量子密钥分发虚拟仿真实验

朱宇峰 19307110069

一、 实验目的

1.掌握保密通信的基本原理和流程,理解密钥系统在保密通信系统中的作用和重要地位。

2. 掌握量子密钥分发安全性所依赖的物理原理。

3. 掌握量子密钥分发的基本原理,熟悉典型的量子密钥分发协议,掌握 BB84 协议及其实现方法、密钥分发的基本流程。

4. 加深对量子测量、海森堡不确定性原理等量子力学概念的理解。

二、 实验原理

1. 量子密钥分发

量子密钥分发是利用量子力学特性实现密码协议的安全通信方法。它使通 信的双方能够产生并分享一个随机的、安全的密钥,来加密和解密消息。它常 常被误称为量子密码学,因为它是量子密码学任务中最著名的例子。量子密钥 分发的一个最重要的,也是最独特的性质是:如果有第三方试图窃听密码,则 通信的双方便会察觉。这种性质基于量子力学的基本原理:任何对量子系统的 测量都会对系统产生干扰。第三方试图窃听密码,必须用某种方式测量它,而 这些测量就会带来可察觉的异常。通过量子叠加态或量子纠缠态来传输信息, 通信系统便可以检测是否存在窃听。当窃听低于一定标准,一个有安全保障的 密钥就可以产生了。

量子密钥分发的安全性基于量子力学的基本原理,而传统密码学是基于某 些数学算法的计算复杂度。传统密码学无法察觉窃听,也就无法保证密钥的安 全性。量子密钥分发的安全性是是可以依据信息论证明的,而且它还具有前向 安全性。

量子密钥分发只用于产生和分发密钥,并没有传输任何实质的消息。密钥 可用于某些加密算法来加密消息,加密过的消息可以在标准信道中传输。跟量 子密钥分发最常见的相关算法就是一次性密码本,如果使用保密而随机的密 钥,这种算法是具可证明的安全性。在实际的运用上,量子密钥分发常常被拿 来与对称密钥加密的加密方式,如 AES 这类算法一同使用。

2. 量子密钥交换

量子通信中,消息编码为量子态,或称量子比特;与此相对,经典通信 中,消息编码为比特。通常,光子被用来制备量子态。量子密码学利用量子态 的特性来确保安全性。量子密钥分发有不同的实现方法,但根据所利用量子态 特性的不同,可以分为两大类。

1基于制备和测量的协议:与经典物理不同,测量是量子力学不可分割的组成部分。一般来讲,测量一个未知的量子态会以某种形式改变该量子的状态。这被称为量子的不确定性,它的一些基本结论有维尔纳·海森堡的不确定性原理、信息干扰理论和不可克隆原理。这些性质可以被利用来检测通信过程中的任何窃听(窃听必然需要测量),更重要的是,能够计算被截获消息的数量。2基于纠缠态的协议:两个或更多的量子态能够创建某种联系,使得他们无论距离多远依然要被看作是一个整体的量子态,而不是独立的个体。这被称为量子纠缠。他们之间的联系是,比如,对其中一个量子比特的测量会影响其他量子比特。如果纠缠的量子比特对被通信的双方分别持有,任何对消息的拦截会改变整个系统,使第三方的存在(以及他截获消息的数量)被检测到。

3. BB84 协定及实现过程

在 BB84 协议中,信息的物理载体是单个光子。因此在量子密钥分发实验 中应当使用某种每触发一次就发射且仅发射一个光子的设备作为光源,这样的 设备被称为"单光子光源"。

密钥分发与数据处理:发送方 Alice 制备一系列的光子发送给接收方 Bob,每个光子的偏振态独立随机地从水平偏振态 | → >、竖直偏振态 | ↑ >、右 斜 45 度偏振态 | ノ >和左斜 45 度偏振态 | ヽ > 四个偏振态中选取,如果 Alice 发 送光子的偏振态为水平偏振态 | → > 或者竖直偏振态 | ↑ >,则称 Alice 选择 X 基制备光子,如果 Alice 发 送光子的偏振态是右斜 45 度偏振态 | ノ > 或者左 斜 45 度偏振态 | ヽ >,则称 Alice 选择 Y 基制备光子。



