Literature Review On Quantum Cryptography

by

Mingke Wang

Bachelor

School of Electronic Information
and Electrical Engineering

Shanghai Jiao Tong University

Shanghai, China

2019

Acknowledgments

This thesis is the final project of class EE378, and the main topic I choose is quantum cryptography.

Abstract

In this artical, I mainly talk about what is quantum, how does it related to transmission cryptography, and the drawback of it.

Contents

1. Introduction

1.1 Overview

“最近的 16 公里量子态隐形传输的成功试验表明, 中国将有能力建立起卫星与地面的安全量子通信网络。”——美国《时代周刊》在“爆炸性新闻”栏目中以“中国量子科学的飞跃”为题, 对 2010 年中国科技大学与清华大学合作完成的 16 公里量子态隐形传输试验进行了评论。相比于经典通信, 量子通信究竟有哪些优势, 有哪些应用, 源于何种原理以及方法和技术手段等, 无疑是大家所关心的。我们将在此介绍量子通信的基本概念与方法、技术现状, 以及未来应用前景。量子通信的基本思想主要由 Bennett 等于 20 世纪 80 年代和 90 年代起相继提出, 主要包括量子密钥分发 (quantum key distribution, QKD)Bennett and Brassard 2014 和量子态隐形传输 (quantum teleportation)Bennett, Brassard, et al. 1993。量子密钥分发可以建立安全的通信密码, 通过一次一密的加密方式可以实现点对点方式的安全经典通信。这里的安全性是在数学上已经获得严格证明的安全性, 这是经典通信迄今为止做不到的。现有的量子密钥分发技术可以实现百公里量级的量子密钥分发, 辅以光开关等技术, 还可以实现量子密钥分发网络。量子态隐形传输是基于

量子纠缠态的分发与量子联合测量, 实现量子态 (量子信息) 的空间转移而又不移动量子态的物理载体, 这如同将密封信件内容从一个信封内转移到另一个信封内而又不移动任何信息载体自身。这在经典通信中是无法想象的事。基于量子态隐形传输技术和量子存储技术的量子中继器可以实现任意远距离的量子密钥分发及网络。

超级计算机的快速发展和量子计算机的前景对通信的安全性构成越来越严重的威胁。利用量子密码学的原理，量子通信提供了可证明的通信安全性，并且是应对此类威胁的有希望的解决方案。量子密码学不依赖对手的计算机能力，但由量子物理学定律绝对地保证，尽管它处于起步阶段，但有必要在学术界，工业界和社会中激励研究工作通常，将其作为安全性的可靠替代方案。

毫无疑问，QKD 在使用量子信息进行密码学方面引起了人们的关注（事实上，“量子密码学”一词经常与 QKD 等同，这是一种误解），然而，量子信息在密码学中还有许多其他用途。此外，量子信息打开了密码领域，允许仅使用经典信息就无法实现的功能，例如不可克隆的量子货币。但是，我们注意到，密码学中使用量子信息有其局限性和挑战。例如，我们知道仅量子信息不足以实现信息理论上安全的比特承诺；并且一种称为倒带的证明技术（通常用于建立协议的零知识特性）不会直接延续到量子世界，而必须根据量子信息重新进行研究。

2. 量子

2.1 状态空间

位是经典信息处理的基本信息单元。在量子信息处理中，对应的单位是 qubit，在数学上由二维复数向量空间中长度为 1 的向量描述。使用物理学上的符号来表示代表量子态的矢量，将矢量封装在 ket 中。

2.2 幺正演化与电路

量子系统的基本演化是通过保持标准的线性运算来描述的。形式上，这些运算可以表示为 unit 复矩阵。

量子算法通常被描述为由通用集合中的基本量子门组成的电路（而非量子图灵矩阵机)。

2.3 测量

除了幺正演化之外，指定了一种称为测量的操作，在最简单的情况下，该操作需要一个 qubit 并输出一个经典位

进一步规定，在测量过程之后，量子系统崩溃到测量的结果。因此，量子态受到干扰，成为经典态：任何进一步的测量都有确定性的结果。已经根据标准描述了度量；当然，可以根据任意基础描述测量。结果的概率可以通过首先应用相应的基础变化，然后进行标准基础测量来计算。实际上可以更一般地描述测量：可以描述量子系统的严格子集的测量结果-描述结果的数学形式主义使用密度矩阵形式主义，在此不做描述。Broadbent and Schaffner (2016)

