量子密码学阅读报告

姓名：张青铭　　学号 3200105426

所在学院：信息与电子工程学院, 浙江大学
Email: 3200105426@zju.edu.cn

摘要：量子密码术是一种新的重要加密方法，它利用单光子的量子性质，借助量子密钥分配协议可实现数据传输的可证性安全。量子密码理论上具有无条件安全的特性，但由于所采用的量子器件的非理想性，给窃听者带来了新的攻击手段。本文对近年来量子密钥分配协议的发展，从 BB48 协议到测量设备独立的量子密钥分发，再到差分相位量子密钥分发协议做简单的介绍。

一．量子密码学背景介绍

随着科学技术的发展，信息交流已经深入到社会生活的各个角落，各种通信手段形成一张大网，将人们紧密联系在一起。人们对信息交流的依赖性越来越强，对信息交流的安全性要求也越来越高，但过去基于数学理论的经典通信保密机制并不能从根本上保证通信的安全。然而，随着近年来量子物理学的迅速发展，基于量子物理理论的信息保密方法——量子密码学开始出现，这种保密机制从理论角度看可以根本上保证信息的安全。

量子密码学是量子物理学和密码学融合的一门学科，它采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。量子密码的安全性由量子力学原理所保证，它通过量子选择来阻止信息被截取，现在的应用以密钥分配、量子身份认证、量子签名、量子加密算法为主。

二．量子密钥分发基本原理

密钥分发用来在通信双方（Alice 和 Bob）分发一个密钥，后续可以用该密钥安全通信。BB48 协议是第一个量子密钥分发协议，被研究的最多，也最具代表性，在量子密码研究中占有重要地位。在此以 Bennett 和 Brassard 提出的原始协议为例，对量子密钥分发的理论原理进行推导。

BB48 协议使用光子作为量子态的载体，使用 2 组偏振基编码数据。一种为线偏振基（记为“+”），水平偏振状态记为$|\leftrightarrow\rangle$，垂直偏振状态记为$|\updownarrow\rangle$；另一种为圆偏振基（记为“〇”），左旋偏振状态记为$|\nearrow\rangle$， 右旋偏振状态记为$|\searrow\rangle$。在这 2 组基下，比特“ 0 ”分别被编码为$|\leftrightarrow\rangle$和$|\nearrow\rangle$，比特“ 1 ”分别被编码为$|\updownarrow\rangle$和$|\searrow\rangle$。描述光子线偏振和圆偏振的力学量算符不可对易，由 Heisenberg 不确定性原理，这 2 种偏振状态无法被同时确定。