图一: BB84 协议原理示意图

接收方 Bob 与 Alice 完全独立地随机选取 X 基和 Y 基测量 Alice 发送过来 光子的偏振态,并记录下测量到光子的位置信息。Alice 和 Bob 对比测量光子 偏振态所选取的基,即双方仅保留相同的基(Alice 制备基和 Bob 测量基)时 Bob 测量到光子位置的光子偏振态信息,双方选取的基不同时则直接抛弃相关 信息。

Alice 和 Bob 将保留的光子偏振态信息转换成相应的密钥比特信息,即对 比使用的基后保留的光子偏振态按水平偏振态 | → }和右斜 45 度偏振态 | ノ }转换 为比特 "0",竖直偏振态 | ↑ }和左斜 45 度偏振态 | ヽ }转换为比特 "1"。

Alice 和 Bob 通过经典公开信道对上一步中获得的密钥比特进行处理,其 过程主要分成纠错和保密放大来进行,纠错就是使得密钥比特一致,而保密放 大就是将可能泄漏给窃听者的信息剔除掉。实际量子密钥分发时,用两位的 bit 编码表示光子信息,其中个位 bit 代表基矢信息,十位 bit 代表密钥信 息;例如: Alice 端水平偏振编码为 00,垂直偏振编码为 10,右斜 45 度偏振 编码为 01, 左斜 45 度偏振编码为 11;相应的 Bob 端四路探测器探测到信号, 分别也是按照上述编码方式进行编码。 密钥分发的过程中,光子传输探测后, 会得到一系列的这种两位编码的信息数据,如何从这些数据中提取出有用信 息,需要原始数据经过对基、纠错、保密放大等过程,最后得到安全密钥,以 保证密钥的安全性。 当然,考虑到是否存在窃听,需要对系统的每次传输过程进行误码估计。 以保证此次的传输数据有效。Alice 和 Bob 两端传输探测完成后会得到一系列 两位编码的信息数据,首先需要对两端的数据进行对基,再对对基的数据进行 比对,计算出系统的误码率。当误码率低于理论安全界限 11%时,本次传输有 效,继续进行后续处理过程。

三、 实验过程

 打开虚拟仿真实验软件,选择"理想的量子密钥分发虚拟实验(无窃 听)"模块。

2. 收发双方实现约定编码规则。

3. 收发双方各自选择实验器材,搭建实验系统。

发射方:单光子源、四个发射偏振片,透射方向分别为H/V/D/A。

接收方: 四个接收偏振片,透射方向分别为 H/V/D/A 与单光子探测器。

4. 发射方启动单光子源发射单光子,随机选择一个偏振片,记录发射光子的 偏振态数据;接收方随机选择一个偏振片,观测单光子探测器是否检测到单光子 信号,并记录接收光子偏振态数据。

5. 双方比较偏振基准选择情况,若双方偏振基准选择一致,保留测量结果作为密钥比特;若双方偏振基准选择不一致,则放弃这组结果。

6. 重复上述步骤,生成一系列密钥(40组实验以上)。

7. 双方随机选取一定数量密钥进行比较,并检查误码率。

8. 加入窃听者重复上述实验,即窃听者需要随机选取偏振片并记录接收光子的偏振态数据,并根据记录的偏振态数据发射一个相同偏振态的光子,其他步骤 与不存在窃听者时相同。

四、 实验仪器

单光子源、两套四个不同方向的偏振片(分别为 H/V/D/A 方向)和单光子探测器。对于存在窃听者情况,需要两套相同的仪器。

五、 实验记录与分析

首先选择"理想无窃听"模块进行实验,进入实验后选取单光子源和四个 方向不同偏振片作为发射端实验装置,同时选取四个方向不同偏振片和单光子



探测器作为接收端实验装置,并约定编码规则,如图二所示:

图二:编码规则

每次发射一个单光子,并随机选择一个偏振片,共记录四十组数据,将数 据记录到表格中,如图三所示:



接收者随机选择偏振片接收单光子,并根据单光子探测器结果和相应偏振态编码规则记录测量结果。当计数器结果为1时,记录该偏振态对应编码;当计数器结果为0时,记录该与该偏振态正交的偏振态的编码,如图四所示:



图四: 接收并测量单光子偏振态

随后接收者讲测量基准发送给发送者,由发送者判断两人使用的偏振基准 是否一致,判断完成后接收者保留使用相同偏振基准测量的光子所对应的密

- Рительного
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 0
 1
 1
 0
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 <th1</th>
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 <th1</th>
 <th1<
- 钥,并抽取十组密钥发送给发送者进行对比,如图五所示:

图五:保留一致基准下的密钥并检查误码率

经检验误码率为 0%, 说明符合理想情况下(无噪声)无窃听的密钥分发过程, 并放弃已公开密钥, 将未公开的保留密钥作为密钥, 记录下密钥并完成实验, 随后进入"理想有窃听模块"进行实验。

对于"量子密钥分发理想(有窃听)模块",实验步骤大致与无窃听情况 一致。首先约定同样的编码规则,并由发射者随机选取偏振片发射40个单光 子。随后窃听者随机选取偏振片测量光子的偏振态并记录,若检测到光子则发 射相同偏振态的光子,若未检测到光子则发射与之垂直的偏振态下的光子,具 体过程如图六所示:



图六: 窃听过程示意图

随后接收者随机选取偏振片测量光子的偏振态并记录相应的密钥,并将每 个光子的测量基准发送给发送者,由发送者判断选用测量基准是否一致,并返 回判断结果。接收者将一致的偏振基准的光子保留作为密钥,并选取12组密钥 公布核对误码率。判断后误码率为41.7%,则证明窃听者存在,并将这一组密 钥舍弃,并完成实验。

在理想无噪声无窃听的情况下,共有 23 组偏振基准选取一致,且公开的十 组数据误码率为 0%,则剩余的 13 组数据可作为密钥使用;在理想无噪声有窃 听的情况下,当样本数量足够大时,误码率应为 25%。但在实验中选取 12 组数 据公布误码率为 41.7%,原因在于对于接收者和发送者选择相同偏振基准的情 况下,窃听者使用的偏振基准与正确的偏振基准一致的概率小于 50%,同时数 据数量较少,并不能满足大数定律,故导致实验与理论上的误码率有较大差 距。

总体上通过两个理想情况下的量子密钥分发实验,较好模拟了量子密钥分发(无窃听和有窃听)的理想情况,但仍然有以下建议:

1. 增加有噪声情况下的量子密钥分发实验,使得实验更接近于真实情况。

2. 在两个实验中已经默认窃听者知晓光子偏振基准的选取标准以及编码标准,而在实际密钥分发过程中窃听者可能随机选取光子偏振方向测量,而在量子通信过程中可能随机选取电子的自旋方向测量。可以设计实验假设窃听者沿特定方向测量偏振或电子自旋,探究是否会使得误码率超过11%,而理论数值均可通过简单计算得出,结合噪声印象可以更加接近于真实体系。

为使得实验更加接近现实中的密钥分发,应增加发射的光子数1个数量
级以上,以便对误码率的测量更加准确,以此判断是否存在窃听者会更为准确。

六、 实验结论

本实验借助量子密钥分发实验的虚拟仿真平台,对理想情况下量子密钥传 输过程进行模拟,在无窃听情况下误码率为0%,在有窃听情况下误码率为 41.7%,与理论结果较为符合。通过本次虚拟仿真实验,加深了对于量子通信的 认识和测量导致波函数塌缩、海森堡不确定原理和量子不可克隆原理的理解。

物质对 β 射线吸收虚拟仿真实验

朱宇峰 19307110069

一、 实验目的

1. 学习了解 G-M 技术器的原理、特性和使用方法。

2. 了解β射线的性质以及物质对于β射线的吸收规律。

二、 实验原理

1.G-M 计数器:

G-M 计数器由 G-M 计数管、高压电源和定标器三部分组成,如图一所示。 用高压电源提供 G-M 计数管的工作电压,计数管在射线作用下可以产生电脉 冲,而定标器则用来记录计数管所输出的脉冲数。



