Week 13

Nite

2025-03-19T12:18:00+11:00

阅读 PDF

量子密码学 (Quantum Cryptography)

什么是量子密码学?

量子密码学 (Quantum Cryptography) 是指利用量子计算机 (Quantum computers) 来进行密码学的相关工作。

- **量子计算机 (Quantum Computers):** 将量子物理 (Quantum physics) 应用于计算任务的计算机。
- **量子密码分析 (Quantum Cryptanalysis):** 研究量子计算对经典密码学的威胁和影响。
- **可行性:** 我们能否利用量子效应来解决当前我们面临的安全困境?

量子物理 (Quantum Physics) 基础

- **物质的“量子化”(Quantised):** 物质的能量等物理量是离散的，不是连续的。原子以称为“光子”(photons) 的离散能量量子 (quanta) 形式发射能量。
- **叠加态 (Superposition):** 在被观测前，原子的某些属性（如自旋）是不确定的，表现为多种状态的“叠加”。例如，一个原子的自旋可以是“上”，也可以是“下”，甚至可以同时是“上和下”。
- **退相干 (Decoherence):** 当叠加态的量子系统与环境发生相互作用（例如被观测）时，会瞬间“坍缩”到一个确定的经典状态。
- **量子比特 (Qubits):**
  - 经典比特 (Classical Bits) 只能是 0 或 1。
  - 量子比特 (Qubits) 可以是 0、1，或者 0 和 1 的叠加态。

传统密码学的实现方式

我们之前学习的密码学主要基于复杂的数学问题，特别是**近单向函数 (near one-way functions)**。

- 这类函数正向计算（加密）很容易。
- 但在没有密钥的情况下，逆向计算（解密）非常困难。

其安全性依赖于:

- **计算上的难解性 (Computational Intractability):** 破解密码的计算量极其巨大。
- **密钥长度:** 最好的解密方法的处理时间会随着密钥长度的增加而急剧增长。
- **大数分解难题 (Difficulty of Factoring):** 这是现代许多加密方法（如 RSA）的核心。

完美保密 (Perfect Secrecy)

- **一次性密码本 (One-Time Pad, OTP):** 这是一种理论上无法被破解的加密方法。它使用一个只使用一次的随机密钥（密码本）对信息进行加密。
- 香农 (Shannon) 在 1949 年证明了其**完美保密性**。
- **问题:** 最大的挑战在于如何**安全地**将这个一次性密码本从发送方传输给接收方。

量子密码学如何解决问题

- **基本思想:** 由 Brassard 和 Bennett 于 1984 年首次提出，量子密码学提供了一种使用单个光子 (single photons) 来安全传输一次性密码本（即密钥）的方法。
- **窃听检测: 任何窃听行为（例如，尝试复制密钥）都会对光子的量子态造成可被检测到的扰动。**
- **真随机性:** 密钥可以基于从自然界中获取的真正随机性来生成。

密码学的基本要求

1. **随机性 (Randomness)**
    - 计算机很难生成**真随机数**，因为它们依赖于固定的算法 (fixed algorithm)。
    - 量子物理学可以实现真随机性，例如：
        - **量子退相干 (Quantum Decoherence):** 量子态因与环境相互作用而失去相干性，这个过程是随机的。
        - **光子在半透半反镜上的反射行为。**
        - **量子涨落 (Quantum Fluctuations):** 例如，澳大利亚国立大学 (ANU) 的量子随机数生成器 (QRNG)。
2. **不可逆性 (Irreversibility)**
    - 目前没有已知的**数学上绝对不可逆的 1 对 1 函数**。
    - 我们使用的最佳近似是**大数分解**：两个大质数相乘很容易，但将乘积分解回两个质数则非常困难。类似的还有微分与积分的难易度对比。
    - 在量子物理学中，我们可以依赖**观测者效应 (observer effect)**：一个处于叠加态的系统在与观测者相互作用后，会坍缩到一个单一的本征态。这个过程是不可逆的。

EPR 纠缠和波函数坍缩

- **量子纠缠 (EPR Entanglement):** 意味着两个（或多个）纠缠的粒子是一个整体，即使相隔很远，一个粒子的状态变化会瞬间影响到另一个粒子，就像“左手知道右手在做什么”。
- **波函数坍缩 (Wavefunction Collapse):** 这是我们的第二个关键要素，它就像一个**一次性的“锁和钥匙”(one-time lock/key)**。一旦状态被测量并坍缩，就无法回到原来的叠加态。

量子密钥分发 (Quantum Key Distribution, QKD)