2.4 量子不可复制性

量子信息的最基本特性之一是，从总体上讲，物理上不可能克隆量子系统（即，没有物理过程将单个量子系统作为输入，并输出其输入的两个相同副本）。从量子操作的线性可以得到一个简单的证明。5 在直觉上，这个原理几乎存在于所有量子密码学中，因为它阻止了给定量子位系统描述的经典重构。例如，给定单个副本 α 和 β，因为测量会干扰状态。但是，在形式层面上，通常使用通用的 qubit $\alpha|0\rangle+\beta|1\rangle$，因此不可能“提取”需要更复杂工具的完整经典描述。证明量子密码协议的安全性。

2.5 量子纠缠与非局域性

量子力学的一个有悖于直觉的特征就是量子纠缠，这是一种物理现象，当量子粒子以无法单独描述每个粒子的量子态的方式工作时，就会发生这种现象。这种纠缠状态的一个简单示例是状态 $\frac{(|00\rangle_{AB}+|11\rangle_{AB})}{\sqrt{2}}$ 中的两个量子位。当爱丽丝测量她 qubit（在系统 A 中），她获得一个随机位 $a \in \{0,1\}$ 作为结果，并且她的 qubit 崩溃到观察到的状态 $|a\rangle_B$。同时，鲍勃的量子位（在系统 B 中）也崩溃为 $|a\rangle_B$，因此，鲍勃随后进行的测量得出了相同的结果 $b = a$。重要的是要意识到，鲍勃一侧的状态崩溃与爱丽丝的测量同时发生，但不允许玩家将信息从爱丽丝发送到鲍勃。

它只是为 Alice 和 Bob 提供了一个共享的随机位。通常，量子纠缠并不与相对论的基本非信号原理相矛盾，该原理指出，没有信息能够以比光速更快的速度传播。

2.6 量子密码构造

许多量子密码协议具有显着的特征，即基于称为共轭编码的非常简单的量子信息模式。由于其在量子密码学中的最重要意义，我们首先提出这一概念。然后，我们将说明共轭编码是量子货币 QKD，从遗忘转移到比特承诺的量子缩减，有限量子存储模型和委托量子计算的重要组成部分。本节中涉及的其他主题是量子硬币翻转和与设备无关的加密技术。

3. Quantum Key Distribution

迄今为止，QKD 是量子信息在密码学中最成功的应用。到目前为止，QKD 是大量调查的主要主题。

3.1 Comparsion with Traditional Cryptography

在传统的公共密钥密码学中，尽管两个用户之间没有任何初始共享的秘密信息，但陷阱门功能用于从被动窃听者隐藏两个用户之间的消息含义。

在量子公共密钥分发中，量子通道不是直接用于发送有意义的消息，而是用于在最初不共享秘密信息的两个用户之间传输随机位的提供，以这种方式，用户可以通过随后的协商在一个普通的非量子通道上进行被动窃听，可以很容易地判断原始量子传输是否在传输过程中受到干扰，就像窃听者那样（强迫窃听是主动的，这是量子通道的特质）。如果传输没有受到干扰，则他们同意以众所周知的方式将这些共享机密比特用作一次性密码，以掩盖后续有意义的通信的含义，或者用于需要共享机密的其他密码应用程序（例如，身份验证标签）随机信息。如果传输受到干扰，他们将放弃并重试，推迟任何有意义的通信，直到他们成功通过量子信道传输了足够的随机比

特以用作一次性填充。

3.2 Protocol

一个用户（“Alice”）选择一个随机的位串和一个随机的极化基序列（直线或对角线）。然后，她向另一位用户（“Bob”）发送一列光子，每个光子代表为该位位置选择的基础上的字符串的一位，水平或 45 度光子代表二进制零，垂直或 135-度光子代表二进制 1。

当 Bob 接收光子时，他决定独立于每个 Alice，对每个光子随机地测量光子的直线极化还是对角极化，并将测量结果解释为二进制零或一。如前一节所述，当尝试测量对角光子的直线偏振时，会产生随机答案，并且所有信息都会丢失，反之亦然。因此，Bob 仅从他检测到的一半光子中获得有意义的数据，这些光子他猜出了正确的极化基础。实际上，有些光子在传输中会丢失或无法由 Bob 的效率不佳的检测器计数，从而使 Bob 的信息进一步恶化。

