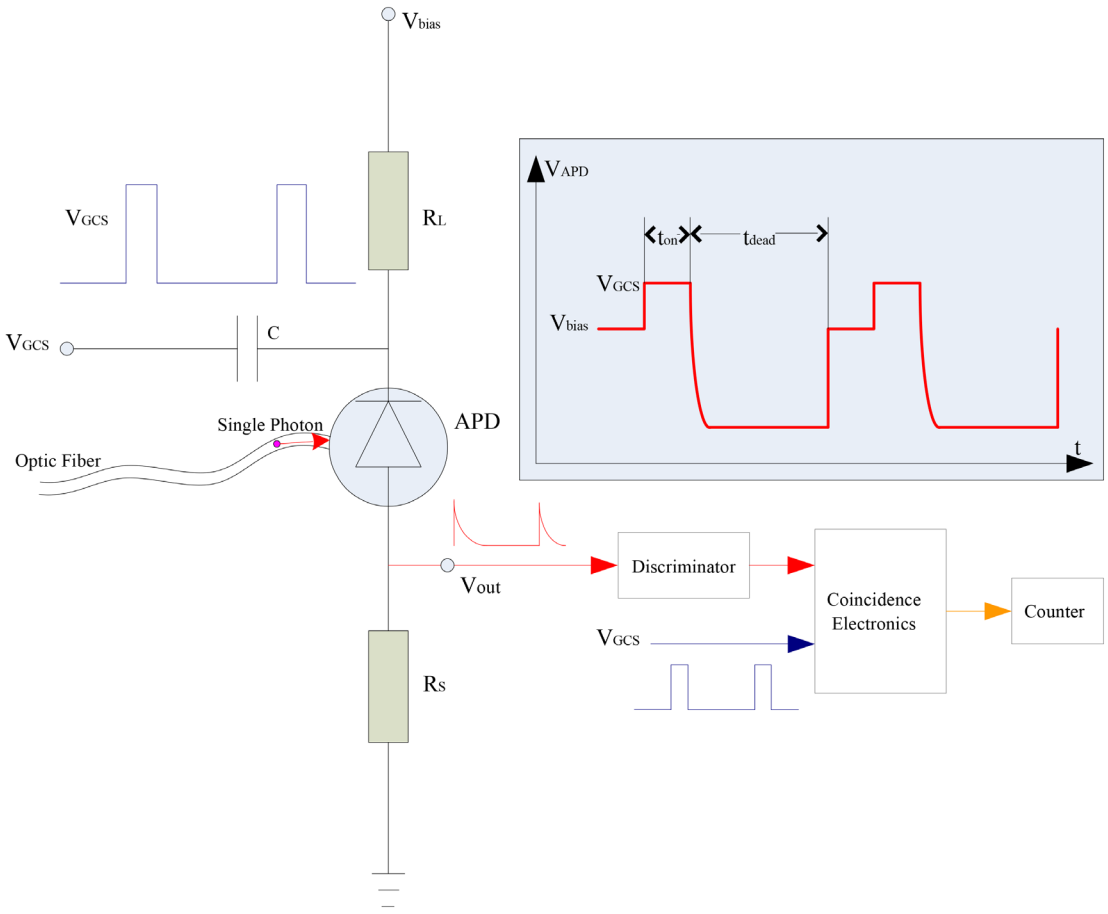

Figure 5. The single photon detector operating in gated “Geiger” mode
图 5. 工作于门控“盖革”模式的单光子探测器