BB48 协议需要一条量子信道和一条经典信道。量子信道可以是光纤或自由空间，经典信道为普通的公共信道，安全性不需考虑。这 2 种信道都允许第三方（Eve）监听。

BB48 协议工作过程如下：

1）Alice 对于某个安全参数n，随机选择稍多于$4n$个比特，对每个比特随机选取线偏振基或圆偏振基进行编码，并将编码后的光子序列通过量子信道发送给 Bob；

2）Bob 收到光子序列后，随机选取线偏振基和圆偏振基对光子序列进行测量。

3）Bob 与 Alice 通过经典信道联系，对比他们所选择的基序列，舍弃选择不同基的比特，一般而言，他们将得到稍多于$2n$个比特；

4）Alice 选择n个比特与 Bob 对比检查是否有第三方监听，如果错误率超过某一个阈值，则放弃本次协议（监听会造成对量子态的干扰，从而显著增大错误率）；

5）Alice 和 Bob 对剩下的n个比特执行密钥纠错和安全性增强，得到最终的密钥。

BB48 协议的工作过程可用下图所示的例子直观描述：

Alice chooses random bits	0	0	1	0	1	1	0	1	0	1	1	0
Alice chooses encoding basis randomly	+	○	○	+	○	+	○	+	+	○	+	○
Alice sends quantum bits	|↔⟩	|↙⟩	|↘⟩	|↔⟩	|↘⟩	|↕⟩	|↙⟩	|↕⟩	|↔⟩	|↘⟩	|↕⟩	|↙⟩
Bob chooses measuring basis randomly	+	+	○	+	○	○	+	+	○	+	○	○
Bob's measuring result①	|↔⟩	|↔⟩	|↘⟩	|↔⟩	|↘⟩	|↙⟩	|↕⟩	|↕⟩	|↘⟩	|↔⟩	|↘⟩	|↙⟩
Alice and Bob compare their basis	√	×	√	√	√	×	×	√	×	×	×	√
Alice and Bob keep the bits from the same basis	0		1	0	1			1				0
Comparison	Half of the reserved bits are compared, and the protocol is aborted when the error rate exceeds the threshold											
Error correction	Alice and Bob perform error correction on the remaining bits											
Security enhancement	Alice and Bob enhance the security of the corrected bits to get the final key											

三．量子密钥分发协议的发展

1.BB48 存在的不足

Bennett 和 Brassard 提出的 BB84 量子密钥分配协议从理论上被证明是绝对安全的，然而在实际中量子密钥分配所采用的具体实现方案，以及所采用的量子器件的非理想性，给窃听者带来了新的攻击手段。是否能够从理论上排除掉所有可能的攻击手段？Mayers 和姚期智在 *Quantum cryptography with imperfect apparatus* 中提出了现在被称作“设备无关”的思想：是否有可能仅对设备做最基本的空间上需要分离的假定，除此以外对设备不做任何限制，其安全性完全由对设备本身的测试来完成。这一思想突破了安全性对系统设备的依赖性, 成为最近十几年量子密码学界研究的重点。

2. 测量设备独立的量子密钥分配

经过仔细分析，Lo 等人发现量子密钥分配系统的侧信道大多出现在测量端，基于此，他们提出了一个简单的解决方案来解决这个问题，即测量设备独立的量子密钥分配。

MDI-QKD 协议的基本装置如下。Alice 和 Bob 在不同 BB84 偏振状态下制备相位随机化弱相干脉冲（WCP），该偏振状态通过偏振调制器（Pol-M）为每个信号独立随机选择。诱饵状态使用强度调制器（诱饵 IM）生成。在测量设备内部，来自 Alice 和 Bob 的信号在 50:50 的分束器（BS）处发生干扰，该分束器的两端都有一个偏振分束器（PBS），将输入光子投影到水平（H）或垂直（V）偏振状态。使用四个单光子探测器来检测光子，并公开宣布检测结果。成功的钟态测量对应于精确地观察到两个被触发的探测器（与正交极化相关）。在D_{1H}和D_{2V}中或在

D_{1V}和D_{2H}中单击，表示投影到钟形态$|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$，而在$D_{1H}$和$D_{1V}$中或在$D_{2V}$和$D_{2V}$中单击，则显示到钟形态的投影$|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$。

两相随机 WCP 之间的 Hong-Ou-Mandel 干扰。平均光子数为每脉冲 0.1。在不同的时间延迟下记录符合率。误差条显示由于数据大小有限导致的统计波动。