该协议的后续步骤在一个普通的公共通信信道上进行，假定该信道易于被窃听，但不易于消息的注入或更改。Bob 和 Alice 首先通过公开交换消息来确定成功接收了哪些光子，以及以正确的基础接收了哪些光子。如果量子传输没有受到干扰，即使从未在公共信道上讨论过该数据，Alice 和 Bob 也应就这些光子编码的比特达成一致。换句话说，这些光子中的每一个可能携带一点 Alice 和 Bob 所知的随机信息（例如，直线光子是垂直还是水平）。

由于量子传输中直线形光子和对角线光子的随机混合，任何窃听都存

在改变传输率的风险，从而使鲍勃和 Alice 在他们认为应该同意的某些位上产生分歧。具体来说，可以证明窃听者在传输光子时没有任何测量结果，窃听者只有在完成测量后才获悉光子的原始基础，才能产生超过 $\frac{1}{2}$ 的预期比特关于由该光子编码的密钥位的信息；并且，如果这样的测量产生了 b 位的预期信息（$b \leq \frac{1}{2}$），则如果测量的光子必须引起概率至少为 $\frac{b}{2}$ 的分歧。，或尝试对其进行伪造，随后将在其原始基础上重新进行测量。（例如，当窃听者以直线方式测量并重新传输所有被拦截的光子，从而了解一半光子的正确极化并在其中的 $\frac{1}{4}$ 以后在原始基础上重新测量的信息中引起分歧时，就会发生这种最佳折衷。）Bennett and Brassard (2014)

因此，Alice 和 Bob 可以通过以下方式测试是否进行了监听公开比较他们认为应该同意的一些比特，尽管这当然牺牲了这些比特的保密性。在此比较中使用的位位置应该是正确接收的位的一个随机子集（例如三分之一），这样，窃听多个光子就不可能逃脱检测。如果所有比较都同意，那么 Alice 和 Bob 可以得出结论，量子传输没有明显的窃听，并且在相同基础上发送和接收的其余比特中的那些也同意，并且可以安全地用作 one-time pad，以便随后通过公共渠道进行安全通信。当 one-time pad 耗尽时，将重复该协议以在量子通道上发送新的随机信息主体。

如果 Alice 和鲍勃事先就一个小秘密密钥达成了共识，则该方案中的公共（非量子）信道免于主动窃听的需求便可以放宽，他们将其用于创建 Wegman–Carter 身份验证标签Goldreich, Micali, and Wigderson 1991，以用于其消息传递。公共频道。更详细地讲，Wegman-Carter 多消息身份验证方案使用一个小的随机密钥为任意大的消息生成依赖于消息的“标签”（类似于校验和），以使窃听者不知道该密钥能够生成任何其他有效消息-标记对的

可能性很小。因此，标签提供了证明消息是合法的证据，并且不是由不知道密钥的人生成或更改的。（密钥位已在 Wegman-Carter 方案中逐渐用尽，在不损害系统可证明的安全性的情况下无法重用；但是，在本应用中，这些密钥位可以由成功通过量子信道传输的新鲜随机位代替。）窃听者仍然可以通过抑制公共信道中的消息来阻止通信，当然，他可以通过抑制或过度干扰通过量子信道发送的光子来阻止通信。但是，无论哪种情况，Alice 和 Bob 都将很可能得出结论，即他们的秘密通信被压制了，而事实上却并非如此，他们不会误认为他们的通信是安全的。

3.3 实用化点对点量子通信

该方法要求随机改变相干态脉冲强度而测出单光子计数率. 以此为输入参数提炼出最终码. 采用该法所得最终码, 其安全性与用理想单光子源所获最终码等价. 对于弱相干态光源所发射的脉冲, 有一部分是多光子脉冲, 一部分是单光子脉冲. 诱骗态方法的主要功能是测算在接受端 Bob 的探测结果 (初始码) 中, 有多少起源于发射端 (Alice 端) 光源的单光子脉冲, 多少起源于发射端的多光子脉冲. 基于这个至关重要的参数, 就可以提炼出安全的最终码, 其安全性等同于只采用了由发射端单光子脉冲产生的那部分初始码而抛弃了多光子脉冲产生的那部分初始码. 在安全性方面最后的效果就等同于使用了理想单光子源.