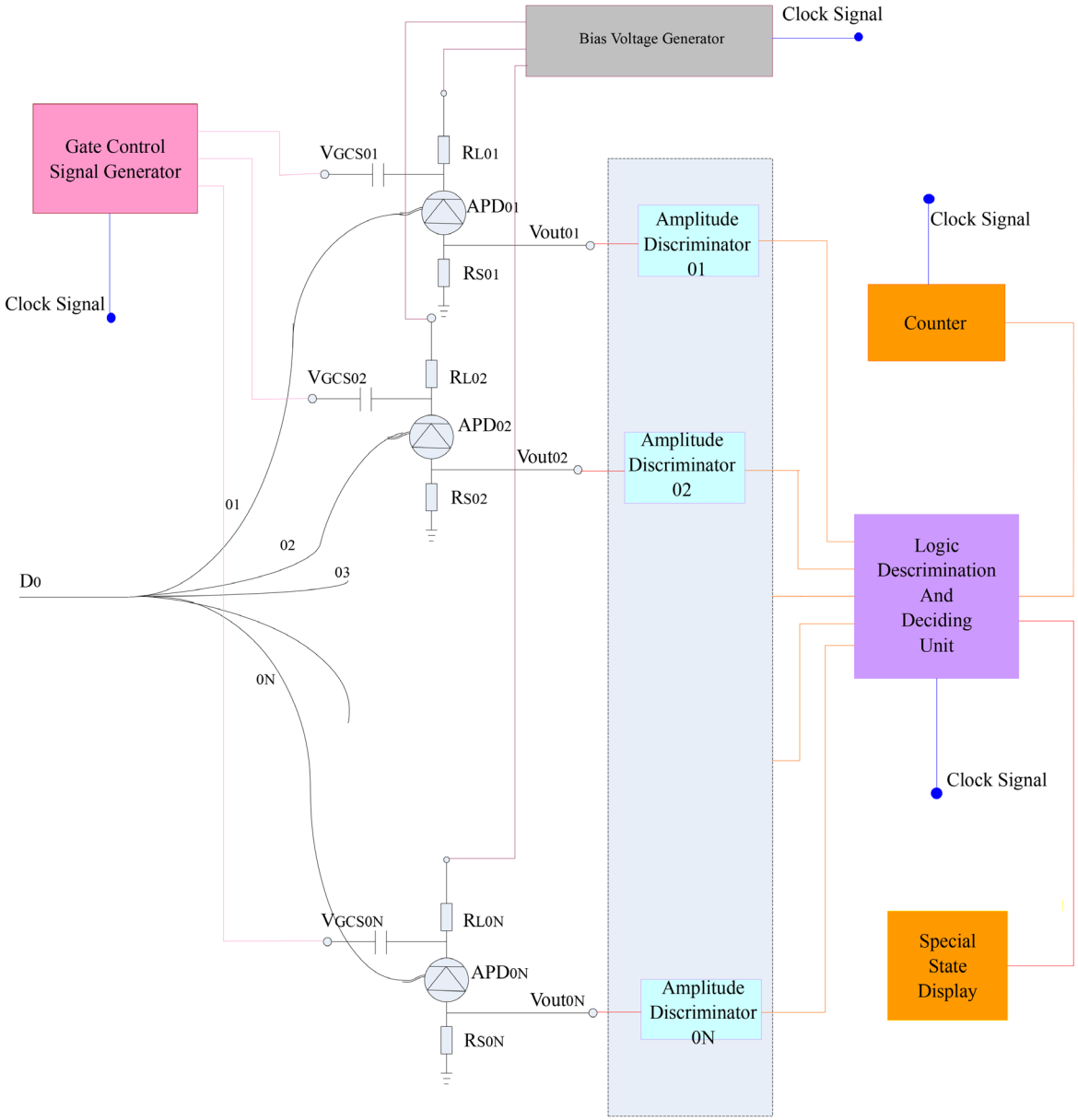

Figure 6. Quick single-photon detector with multi-port splitter and many APDs work on time division
图 6. 多端口分束器与多 APD 结合构成的各端口时分工作模式的快速单光子探测器[29]

链路相连接。每一端口配置一反向偏置的雪崩二极管(APD)。各端口的 APD 均采用门控“盖革”模式工作，其偏置电压由一偏置电压产生器集中提供，其门控信号也由一门控信号发生器集中提供，这样可降低电路的复杂性，减少成本，并有利于提高工作的可靠性。偏置电压产生器与门控信号发生器可由从单光子源提取的时钟信号进行同步控制。从各端口输出的雪崩信号首先经幅度鉴别，然后输入到逻辑判决单元，与时钟信号进行符合，判别是否为暗计数与后脉冲引起的误计数，还可判别是否为多光子脉冲，并将这类特别事件输出显示出来。