QKD 的目标是让 Alice 和 Bob 能够生成并共享一个安全的密钥，同时能发现任何窃听者 Eve 的存在。

安全信息的量由以下公式定义：

$$\Delta_I = I_{AB} - I_E$$

其中：

- I_{AB} 是 Alice 和 Bob 之间可以达成一致的共享信息量。
- I_E 是完全控制了传输信道的第三方（Eve）可能获取的最大信息量。

一个 QKD 设备必须能够：

1. 评估信道参数以限制 I_E 的上界。
2. 高效地对 Alice 和 Bob 之间共享的信息进行协调 (reconcile)。
3. 提取出最终的安全信息（密钥）。

QKD 的两种类型

主要分为两类：离散变量 QKD (DV-QKD) 和连续变量 QKD (CV-QKD)。

特性	**离散变量 QKD (DV-QKD)**	**连续变量 QKD (CV-QKD)**
源	单光子 / 衰减相干激光	弱调制的高亮度相干激光
探测器	单光子探测器	零差探测器 (Homodyne detectors)

离散变量 QKD (DV-QKD)

这是最经典的 QKD 协议，也称为 **BB84 协议**。

核心步骤：

1. **Alice 的准备:**
   - Alice 生成一串随机比特 (0 或 1)。
   - Alice 生成一个随机的**基序列 (basis sequence)**，例如用 + (直线基) 和 x (对角基)。
2. **Alice 的发送:**
   - 对于每个比特，Alice 根据对应的基，将一个光子偏振 (polarised) 后发送出去。例如，对于直线基 +，0 对应水平偏振 ↔，1 对应垂直偏振 ↕。
3. **Bob 的接收:**
   - Bob 不知道 Alice 为每个光子选择了哪个基，所以他为每个接收到的光子**随机选择一个基**（+ 或 x）进行测量。
4. **公开对账:**
   - 通信结束后，Alice 和 Bob 通过一个**公开信道**（不需要保密，但需要认证）**只比较他们为每个比特所选择的基序列**。
   - 他们保留那些双方选择了**相同基**进行测量和发送的比特，丢弃其余的。这些保留下来的比特就构成了共享密钥。
5. **窃听检测:**
   - **如果 Eve 试图拦截并测量光子，她也必须猜测一个基。根据量子力学的原理，她的测量行为会大概率地改变光子的原始状态。**
   - 当 Alice 和 Bob 后来对一小部分保留的密钥进行比对时，如果发现错误率异常高，就意味着有窃听者存在。
   - **如果 Alice 和 Bob 能够验证彼此的身份，那么该协议可以抵抗中间人攻击 (Man-in-the-Middle, MITM)。**

实用性:

- 实现距离越来越长，从 1989 年的 32 厘米发展到现在的约 200 公里。
- 但仍然速度慢、实现困难，并且不能解决所有安全问题，如**认证 (authentication)** 和 **数字签名 (digital signatures)** 等。

连续变量 QKD (CV-QKD)

CV-QKD 使用整个激光束进行量子密码通信，而不是单个光子。它通过测量光场的**正交分量 (quadrature)**，如振幅 (amplitude) 和相位 (phase) 来编码信息。

优势：

- **更高的探测器效率。**
- 可以使用**现成的电信组件 (off-the-shelf components)**。
- 与现有光纤通信网络**兼容**。
- 可以实现**更高的密钥生成速率**。

光学设备	带宽
激光器	本质上无限制
调制器	可用带宽 >40 GHz
探测器	可用带宽 10 GHz

肖尔算法 (Shor’s Algorithm)

- **这是由 Peter Shor 在 1994 年提出的一个量子算法。**
- **核心功能: Shor’s Algorithm 可以在多项式时间内有效地分解大整数和计算离散对数。**
- **重大威胁: 任何依赖于大数分解或离散对数难题的经典公钥密码系统，都无法抵抗量子计算机的攻击。**这包括：
  - RSA
  - DSA (数字签名算法)
  - Diffie-Hellman 密钥交换
  - El Gamal
  - ECC (椭圆曲线密码学)
- **重要提示: 一次性密码本 (OTP) 仍然是安全的。**为什么？因为 OTP 的安全性不依赖于任何计算复杂性难题，而是基于密钥的真随机性和一次性使用。

示例考题与参考答案

问题 1：请解释经典密码学和量子密码学在安全性保障上的根本区别是什么？**(Question 1: Explain the fundamental difference between classical cryptography and quantum cryptography in terms of their security assurance.)**