2003 年, 美国西北大学黄元瑛博士提出了在量子密码理论实用化上具有革命性的 Decoy-State 思想 Hwang 2003 用以解决光子数分离攻击. 可是黄的结果尚不能立即实用于现有真实系统, 清华大学王向斌教授于 2005 年的

理论研究 X. B. Wang 2005 表明, 采用三强度随机切换的诱骗信号量子密码方案可以准确侦察出任何窃听行为, 包括所谓的光子数分离攻击, 并可立即实用于现有真实系统, 其中包含通道噪声, 大损耗等. 三强度诱骗信号方法可以让合法用户计算出至关重要的参量: 多光子脉冲份额的上限值. 有此上限值, 结合前人理论结果, 便可以获得绝对安全的最终码. 由该理论给出的关键计算公式, 诱骗态方法具有了立即的实用价值 (见图 4). 这也使得量子密钥分发有可能成为整个量子信息领域最先走入社会实用的分支.

诱骗态方法的首个实验由清华大学和中国科技大学等单位的联合团队完成 Peng et al. 2007, 这也成为历史上首次超过 100 km 的安全量子密钥分发. 同一时期的实验还有美国橡树岭国家实验室与美国国家标准局团队的合作实验、维也纳大学等单位的实验等. 此后, 中国科技大学结合光开关技术, 把诱骗态方法用于量子网络, 先后实现了 3 节点与 5 节点的量子网络安全通信 Chen, Liang, et al. 2009. 迄今为止, 基于诱骗态方法的量子密钥分发已经至少获得世界主要研究机构近 20 个公开发表的在不同条件下的实验证实. 尽管诱骗态方法未必就是唯一方法, 由于其安全性和实用性, 事实上, 诱骗态方法已经成为当前量子密码走向实际应用的最重要方法. 近年来, 中国科学家们致力于参与这一主战场的研究, 在实验与理论方面取得国际领先的广泛成果. 自清华—中科大联合团队 2007 年在国际上率先利用诱骗态手段实现了绝对安全距离超过一百公里的量子密钥分发 Peng et al. 2007 以来, 中国科技大学潘建伟小组又于 2010 年率先实现绝对安全距离达 200 km 的量子密钥分发, 为目前国际上绝对安全量子密钥分发最远距离. 他们还采用光开关技术, 于 2008 年 10 月初完成了诱骗态量子密钥分发的 “光量子电话网” Chen, Liang, et al. 2009(此前国内外其他小组的量子密码网络的实验因为没

有采用诱骗态方法而不安全). 清华大学王向斌小组则通过系统化的理论研究已经证明即便光源强度有较大涨落诱骗态方法依然有效, 给出了相关安全成码的计算公式

3.4 量子网络通信

辅以光开关技术后, 诱骗态方法还可用以实现量子通信网络. 由于没有量子存储器, 这种网络的量子密钥分发距离不能超越点对点的量子密钥分发距离. 然而, 网络上的任何两个用户可以通过光开关切换实现量子密钥分发. 我国在 2009 年实现了 3 节点的链状量子通信网络 Chen, Liang, et al. 2009, 为世界上首个基于诱骗态方案的量子语音通信网络系统, 实现了实时网络通话和三方对讲功能, 演示了无条件安全的量子通信的可实用化. 此成果很快被美国《Science》杂志以“量子电话”为题进行了报道, 亦被欧洲物理学会《物理世界》以“中国诞生量子网络”为题做了专题报道. 随后, 又实现了 5 节点城域量子通信网络Chen, J. Wang, et al. 2010, 是国际上首个全通型的量子通信网络, 各节点全部演示了安全的语音通信. 值得指出的是, 与欧洲 SECOQC 网络以及 Tokyo QKD network 不同, 这两个量子通信网络是基于诱骗态方案的成熟技术, 追求并逐步实现满足信息论定义下严格安全性要求的实用性, 而不是欧洲、美国和日本同行所做的多种技术的混合展示. 我国此类小规模的演示性网络还有多节点的城域量子政务网.