为了使图 6 中的快速单光子探测器达到最大效能，端口数 N 的选择应该满足以下条件

$$N > \mathrm{Int}\left[\mu * \left(t_{\mathrm{dead}} / t_{\mathrm{on}}\right)\right] + 1 \tag{1}$$

其中 μ 表示每脉冲的平均光子数，Int 表示取 t_{dead}/t_{on} 的较大整数，t_{dead} 与 t_{on} 分别表示单 APD 探测器的死时间与工作窗口的时间宽度。

从其工作过程看，这种探测器中的多端口分束器的端口数如果足够多的话，则可同时检测到达端口的弱相干脉冲中所包含的光子数。

现在有些研究组正在利用光电子集成开发单光子探测阵列[30]。如果单光子探测阵列实现了实用化，则成本可极大降低。通过多端口分束器，可实现脉冲中的光子数检测。端口数越多，检测的准确度越高。当然辅以光开关或时分复用解复用器来控制路由，则可极大提高 QKD 系统的工作频率，提高量子密钥的成码率。

3. 对量子信道安全的物理检测

从量子密钥分配系统来说，只要将相干光源衰减到单光子水平，通过误码率检测和密钥增强的方法，原则上是可以得到安全密钥的。但是对光子数的检测，不仅是个科学问题，对于量子密钥分配系统来说，如果准确知道单脉冲中所包含的光子数，也有助于改进系统的安全性。

当今 QKD 系统中采用的光源一般是激光脉冲经衰减而成。含有极少平均光子数的相干态(单光子 Fock 态)中的光子数遵循泊松分布(Poisson Distribution)，其统计规律为