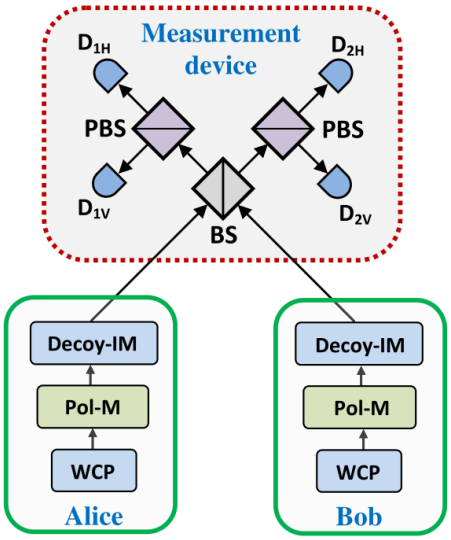

Fig.1 MDI-QKD 协议的基本装置

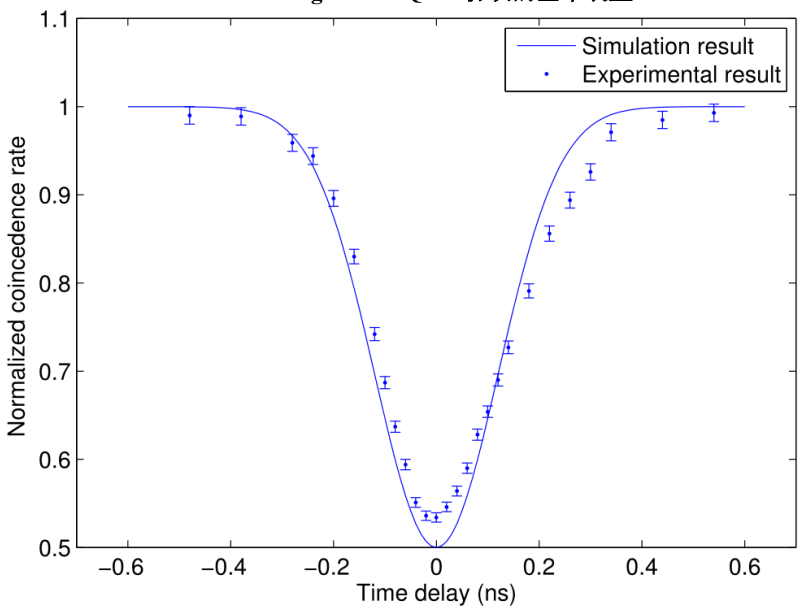

Fig.2 两相随机 WCP 之间的 Hong Ou-Mandel 干扰

它不仅消除了所有探测器侧通道，而且与传统激光器的安全距离增加了一倍。该方案可以用低检测效率和高损耗信道的标准光学元件实现。与之前的全设备独立 QKD 解决方案相比，该想法的实现不需要近单位探测效率的探测器与量子比特放大器（基于隐形传态）或脉冲光子数的量子非破坏性测量相结合。此外，它的密钥生成率比基于全设备无关 QKD 的密钥生成率高出许多数量级。

3. 差分相位量子密钥分配协议(RRDPS).

实验表明, 测量仪器无关量子密钥分配方案原则上是可行的。但是, 实际系统需要两个单光子探测器同时响应, 因此其安全密钥生成效率十分低下, 目前离实际可用还有一定距离。

2014 年 Sasaki 等发表的文章 *Practical quantum key distribution protocol without monitoring signal disturbancez* 中提出了 Round-Robin 差分相位量子密钥分配协议，该协议不需要顾及光源的抖动，且容忍的误码率很高，这在环境干扰特别大的特殊环境下或许具有优势。

现对该方法讨论如下：

1）Bob 的替代测量选择

设$+_L$表示求和模 L。当单光子输入状态$\hat{\rho}$被馈送到测量M时，Bob 宣布$\{\{k, k+_L r\}$，并以概率$\langle k,s|\hat{\rho}|k,s\rangle$获得$s_B = s$，其中$|k,s\rangle \coloneqq |k\rangle + (-1)^s|k+_L r\rangle)/\sqrt{2}$。当$s \neq s_k \oplus s_{k+}r$时，$\langle k,s \mid \Psi_1 \rangle = 0$，Bob 的猜测$s_B$始终等于$s_A$，如果他收到状态$|\psi_1\rangle$。则$\{i，j\}$的概率计算为$P(\{i,j\}) = [P(i) + P(j)]\left[\delta_{i+_L r,j} + \delta_{j+_L r,i}\right]/2$，其中，$P(k) = \langle k|\,\rho|\,k\rangle$是在第 k 个脉冲中发现光子的概率。