4. 限制与挑战

4.1 Impossibility of quantum bit commitment

在第一个 QKD 协议Bennett and Brassard 2014发布后的 10 年中，只有少数密码学家从事量子密码学工作。下面列出了主要的不可能论据。

首先，考虑以下不可能完全安全地实现经典比特承诺的草图：假设存在这样的协议。然后，根据信息理论安全性要求，在承诺阶段结束时，鲍勃对协议的看法必须独立于 b（否则，协议但是相位，两者都被 Bob 接受。因此，位承诺不能绑定。这种独立性意味着 Alice 可以选择在显示中显示 b = 0 或 b =1。有趣的是，相同的证明该结构适用于量子情况，尽管通过调用一些更多的技术工具也是如此。即，我们首先考虑该协议的一个纯净版本，该版本包含所有在量子级别上起作用的各方（通过标准，一个统一的过程代替了测量）接下来，通过信息论的隐藏特性，必须确定鲍勃在提交阶段结束时持有的还原量子态。ical，无论 b = 0 还是 b =1。此条件足以破坏她的系统，以便重新创建与 b = 0 或 b = 1 一致的关节状态。13 因此，她可以选择稍后再打开 b = 0 或 b = 1 时，Bob 会接受：承诺方案不能具有约束力。

回到有关量子比特承诺的原始论文，我们注意到绑定属性的定义中的

一个细微之处是安全性虚假主张的起源：尽管确实如此，该协议使得 Alice 无法同时保存消息。（b = 0 和 b = 1），这不足以证明安全性，因为实际上 Alice 能够延迟会宣布对 b = 0 且 b = 1 的承诺（因此可以选择开放她选择承诺，直到协议结束–此时她可以选择以 b = 0 或 b = 1 打开。

回到有关量子比特承诺的原始论文，我们注意到绑定属性的定义中的一个细微之处是安全性虚假主张的起源：尽管确实如此，该协议使得 Alice 无法同时保存消息。（b = 0 和 b = 1），这不足以证明安全性，因为实际上 Alice 能够延迟会宣布对 b = 0 且 b = 1 的承诺（因此可以选择开放她选择承诺，直到协议结束–此时她可以选择以 b = 0 或 b = 1 打开。

4.2 Impossibility of secure two-party computation using quantum communication

鉴于不可能实现量子比特承诺，下一个要问的问题是：是否存在可以使用量子通信安全地实现的经典通信？实际上，OT 的可能性被认为是一个未解决的问题Montrdal and Centre-ville 1996。不幸的是，这种希望很快就破灭了，因为 LoLo 2008在单边计算中给出了不可能的结果（其中只有一方收到输出）。1 出 2 的 OT 的不可能性—证明技术紧跟为量子比特承诺的不可能性开发的技术。科尔贝花了近 10 年的时间才展示了两个 OT 的第一个不可能结果。侧面的计算，即爱丽丝总是可以获得比鲍勃的输入更多的信息，而不是该函数的值所暗示的信息。类似地，萨尔维尔，沙夫纳和索塔科娃证明，任何非平凡的原始信息的量子协议都会泄漏信息给更糟糕的是，即使在受信方的帮助下，量子通信协议也无法“放大”任何原语的加密能力。

Buhrman，Christandl 和 SchaffnerSalvail, Schaffner, and Sotáková 2015加强了上述不可能的结果，通过证明任何量子协议中的泄漏本质上都可以像人们想象的那样严重：即使在近似正确性和安全性的情况下，如果一个协议对鲍勃“安全”，那么它对爱丽丝也是完全不安全的（在某种意义上，她可以为所有可能的输入计算计算的输出）。由于不可能，导致通用可组合性（UC）框架。

4.3 Zero-knowledge against quantum adversaries: “quantum rewinding”

Goldwasser，Micali 和 Rackoff 引入的零知识交互式证明是交互式证明，其性质是验证者从与诚实证明者的交互中不会学到任何东西，超出了被证明陈述的有效性。这些证明系统在验证中起着重要作用。密码学的基础，并且也是实现密码功能的基本构建块（请参阅Goldreich, Micali, and Wigderson 1991调查）。在零知识的交互证明中，验证者“不了解任何内容”的概念是-通过模拟范式进行恶意化：如果对于每个作弊验证者（在肯定实例中与协议进行交互），都存在一个模拟器（不与证明者进行交互），以使验证者的输出与验证者的输出无法区分模拟器，那么我们说零知识属性成立。在古典世界中，用于建立零知识属性的通用证明技术是倒带：通常通过执行给定的验证程序来构建模拟器-除了某些计算路径被剔除外如果验证者的随机选择与预期效果不一致。通过跟踪交互来完成选择，因此，如果认为交互遵循了错误的路径，则仿真可以简单地重置计算（“快退”）到计算的较早部分（请参阅Goldreich, Micali, and Wigderson 1991其中的参考）。