$$P(n,\mu)=\frac{\mu^n}{n!}\mathrm{e}^{-\mu} \tag{2}$$

其中 μ 为平均光子数，$P(n,\mu)$ 为脉冲中包含 n 个光子的概率。图 7 即为不同平均光子数情况下的光子数泊松分布。

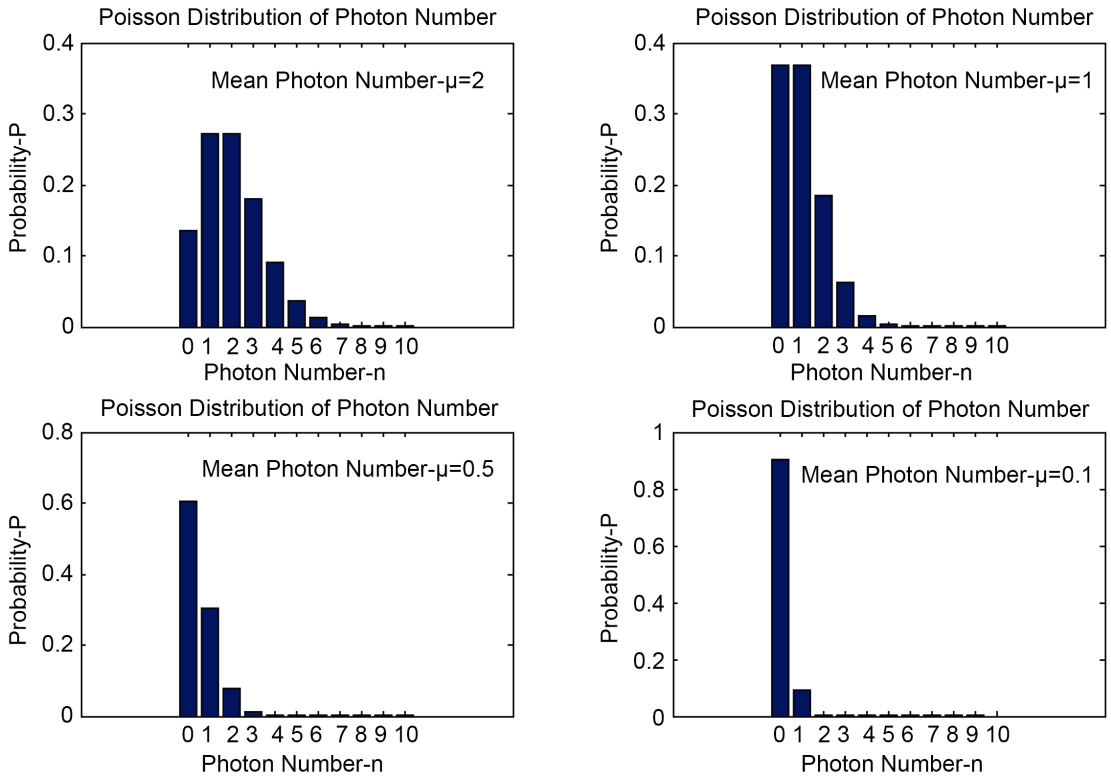

Figure 7. Photon number Poisson distribution with different average photon number
图 7. 不同平均光子数情况下的光子数泊松分布

从图 7 可看出，如果平均光子数 μ 过大，则一个脉冲包含多光子数的概率也较高。窃听者(Eve)原则上可采用光子数分离器(PNS)攻击而摄取其中的光子进行测量，以获得密钥信息。从安全的角度考虑，目前的 QKD 系统中通常是将激光脉冲衰减到 μ = 0.1 的水平，但这时绝大部分脉冲不包含光子，即为空脉冲，因而 QKD 系统的码率大为受限。QKD 系统中的 Alice 与 Bob 方不能肯定在密钥的产生与分配中是否有 Eve 的存在，为了确保密钥的安全，总是要牺牲所获得的一部分量子比特通过一定的算法进行信息调和与密钥增强，最后得到的密钥码率进一步降低。

在进行量子密钥分配时，如果能够实时检测到 Eve 的存在，则总是会采取具体行动，去捕获窃听者。但若能通过检测，确切排除 Eve 的存在，则只要进行纠错而没有必要再进行密钥增强，甚至可以提高脉冲的平均光子数，使密钥码率得到有效提高。

图 6 所示的快速单光子探测器除了能够提高 QKD 系统单光子的探测速率外，还能够实时检测是否存在窃听者(Eve)。图 3 所示的超导 TES 单光子探测器更是能准确检测到弱相干脉冲中所包含的光子数。在 Eve 发起 PNS 攻击时，必定要截取 Alice 发送给 Bob 的光子进行测量，因而脉冲所包含的光子数的泊松分布将可能受到干扰。其检测的原理是同时记录图 6 中的探测器对每一脉冲的响应端口数，以确定该脉冲包含的光子数，然后对脉冲包含的光子数进行统计分析，根据光子数的平均值及统计分布以确定是否受到窃听者的干扰。

窃听者通常要根据脉冲的平均光子数选用截取光子的技术方案。当脉冲的平均光子数较多时，比如 $\mu > 2$，这时他可以选用 PNS 攻击。这种攻击的物理效果对光子数的泊松分布并无改变，只是相当于在量子信道中引入一个固定的损耗。依靠纠错和密钥增强无法探知 Eve 的攻击，且不能杜绝密钥的泄漏，但可以通过检测 Bob 端的平均光子数来确定 Eve 是否存在。通常 Alice 到 Bob 之间的光纤长度及光纤单位距离的损耗是一定的，因而量子信道总的损耗也是一定的。若 Alice 发送的脉冲包含的平均光子数保持不变，Bob 端在考虑信道损耗后，依据检测脉冲的平均光子数是否符合期望值就可以确定是否有 Eve 的存在。另外，Bob 还可以对不同时段的光子数分布求平均，依据光子数平均值的变化确定是否有 Eve 的加入和退出。

当脉冲的平均光子数很少时，比如 μ = 0.1，Eve 可能采用“截收－发送”的光子截取方案。在这种情况下，量子信道中 Alice 发送给 Bob 的光子可能被 Eve 全部截收，Eve 进行量子测量后再发送给 Bob。这时光子数的泊松分布不会改变，依靠光子数检测，不能确定 Eve 的存在。Bob 只能依据光子量子态的测量坍缩引起系统误码率的显著升高来确定 Eve 的存在。Bob 依靠纠错和密钥增强过滤掉可能泄密的量子比特，这是 QKD 系统的常规方法。