1 G-M 计数管的结构与基本原理 G-M 计数器玻璃管壳内有圆筒状阴极(金属圆筒或涂于玻璃管内壁的导电物质),在阴极的对称轴上装有丝状阳极,先将管内抽成真空,然后再充以一定量的惰性气体和少量猝灭气体。

在用 G-M 计数器对射线进行测量时,计数管的两电极间要加几百伏至一千 多伏的高压,在管内形成柱状轴对称电场,显然阳极附近电场最强。射线进入 管内,一旦引起气体电离,所产生的电子就在电场作用下加速向阳极运动,在 阳极附近与气体分子发生打出次级电子的碰撞,次级电子同样向阳极运动,也 与气体分子碰撞,打出更多次级电子,这样,在阳极附近引起所谓"雪崩"放 电。在雪崩过程中,由于受激原子的退激和正负离子复合将发射大量紫外光光 子,这些光子将使雪崩区沿阳极丝向两端扩展,从而导致全管放电。雪崩过程 中产生的大量电子迅速运动到阳极并被中和。而大量的正离子,由于质量大, 向阴极运动的速度慢,在阳极附近形成一层"正离子鞘",正离子鞘较缓慢地移 到阴极被中和掉。计数管可以看作一个电容器,上述迁移与中和过程中阳极电 位降低,随之高压电源通过电阻 R (见图 G-M 计数器)向计数管充电,使阳极 电位逐渐恢复,这样就在阳极上得到一个负的电压脉冲。

在雪崩放电过程中,有许多气体分子被激发,它们退激时发射的光子有可 能在阴极表面打出光电子;正离子运动到阴极打在阴极上也有可能打出电子。 这些电子的出现,又会重复上面讨论的过程,再次引起计数管放电。如此看 来,只要引起计数管放电,它就会连续放电。要想通过计数管放电来测量射线 强度,必须在计数管一次放电之后,猝灭跟之而来的连续放电。而计数管中的 猝灭气体的分子能强烈地吸收光子,使光子不能再射到阴极上打出光电子。同 时猝灭气体分子的电离电位低于惰性气体分子的电离电位,惰性气体的正离子 通过与猝灭气体的分子的碰撞,逐渐被转换成了猝灭气体的正离子,这些正离 子在到达阴极中和时,本身分解成小分子,而不再打出电子,从而猝灭气体起 到了猝灭连续放电的作用。

2 G-M 计数管的坪特性 在进入计数管的射线粒子数不变的情况下,定标器 给出的计数率随加在计数管两极上的电压而变。如图二实线所示的计数率与计数管两极电压的关系曲线,称 G-M 计数管的坪特性曲线。

当计数管两极的电压 V 从 0 开始升高时,起 初由于 V 太低,极间电场不够强,不能引起全管 放电,因而输出脉冲幅度小,不能触发定标器, 计数率为 0,当电压上升到某一值 V_A时定标器开 始计数,这个 V_A就称为计数管的起始计数电压或 阈电压。电压超过 V_A以后,随其升高脉冲幅度增 大,能触动定标器的脉冲数增多,计数率迅速增加



待升高到 V_B时只要在计数管中产生一个离子对,就会引起全管雪崩放电,所以此时凡在管内引起电离的粒子都能被定标器记录下来。进一步升高电压,只能增大脉冲幅度,而不再增加脉冲个数,计数率基本保持不变,直至 V_c,此区称为计数管的坪区。

(V_c-V_B)叫做坪长度。实际上,在坪区内随着电压的升高计数率也略有增加,也就是说坪有一定的坡度。这主要因为多次计数增加,计数管灵敏体积 (入射粒子在其内产生电离便能引起雪崩放电的体积)增大,漏记数减少所 致。通常用电压升高一伏计数率的相对增加量定义坪坡度,即坪坡度为:

$$T = \frac{2(n_c - n_b)}{(n_c + n_b)(V_c - V_b)}$$

电压超过 V_c以后,由于每次放电产生的离子数过多,猝灭不完善,多次计数随 电压升高迅速增加,使计数率急剧上升,直至出现连续放电现象。

G-M 计数管的坪特性取决于计数管的结构、材料、制造工艺等。实验中测量的是 G-M 计数器的坪特性,作为计数器的坪特性,除决定于计数管的特性之外,也与定标器灵敏度和甄别阈的选取有关。如果定标器的灵敏度不够高,或选取高的甄别阈,则会使计数器的阈电压升高,坪长缩短,如图二 G-M 计数管坪特性曲线中的虚线所示。