参考答案 (中)：经典密码学（如 RSA）的安全性主要依赖于**计算复杂性难题**。它假设敌手没有足够的计算能力在合理的时间内解决某个数学难题（例如大数分解）。这种安全性是**有条件的**，可能会随着计算能力的提升（如量子计算机的出现）或新算法的发现而被攻破。量子密码学（如 QKD）的安全性则基于**物理学的基本定律**，特别是量子力学原理（如不确定性原理和观测者效应）。任何对量子信道的窃听行为都会不可避免地扰动量子态，从而被通信双方发现。这种安全性是**无条件的**，不依赖于计算的困难程度，因此理论上是永久安全的。

Reference Answer (EN): The security of classical cryptography (e.g., RSA) relies on **computational complexity problems**. It assumes that an adversary lacks sufficient computational power to solve a specific mathematical problem (like factoring large numbers) within a reasonable time. This security is **conditional** and can be compromised by advances in computing power (like the advent

of quantum computers) or the discovery of new algorithms. In contrast, the security of quantum cryptography (e.g., QKD) is based on the **fundamental laws of physics**, specifically the principles of quantum mechanics (such as the uncertainty principle and the observer effect). Any attempt to eavesdrop on the quantum channel inevitably disturbs the quantum states, which can be detected by the communicating parties. This security is **unconditional**; it does not depend on computational difficulty and is therefore theoretically secure indefinitely.

问题 2：描述 BB84 量子密钥分发协议的工作流程，并解释它如何检测窃听者 Eve 的存在。**(Question 2: Describe the working process of the BB84 Quantum Key Distribution protocol and explain how it detects the presence of an eavesdropper, Eve.)**

参考答案 (中)： BB84 协议工作流程如下：

1. **发送方 (Alice):** 生成一串随机比特，并为每个比特随机选择一个偏振基（例如，直线基 + 或对角基 x）。然后根据比特值和对应的基来制备并发送一系列单光子。
2. **接收方 (Bob):** 为接收到的每个光子随机选择一个基（+ 或 x）进行测量。
3. **公开对账:** Alice 和 Bob 通过公开信道，公布他们为每个光子所选择的基序列，但不公布测量结果。
4. **密钥筛选:** 他们保留那些双方使用了相同基的比特作为原始密钥，丢弃其余的。

窃听检测：如果窃听者 Eve 试图拦截光子，她必须进行测量才能获取信息。为了测量，她也必须猜测一个基。

- 如果她猜对了基，她可以得到正确的比特值并重新发送一个相同状态的光子给 Bob，而不被发现。
- 但她有 50% 的概率猜错基。如果她猜错了（例如，Alice 用 + 基发送，Eve 用 x 基测量），根据量子力学，她的测量会改变光子的状态。当 Bob 再用 + 基去测量这个被改变了的光子时，他将有 50% 的概率得到错误的结果。
- 最终，Alice 和 Bob 会随机抽取一部分筛选后的密钥进行比对。如果在没有信道噪声的情况下，他们发现错误率显著高于 0%（理论上由于 Eve 的窃听会导致约 25% 的错误率），他们就能断定有窃听者存在，并废弃此次生成的密钥。

Reference Answer (EN): The workflow of the BB84 protocol is as follows:

1. **Sender (Alice):** Generates a random bit string and, for each bit, randomly chooses a polarization basis (e.g., rectilinear + or diagonal x). She then prepares and sends a sequence of single photons according to the bit values and corresponding bases.
2. **Receiver (Bob):** For each incoming photon, Bob randomly chooses a basis (+ or x) to perform a measurement.
3. **Public Sifting:** Alice and Bob communicate over a public channel to announce the sequence of bases they used for each photon, but not the measurement results.
4. **Key Establishment:** They keep the bits for which they used the same basis and discard the rest. This forms the raw key.

Eavesdropper Detection: If an eavesdropper, Eve, tries to intercept the photons, she must measure them to gain information. To do so, she also has to guess a basis.

- If she guesses the basis correctly, she can obtain the correct bit value and re-transmit an identical photon to Bob without being detected.
- However, she has a 50% chance of guessing the wrong basis. If she guesses incorrectly (e.g., Alice sends with + basis, Eve measures with x basis), her measurement will alter the photon’s

state due to quantum principles. When Bob then measures this altered photon with the correct + basis, he will have a 50% chance of getting an incorrect result.
- Ultimately, Alice and Bob will compare a random subset of their established key. If, in the absence of channel noise, they find an error rate significantly above 0% (theoretically, Eve's eavesdropping introduces an error rate of about 25%), they can conclude that an eavesdropper is present and will discard the key.