当脉冲的平均光子数介于以上两者之间，比如 μ = 1，Eve 将最可能选用“光子计数－单光子摄取”的光子截取方案。即他有选择的摄取多光子脉冲中的其中一个光子进行测量，以获取关于密钥的信息，而对单光子脉冲中的光子则让其无干扰地通过。这种情况依靠纠错和密钥增强是无法确定 Eve 的存在的，也不能杜绝密钥的泄漏，但将改变光子数的泊松分布。

现在分析 Eve 采用“光子计数－单光子摄取”的光子截取方案时光子数分布的变化。假设无 Eve 干扰，这时光子数遵循泊松分布为 $P(n,\mu)$，其中 μ 为平均光子数，光子数的分布情况如图 7 所示。考虑 Eve 对量子信道中的光脉冲进行光子截取，光子数的分布将变为 $P_d(n,\mu)$，这时满足下列关系：

$$P_d(n=0,\mu)=P(n=0,\mu) \tag{3}$$

$$P_d(n=1,\mu)=P(n=1,\mu)+P(n=2,\mu) \tag{4}$$

$$P_d(n=2,\mu)=P(n=3,\mu) \tag{5}$$

$$P_d(n=3,\mu)=P(n=4,\mu) \tag{6}$$

…

$$P_d\left(n=k,\mu\right)=P\left(n=k+1,\mu\right) \tag{7}$$

图 8 所显示的是依据(3)~(7)式得出的 Eve 截取多光子脉冲中的一个光子后的光子数分布。从图 8 可看出，Eve 截取光子后，明显地改变了光子数的分布情况，其中含有一个光子的脉冲显著增多。这种变化还与 Alice 发送脉冲的平均光子数有关，当 $\mu=1$ 时表现尤为显著。

从上可看出，光子数检测是对所有脉冲包含的光子数进行实时检测与监控，是一种统计检测。结果的准确度将受到图 6 所示的快速单光子探测器的光子端口路由的影响。如果一个脉冲的多个光子进入同一个端口，则只引起一个端口探测器的响应，光子的计数只为 1，使检测结果偏离图 7 和图 8 的分布。由此引起的光子数分布不确定度以 U_1 表示，其大小应该反比于端口数 N，即

$$U_1=\frac{k}{N} \tag{8}$$

上式中的 k 为一常数，可由实验测定。

每一端口的雪崩二极管(APD)的暗计数也会影响光子数检测结果的准确度。由暗计数引起的光子数检测的不确定度以 U_2 表示，假设每一门脉冲时间 τ 内的暗计数率为 P_{dark}，则 U_2 为

$$U_2=NP_{dark}\tau \tag{9}$$

光子数检测结果的总不确定度 U 为

$$U=\sqrt{U_1^2+U_2^2}=\sqrt{\left(\frac{k}{N}\right)^2+\left(NP_{dark}\tau\right)^2} \tag{10}$$