2. 物质对β射线的吸收

当一定能量的 β 射线(即高速电子束)通过物质时,与该物质原子或原子 核相互作用而损失能量,强度会逐渐减弱,即在物质中被吸收。电子与物质相 互作用导致强度减弱的机制主要有三种:

 1. 电离损失:电子与物质原子的核外电子发生非弹性碰撞,使原子激发或 电离。电离损失的能量与入射电子的速度、物质的原子序数、原子的平均激发 能等因素有关。

2. 辐射损失:电子受物质原子核库仑场的作用而被加速,根据电磁理论作加速运动的带电粒子会发射电磁辐射,称为轫致辐射,使电子的部分能量以X射线的形式放出。这主要在能量较高的电子与物质相互作用时发生。辐射损失与物质的 Z²成正比,与入射电子的能量成正比。

3. 多次散射: β 射线在物质中与原子核的库仑场发生弹性散射, 使 β 粒 子改变运动方向,因电子质量小,可能发生比较大角度的散射,还可能发生多 次散射,因而偏离原射束方向,使入射方向上的射线强度减弱。如果散射角超 过 90°,称为反散射。

考虑一束初始强度为 I₀的单能电子束,当穿过厚度为 x 的物质时,强度减弱为 I,强度 I 随厚度 x 的增加而减小且服从指数规律,可表示为:

$$I = I_0 e^{-\mu x}$$

其中 μ 为该物质的线性吸收系数。实验指出,不同物质的线性吸收系数有很大的差别,但随原子序数 Z 的增加,质量吸收系数 $\mu_m = \mu/\rho$ 却只是缓慢地变

化,因而常用质量厚度 $d = \rho x$ 代替线性厚度 x。因而透射强度 I 也可用以下公式计算: $I = I_0 e^{-\mu m d}$ 。

原子核 β 衰变放出高速电子的同时,还放出中微子,因此放出的电子并不 是单一能量的,而是具有各种能量分布的连续能谱,因此 β 射线的吸收曲线并 不精确地服从指数规律。对于典型的 β 衰变,存在一最大能量 Emax,不同的 核发生 β 衰变时,放出的电子能谱的 Emax 值不同,常以 Emax 代表 β 射线的 特征能量,同时某些放射性核素会同时发射集中最大能量不同的 β 射线。通常 定义 β 射线通过吸收物质后,射线强度降低到 $\frac{I}{I_0} = 10^{-4}$ 时,所对应吸收物质厚 度 d 即为 β 射线的射程 R。

若吸收物质是铝,在 β 射线的射程和 β 射线的最大能量之间,当 $R > 0.3 g/cm^2$ 时,有经验公式: E = 1.85R + 0.245,其中 E 为 β 射线的最大能量,单位 MeV。

三、 实验内容

物质对 β 射线的吸收:

1. 了解 G-M 计数管的结构和工作原理,测量其坪曲线,求出坪长度、坪坡度,确定合适的工作电压范围。

2. 测量铝片对 β 射线的吸收曲线, 求出 β 射线的射程和最大能量。

四、 实验仪器

物质对 β 射线的吸收系列实验装置如图三所示,从左到右依次为:自动定标器仿真仪器、计数管仿真仪器、铝盒和铝片以及电离隔离箱仿真仪器(内有放射源)。



五、 实验过程及数据处理

进入虚拟仿真实验平台,学习与放射源有关的安全教育,随后选择物质对 β 射线吸收实验进入实验模块。

1. 测量 G-M 计数管的坪特性:

打开隔离箱,鼠标选取放射源并拖拽到桌面上固定,关闭隔离箱。打开计数管大视图,打开放射源盖子与计数管舱门,将放射源放入计数管舱内,关闭计数管舱门。接着打开自动定标器,并打开高压开关,设定时间为20s,调节电压为250V,启动并开始计数,并将计数值填入表格。随后将电压每次增加10V,并重复上述步骤,记录数据,直至电压升高到500V,过程如图四所示;



图四:不同电压下计数示意图

将计数器示数除以时间,即可求得计数率 n,以电压为横轴,计数率 n 为纵轴作图,即可得到 G-M 计数器的坪曲线,如图五所示。从图中可看出,G-M 计数器的坪曲线大致与理论一致。

当电压小于 270V 时,管内电场较弱,不能 引起全管放电,因而脉冲幅度较小不能触发定 标器;当电压超过 280V 定标器开始计数,随着 电压增大计数率迅速增加,故可以判断 G-M 计 数器的阈电压在 270-280V 之间。当电压升高到 370V 左右,随着电压升高至 460V 计数率变化均



不明显,故认为进入坪区。在这段区间只要在计数管中产生一个离子对就会引起 全管雪崩放电,此时在关内引起电离的离子都能被定标器记录,进一步增大电压 只能增加脉冲幅度而不增加脉冲个数,故计数率基本保持不变。通过简单计算可 得出,坪长度为 90V、坪坡度为1.44×10⁻⁴V⁻¹。坪坡度产生原因在于多次计数 增加、计数管灵敏体积增大以及漏记数减少。当电压超过 460V 并逐渐增大时, 每次放电产生离子数较多,猝灭不完善,多次计数随电压升高迅速增加,使计数 率急剧上升。这一点虽然在图中并不明显,但已经存在该趋势。

2. 测量铝片对 β 射线的吸收曲线:

在之前实验的基础上,根据分析在坪区选取电压为420V,将时间调为300s, 将放射源从 G-M 计数管中取出,放入塑料板,在未放入铝片的前提下测量本底计 数值,测得300s 时间本底计数值为164。随后打开 G-M 计数管,将放射源放入, 不放入铝片,保持工作电压420V,时间300s进行计数,并记录数据。随后保持 其他条件不变,每次放入一片铝片,并计数记录数据。

在 11 组数据记录完成后,可以根据铝片参数计算得出铝片的质量厚度 d, 并可以根据净计数算得计数率。由于射线强度正比于计数率,故可以通过计数率 比值计算*I*/*I*₀。根据公式*I* = *I*₀*e*^{-μmd},将ln (*I*/*I*₀)对质量厚度 d 线性拟合,斜率

即为 $-\mu_m$, 拟合结果如图六所示。其 中相关系数 $R^2 = 0.998$, 线性相关性 良好, 从而证明物质对 β 射线的吸收 与理论相一致。根据理论推导可知, 截距应当为 0, 也落在不确定度范围 内。可以外推得到 β 射线通过铝片的 射程 $R = 1.07 g/cm^2$, 根据经验公式 估算得到 β 射线的最大能量E = 2.224 MeV。



本实验由于是虚拟仿真实验,对于铝片参数的测量不存在误差,G-M计数管 在实验过程中也不受外界环境和具体操作的影响。故实验误差主要来自于G-M计 数器计数上的误差,由于实验探测时间选为300s,计数较大,可以近似认为消除 了涨落对于计数率的影响,从而认为实验结果较为准确。

该虚拟仿真实验对于实际情况模拟程度较高,同时避免了接触放射源对身体 的损害;但实验过程中的系统内部数据记录不规范,对于数据的精度选取不太严 谨,曲线拟合也没有给出相应参数,故在实验过程中重新分析数据并使用 origin 软件绘图。

六、 实验结论

本实验运用 G-M 计数器和放射源, 绘制了 G-M 计数器的坪曲线, 与理论结果大致相符, 同时计算得到坪长度为 90V、坪坡度为 $1.44 \times 10^{-4}V^{-1}$ 。除此之外, 本实验还验证了铝片对 B 射线吸收的理论公式, 计算得到 B 射线通过铝片的射程 $R = 1.07 g/cm^2$,并估算得到 B 射线的最大能量E = 2.224 MeV。