2）安全密钥速率的推导

随机相移δ使 Alice 能够用以$v > v_{th}$来标记每一轮。我们假设该标记部分（最多Ne_{src}/Q位）完全泄漏给 Eve，导致方程：

$$G = N\left[1 - h(e_{\text{bit}}) - \frac{e_{\text{src}}}{Q} - \left(1 - \frac{e_{\text{src}}}{Q}\right)h\left(\frac{v_{\text{th}}}{L-1}\right)\right]$$

产生$-e_{src}/Q$项。

对于未标记部分，可以显示序列$S_1 S_2 \cdots S_L$相当于$\{|0\rangle, |1\rangle\}$基测量L个量子位的结果，L个量子位是在一种状态下制备的，如果它们是在共轭$\{|+\rangle, |-\rangle\}$基中测量的，则在$|-\rangle$状态下发现的量子位不超过n个。然后，在对量子位i和j进行受控非运算后，通过对量子位j的$\{|0\rangle, |1\rangle\}$基测量给出关键位$s_{\text{A}} = s_i \oplus s_j$。可以表明，在状态$|-\rangle$中找到量子位$j$的概率最多为$n$次，从而导致方程

$$G = N\left[1 - h(e_{\text{bit}}) - \frac{e_{\text{src}}}{Q} - \left(1 - \frac{e_{\text{src}}}{Q}\right)h\left(\frac{v_{\text{th}}}{L-1}\right)\right]$$

中的剩余项。

2015 年潘建伟等发表了 *Experimental passive round-robin differential phase-shift quantum key distribution*，其中完成了改造的 RRDPS 方案的实验验证, 该实验系统在 50 km 距离, 误码率为 29% 的情况下仍能够生成安全的密钥。

但这种协议方式仍不是绝对安全的，在针对量子协议的安全性分析和攻击方法方面，如今提出了一种截获——重发攻击和以及利用量子隐形传态进行攻击，证明了该方法仍存在不足和完善的空间。

四．总结与展望

基于量子力学的机制，量子密码学有着先天的优势。从理论上来看，量子密码学有着无条件安全性的特点，这是信息安全领域理想的目标之一。然而在实际应用时，由于设备缺陷、噪声影响等因素，还存在许多安全问题，需要从理论和实践两个层面去解决。此外在效率、易用性等方面也存在诸多问题有待解决。在量子密码学安全方案设计方面， 同经典密码一样，由于很难穷举所有攻击方式，仅进行启发式分析是远远不够的，必须考虑可证安全理论。

而从最初的 BB48 到测量设备独立的密钥分配，再到差分相位量子分配，甚至如今针对量子隐形传态的攻击研究相应的分配协议，有关理论仍在不停进步中。

但对于上述理论，除了老师课上讲过的 BB48，其他我都只能理解其中的大概，对于其中的公式推导基本都是一头雾水。某种意义上也说明了该领域从 Bennett 和 Brassard 开始已经向前走了很长的距离。

量子力学有其独特的机制，如量子纠缠、未知量子态不可克隆等，其中的理论潜能还有很大一部分能够被我们所挖掘。而在将来，随着计算机算力的不断提升，要对付拥有量子计算能力的密码破译者，量子密码体制可能是唯一的选择。

参考文献：

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. arXiv preprint arXiv:2003.06557, 2020.

[2] Mayers D, Yao A. Quantum cryptography with imperfect apparatus[C]//Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280). IEEE, 1998: 503-509.

[3] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical review letters, 2012, 108(13): 130503.

[4] Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance[J]. Nature, 2014, 509(7501): 475-478.

[5] Guan J Y, Cao Z, Liu Y, et al. Experimental passive round-robin differential phase-shift quantum key distribution[J]. Physical review letters, 2015, 114(18): 180502.