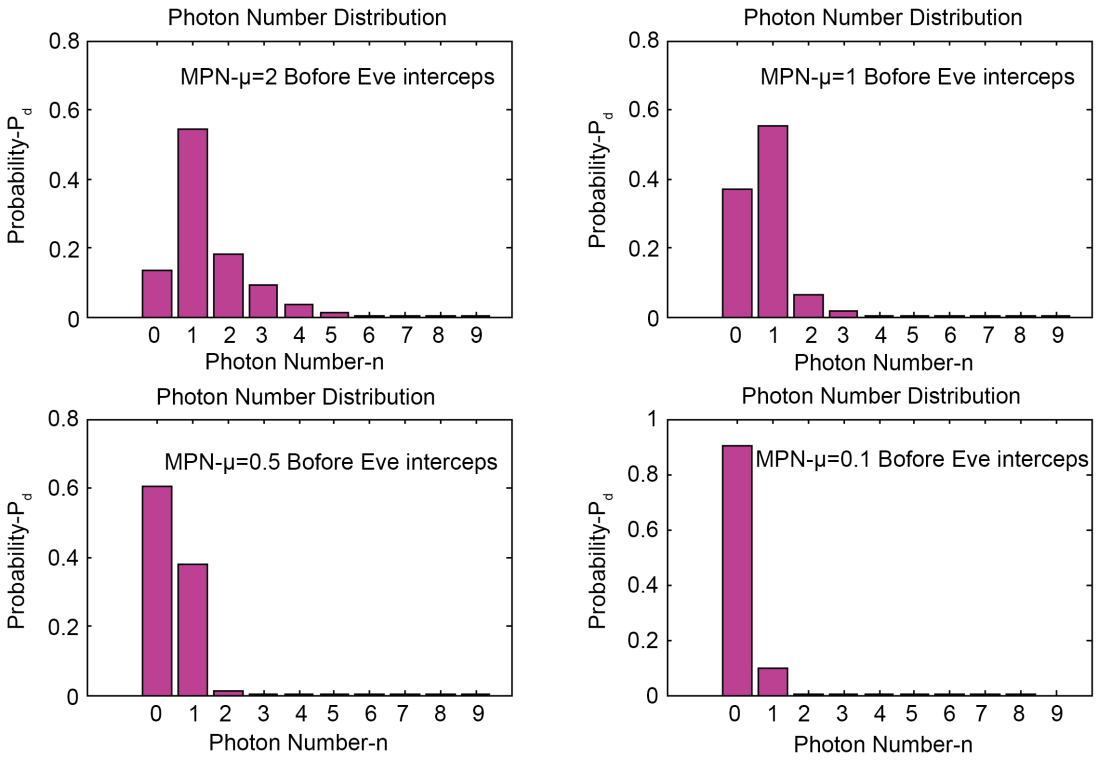

Figure 8. Photon number distribution after a photon intercepted by Eve in a multiphoton pulse
图 8. Eve 截取多光子脉冲中的一个光子后的光子数分布

由(10)可以看出，要提高光子数检测结果的准确度，必须选取合适的端口数 N，尽力减小暗计数率为 P_{dark}，并限制门脉冲的宽度 τ。

综上所述，通过图 6 所示的快速单光子探测器来检测光子数的分布，在(10)所容许的范围内分析其是否偏离泊松分布，可以检测是否存在 Eve 的“光子计数－单光子摄取”攻击；通过分析光子数平均值的变化，可以检测是否存在 Eve 的光子数分离器(PNS)攻击。如果检测出没有 Eve 的存在，原则上可以提高发送脉冲的平均光子数 μ 在 1~2 的水平，以减少空脉冲的数量，将量子密钥分配的码率提高一个数量级；还可以在纠错的基础上，不用再进行密钥增强，以充分利用成功获得的量子比特，进一步提高密钥分配的码率。

如果采用图 2 所示的超导 TES 单光子探测器来检测脉冲中的光子数，由于其很低的暗计数率，因此检测准确度相较于(10)式将大为提高。当然这时 QKD 系统的工作频率将受到 TES 探测器响应时间的限制。

4. 结语

超导 TES 单光子探测器由于具有极低的暗计数率、很高的探测效率、可分辨光子数及可实现光子能量的分辨，因此可对脉冲中所包含的光子数进行准确检测。用于光纤通信波段的量子密钥分配系统中的以 InGaAs/InP 为材料的 SAGM 型 APD 为核心的单光子探测器尚难以直接进行光子数检测。多 APD 与多端口分束器相结合，可以对弱相干光脉冲中的光子数进行统计检测，由此确定 QKD 系统中是否存在窃听者攻击。基于光子数检测，在保证安全性的前提条件下，可将发送的光脉冲中的平均光子数提高一个量级，使 QKD 系统的码率得以提高。

参考文献 (References)

[1] Hwang, W.Y. (2003) Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*, **91**, 057901. https://doi.org/10.1103/PhysRevLett.91.057901