考试复习 (Exam Review)

期末考试安排

- **考试时间:** 2 小时写作时间 + 10 分钟阅读时间。
- **考试形式: 闭卷考试 (CLOSED book exam)**，不允许携带任何材料。
- **允许携带:** 不可编程的计算器。
- **提供的材料:** Gradescope MCQ 答题卡，2 张草稿纸。

考试结构

考试包含两个部分，共 25 个问题，总分 50 分。

- **A 部分 - 选择题 (Multiple Choice)** [共 20 分]
  - 共 20 题，每题 1 分。
  - 答案必须填涂在 **Gradescope MCQ 答题卡**上。
  - 内容分布:
    * 6 题来自 Weeks 1-7。
    * 14 题来自 Weeks 8-13。
- **B 部分 - 简答题 (Short answer question)** [共 30 分]
  - 共 5 题，每题 6 分。
  - 答案必须写在**试卷本上指定的答题区域内**。
  - 内容分布:
    * 2 题来自 Weeks 1-7。
    * 3 题来自 Weeks 8-13。

各周复习要点

- **Week 1:** 安全基本原则 (Basic Principles of Security), CIA 三元组 (CIA triad), 柯克霍夫原则 (Kerckhoff's Principle), 安全哈希函数属性 (Properties of Secure Hash Functions), 抗碰撞性 (Collision Resistance)。
- **Week 2:** 密码与密码分析 (Ciphers and cryptanalysis), 常见攻击类型 (COA, KPA, CCA), 替换密码 (Substitution Ciphers), 凯撒密码 (Caesar Cipher), 维吉尼亚密码 (Vigenere Cipher), 一次性密码本 (OTP), 伪随机数生成器 (PRNGs)。
- **Week 3:** 分组密码 (Block Ciphers), DES 设计原理, 工作模式 (modes of operation), ECB, CBC, OFB。
- **Week 4:** 数论 (Number theory), Diffie-Hellman 密钥交换, RSA 公钥加密。
- **Week 5:** 对 RSA 的攻击 (Attacks on RSA), 基于 RSA 的数字签名 (Digital Signatures), 认证 (Authentication), 密码 (Passwords), 零知识证明 (Zero Knowledge Proofs)。

- **Week 6:** Diffie-Hellman 中间人攻击 (MITM Attacks), 使用证书颁发机构 (Certificate Authorities) 的公钥管理, SSL/TLS 协议及其攻击。
- **Week 7:** Shamir 秘密共享 (Shamir Secret Sharing), 承诺协议 (Commitment Protocols), 隐写术 (Steganography), 僵尸网络攻击 (Botnet Attacks)。
- **Week 9:** 区块链网络 (Blockchain Network), 工作量证明 (Proof-of-Work), 区块链安全与攻击。
- **Week 10:** 软件安全 (Software Security), Bell-Lapadula 模型, 缓冲区溢出攻击 (Buffer Overflow Attacks) 及预防, 竞争条件 (Race Conditions), 时间攻击 (Timing Attacks)。
- **Week 11:** 网络安全 (Network Security), OSI 模型, TCP/IP 握手, 欺骗攻击 (Spoofing Attack), 网络 DoS 攻击 (SYN Flooding, Smurfing), DDoS, 会话劫持 (Session Hijacking), 端口扫描 (Port Scanning), 防火墙 (Firewalls), ARP 攻击, DNS 攻击, Web 安全 (SQL 注入, XSS, CSRF)。
- **Week 12:** 无线安全 (Wireless Security), WEP, WPA/WPA2, 硬件安全 (Hardware Security)。
- **Week 13:** 量子密码学 (Quantum Cryptography), 量子密钥分发 (QKD), 肖尔算法 (Shor’s Algorithm)。

期末考试技巧

- **注意时间管理。**
- 书写要**清晰、简洁**。
- 确保在试卷首页和 B 部分的指定位置清晰填写**学号**。
- **只有写在指定答题区内的答案才会被评分**，草稿纸不会被批改。
- 可以用图表或例子来辅助说明你的简答题答案，但**例子不能替代定义**。
- **仔细读题，直接回答问题**，不要包含不相关的信息。

知识点考法分析与示例

可能的考法

1. **概念对比：**考试可能会要求你对比经典密码学和量子密码学的根本区别，尤其是在安全性的基础上（计算复杂度 vs. 物理定律）。
2. **协议解释：**可能会要求详细解释一个 QKD 协议，例如 BB84，并说明其如何发现窃听者。这是核心考点。
3. **影响分析：** Shor’s Algorithm 是一个非常重要的考点，可能会问它对现有密码体系（特别是 RSA）的影响，以及为什么像 OTP 这样的系统不受其影响。
4. **优缺点分析：**可能会要求比较 DV-QKD 和 CV-QKD 的优缺点。