在量子环境中，这种倒带方法是不可能的：无克隆定理告诉我们，一般来说，不可能保留成绩单的第二份副本以便以后再返回。在最一般的情况下，验证者以某种辅助方式开头，这一事实使这一问题进一步恶化。量子信息（通常我们不知道如何重新创建）-因此，即使是简单的情况下模仿倒带方法的“补丁”，在辅助量子信息的情况下也似乎会失败。以上关于零知识特性的关注点适用于纯古典协议：诚实的当事人是完全古典的，但是我们希望针对可能接收，存储和处理量子信息的验证者建立零知识特性。

4.4 光子数分离攻击

单光子的不可分割性是量子密码安全性的重要物理基础。然而, 多光子脉冲不再拥有不可分割性。例如, 一个包含两个光子的脉冲, 原则上可以被分割为两个单光子脉冲, 所以其安全性基础就不复存在了, 就会遭受光子数分离攻击, 下面我们来具体介绍下光子数分离攻击 Huttner et al. 1995,Brassard et al. 2000。由于量子通信通道损耗率极大, 对于 100 km 以上的距离, 加上探测效率, 整体效率将小于千分之一。根据理论证明, 理想单光子源即便在高损耗通道下也是绝对安全的, 可是实际系统使用的弱光在高损耗通道下则结果完全不同: 窃听者可以冒充通道损耗通过光子数分离攻击而获得全部密码。如图 3 所示, 为表述方便, 我们以偏振空间为例。弱相干态脉冲实际上是单光子与多光子脉冲的概率混合。即, 在所发出的非真空脉冲中, 有些是单光子的, 有些是多光子的 (2 光子,3 光子……)。多光子脉冲即包含了多个全同偏振光子。窃听者可将其分离, 自己留下一个, 将剩余光子送到远程合法用户。对于这些多光子脉冲, 窃听者可以拥有与合法用户完全一样的偏

振光子而不对远程合法用户的光子偏振态造成任何扰动。即, 对于多光子脉冲, 窃听者可以拥有 100% 的信息而不被察觉。窃听者可以选择将所有单光子脉冲完全吸收而使得远程合法用户的所有比特皆由光源的多光子脉冲产生。窃听者的行为不会被合法用户察觉, 因为窃听者可以对每个单独脉冲随时调整通道衰减系数, 从而使得远程合法用户的探测器计数率等同于高损耗自然通道。

对于 2005 年以前的弱相干态密钥分发实验 Kimura et al. 2004, 窃听者可获取全部信息而不留下任何痕迹。事实上, 量子密码发明者之一, Brassard 等 Huttner et al. 1995,Brassard et al. 2000 早在 2000 年就对弱相干态量子密码实验做出批评, Brassard 等在其著名论文的摘要部分指出: “Existing experimental schemes (based on weak pulses) currently do not offer unconditional security for the reported distances and signal strength”, 即: “现有基于 (相干态) 弱脉冲的做法, 据其所报告的距离及所采用的脉冲强度, 并不提供绝对安全性。” Brassard 的这一评论适用于 2005 年以前所有基于弱相干光的量子密钥分发实验 Kimura et al. 2004。幸运的是, 于 2005 年起发展起来的诱骗态量子密码理论, 提供了一个基于弱相干光源的安全量子密钥分发方案。

4.5 侧信道攻击和木马攻击

尽管量子通信技术在理论上具有“无条件安全性”, 但理论方案安全性和实际系统安全性这两个层面之间仍存在一条狭窄但分明的缝隙. 利用量子保密通信系统器件的性能缺陷进行窃听, 或者针对器件的弱点进行主动攻击都可能削弱甚至破坏量子保密通信系统的安全性. 自 2000 年以来, 随着量

子通信技术的逐步实用化, 实用系统中的安全攻防问题变得越来越重要, 并引起研究者的高度重视. 针对早期方案和实验技术中的安全性漏洞, 已提出了大量的攻击方案, 如伪装态攻击、相位重映射攻击、定时侧信道攻击、大脉冲攻击、光学部件高能破坏攻击等. 这些攻击方案, 统称为侧信道攻击和木马攻击.