[2] Gottesman, D., Lo, H.K., Lutkenhaus, N. and Preskill, J. (2004) Security of Quantum Key Distribution with Imperfect Devices. *Quantum Information & Computation*, **4**, 325-360. https://doi.org/10.1109/ISIT.2004.1365172

[3] Wang, X.-B. (2005) Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Physical Review Letters*, **94**, 230503. https://doi.org/10.1103/PhysRevLett.94.230503

[4] Lo, H.-K., Ma, X. and Chen, K. (2005) Decoy State Quantum Key Distribution. *Physical Review Letters*, **94**, 230504. https://doi.org/10.1103/PhysRevLett.94.230504

[5] Lo, H.-K. and Chau, H.F. (1999) Unconditional Security of Quantum Key-Distribution over Arbitrarily Long Distances. *Science*, **283**, 2050-2056. https://doi.org/10.1126/science.283.5410.2050

[6] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. and Makarov, V. (2010) Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination. *Nature Photonics*, **4**, 686-689. https://doi.org/10.1038/nphoton.2010.214

[7] Xu, F., Qi, B. and Lo, H.-K. (2010) Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System. *New Journal of Physics*, **12**, 113026. https://doi.org/10.1088/1367-2630/12/11/113026

[8] Lo, H.-K., Curty, M. and Qi, B. (2012) Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, **108**, 130503. https://doi.org/10.1103/PhysRevLett.108.130503

[9] Ma, X. and Razavi, M. (2012) Alternative Schemes for Measurement-Device-Independent Quantum Key Distribution. *Physical Review A*, **86**, 062319. https://doi.org/10.1103/PhysRevA.86.062319

[10] Peng, C.-Z., Zhang, J., Yang, D., Gao, W.-B., Ma, H.-X., Yin, H., Zeng, H.-P., Yang, T., Wang, X.-B. and Pan, J.-W. (2007) Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding. *Physical Review Letters*, **98**, 010505. https://doi.org/10.1103/PhysRevLett.98.010505

[11] Rosenberg, D., Harrington, J.W., Rice, P.R., Hiskett, P.A., Peterson, C.G., Hughes, R.J., Lita, A.E., Nam, S.W. and Nordholt, J.E. (2007) Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. *Physical Review Letters*, 98, Article ID: 010503. https://doi.org/10.1103/PhysRevLett.98.010503

[12] Liu, Y., Chen, T.-Y., Wang, J., Cai, W.-Q., Wan, X., Chen, L.-K., Wang, J.-H., Liu, S.B., Liang, H. and Yang, L.

(2010) Decoy-State Quantum Key Distribution with Polarized Photons over 200 km. *Optics Express*, **18**, 8587-8594. https://doi.org/10.1364/OE.18.008587

[13] Liu, Y., Chen, T.-Y., Wang, L.-J., Liang, H., Shentu, G.-L., Wang, J., Cui, K., Yin, H.-L., Liu, N.-L. and Li, L. (2013) Experimental Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, **111**, Article ID: 130502. https://doi.org/10.1103/PhysRevLett.111.130502

[14] Fukuda, D., Damayanthi, R.M.T., Yoshizawa, A., Zen, N., Takahashi, H., Amemiya, K. and Ohkubo, M. (2007) Titanium Based Transition Edge Microcalorimeters for Optical Photon Measurements. *IEEE Transactions on Applied Superconductivity*, **17**, 259-262. https://doi.org/10.1109/TASC.2007.897393

[15] Martinis, J.M., Hilton, G.C., Irwin, K.D. and Wollman, D.A. (2000) Calculation of TC in a Normal-Superconductor Bilayer Using the Microscopic-Based Usadel Theory. *Nuclear Instruments and Methods in Physics Research Section A*, **444**, 23.

[16] Zhang, Q.-Y., Dong, W.-H., He, G.-F., Li, T.-F., Liu, J.-S. and Chen, W. (2014) Review on Superconducting Transition Edge Sensor Based Single Photon Detector. *Acta Physica Sinica*, **63**, Article ID: 200303.

[17] Miller, A.J., Nam, S.W., Martinis, J.M., *et al*. (2003) Demonstration of a Low-Noise Near-Infrared Photon Counter with Multiphoton Discrimination. *Applied Physics Letters*, **83**, 791-793. https://doi.org/10.1063/1.1596723

[18] Zhang, Q., Liu, J., Dong, W., Wang, T., He, G., Li, T., Zhou, X. and Chen, W. (2014) Design and Fabrication of Superconducting Transition Edge Sensor Bolometers with Background Limited Noise Performance. *Chinese Science Bulletin*, **59**, 2292. https://doi.org/10.1007/s11434-014-0338-y

[19] Ribordy, G., Gisin, N., Guinnard, O., *et al*. (2004) Photon Counting at Telecom Wavelengths with Commercial InGaAs/InP Avalanche Photodiodes: Current Performance. *Journal of Modern Optics*, **51**, 1381-1398.

[20] Lacaita, A., Zappa, F., Cova, S., *et al*. (1996) Single-Photon Detection beyond 1 m: Performance of Commercially Available InGaAs/InP Detectors. *Applied Optics*, **35**, 2986-2996. https://doi.org/10.1364/AO.35.002986

[21] Prochazka, I., Hamal, K. and Spoko, B. (2004) Recent Achievements in Single Photon Detectors and Their Applications. *Journal of Modern Optics*, **51**, 1289-1313. https://doi.org/10.1080/09500340408235273

[22] Dovrat, L., Bakstein, M., Istrati, D., *et al*. (2012) Simulations of Photon Detection in Silicon Photomultiplier Number-Resolving Detectors. *Physica Scripta*, **T147**, Article ID: 014010. https://doi.org/10.1088/0031-8949/2012/T147/014010

[23] Worsely, A.P., Coldenstrodt-Ronge, H.B., Lun deen, J.S., *et al*. (2009) Absolute Efficiency Estimation of Photon-Number-Resolving Detector Using Twin Beams. *Optics Express*, **17**, 4397-4411. https://doi.org/10.1364/OE.17.004397

[24] Pearlman, A.J., Ling, A., Goldschmidt, E.A., *et al*. (2010) Enhancing Image Constrast Using Coherent States and Photon Number Resolving Detectors. *Optics Express*, **18**, 6033-6039. https://doi.org/10.1364/OE.18.006033

[25] He, B., Wang, J., Yu, B., Liu, Y., Wang, X., Xiao, L. and Jia, S. (2013) Measurement of Multi-Photon Response Time by Using a Single Photon Detector. *Journal of Optoelectronics Laser*, **24**, 758-762.

[26] Achilles, D., Silberhorn, C., Liwa, C., *et al*. (2003) Fiber-Assisted Detection with Photon Number Resolution. *Optics Letters*, **28**, 2387-2389. https://doi.org/10.1364/OL.28.002387

[27] Jiang, L.A., Dauler, E.A. and Chang, J.T. (2007) Photon-Number-Resolving Detector with 10 Bits of Resolution. *Physical Review A*, **75**, Article ID: 062325. https://doi.org/10.1103/PhysRevA.75.062325

[28] Laiho, K., Avenhaus, M., Cassemiro, K.N., *et al*. (2009) Direct Probing of the Wigner Function by Time-Multiplexed Detection of Photon Statistics. *New Journal of Physics*, **11**, Article ID: 043012.

[29] Jian, P., Fu, Y., Yao, L., Shang, X., Lu, Z., Yang, B. and Yu, L. (2008) Quick Single-Photon Detector with Many Avalanche Photo Diodes Working on the Time Division. *Chinese Optics Letters*, **6**, Article ID: 050320. https://doi.org/10.3788/COL20080605.0320

[30] Zheng, L.-X., Wu, J., Zhang, X.-C., Tu, J.-H., Sun, W.-F. and Gao, X.-J. (2014) Sensing Detection and Quenching Method for InGaAs Single-Photon Detector. *Acta Physica Sinica*, **63**, Article ID: 104216.