“木马攻击”中的木马是指实际的量子保密通信系统其信号源、接收器以及其他部件有可能存在的某种弱点, 针对这种弱点, 可以设计攻击方案, 主动诱使系统内部信息泄露. 如果不弥补器件的弱点, 这种攻击常常能有效地击破量子保密通信系统的安全性. 比如说“大脉冲攻击”法, 由于光学器件总会有一定反射能力. 窃听者因此向光路中发射高亮度激光. 对于某些量子保密通信系统的实现方案, 被反射回来的光会被系统中的极化或相位调制器调制, 这样, 攻击者就得到了发射方信号态的极化或相位信息, 而不会引入额外的干扰, 也就不会被发现. 再如“高能破坏攻击”使用高亮度激光击毁衰减器, 破坏了弱相干光源, 随后就可以使用“分束器攻击”或者“分离光子数攻击”窃取密钥. 主动攻击法还有“伪装态攻击”、“相位再映射攻击”等. 而侧信道攻击法是指量子通信系统可能存在泄漏密钥信息的侧信道. 侧信道攻击最出名的就是分离光子数攻击, 此外, 最近提出的针对有记忆的装置无关 QKD 系统的攻击就利用了经典协商信道的侧信道泄漏.

Bibliography

Bennett, Charles H. and Gilles Brassard (2014). "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560.P1, pp. 7–11. ISSN: 03043975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025.

Bennett, Charles H., Gilles Brassard, et al. (1993). "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Physical Review Letters* 70.13, pp. 1895–1899. ISSN: 00319007. DOI: 10.1103/PhysRevLett.70.1895.

Brassard, Gilles et al. (2000). "Limitations on practical quantum cryptography". In: *Physical Review Letters*. ISSN: 00319007. DOI: 10.1103/PhysRevLett.85.1330. arXiv: 9911054 [quant-ph].

Broadbent, Anne and Christian Schaffner (2016). *Quantum cryptography beyond quantum key distribution*. Vol. 78. 1. Springer US, pp. 351–382. ISBN: 1062301501. DOI: 10.1007/s10623-015-0157-4. arXiv: 1510.06120.

Chen, Teng-Yun, Hao Liang, et al. (2009). "Field test of a practical secure communication network with decoy-state quantum cryptography". In: *Optics Express*. ISSN: 1094-4087. DOI: 10.1364/oe.17.006540.

Chen, Teng-Yun, Jian Wang, et al. (2010). "Metropolitan all-pass and inter-city quantum communication network". In: *Optics Express*. ISSN: 1094-4087. DOI: 10.1364/oe.18.027217. arXiv: 1008.1508.

Goldreich, Oded, Silvio Micali, and A V I Wigderson (1991). "Zero-Knowledge twenty years after its invention". In: *Computing* 38.1, pp. 691–729.

Huttner, B. et al. (1995). "Quantum cryptography with coherent states". In: *Physical Review A*. ISSN: 10502947. DOI: 10.1103/PhysRevA.51.1863. arXiv: 9502020 [quant-ph].

Hwang, Won Young (2003). "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Physical Review Letters*. ISSN:

10797114. DOI: 10.1103/PhysRevLett.91.057901. arXiv: 0211153 [quant-ph].

Kimura, Tadamasa et al. (2004). "Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography". In: *Japanese Journal of Applied Physics, Part 2: Letters*. ISSN: 00214922. DOI: 10.1143/JJAP.43.L1217.

Lo, Hoi-kwong (2008). "Insecurity of Quantum Secure Computations". In: pp. 1–28. arXiv: 9611031v2 [arXiv:quant-ph].

Montrdal, Universitd De and Succursale Centre-ville (1996). "Cryptology Column 25 Years of Quantum Cryptography". In: pp. 13–24.

Peng, Cheng Zhi et al. (2007). "Experimental long-distance decoy-state quantum key distribution based on polarization encoding". In: *Physical Review Letters*. ISSN: 00319007. DOI: 10.1103/PhysRevLett.98.010505. arXiv: 0607129 [quant-ph].

Salvail, Louis, Christian Schaffner, and Miroslava Sotáková (2015). "Quantifying the leakage of quantum protocols for classical two-party cryptography". In: *International Journal of Quantum Information* 13.4. ISSN: 02197499. DOI: 10.1142/S0219749914500415. arXiv: 1501.01549.

Wang, Xiang Bin (2005). "Beating the photon-number-splitting attack in practical quantum cryptography". In: *Physical Review Letters*. ISSN: 00319007. DOI: 10.1103/PhysRevLett.94.230503. arXiv: 0410075 [quant-ph].