work4

姓名：吴浩哲

学号：2223612444

1. 阐述不经意传输的涵义

不经意传输（Oblivious Transfer, OT）是一种密码学协议，允许发送方将多个秘密消息，如$m_1, m_2, \ldots, m_n$，发送给接收方，但接收方只能选择获取其中一个特定消息m_σ，且发送方无法得知接收方选择了哪个消息，同时接收方也无法获取其他未选择的消息内容。

2. Rabin的不经意传输协议

Rabin的不经意传输协议（Rabin-OT）是最早由Michael Rabin在1981年提出的密码学协议，其核心思想是发送方（Alice）将秘密消息m通过加密传输给接收方（Bob），但Bob仅以$1/2$的概率成功解密获取m，且Alice无法确认Bob是否成功解密。协议基于大整数分解难题和二次剩余问题：Alice生成两个大素数p, q并发送$N = pq$给Bob；Bob随机选择$x \in \mathbb{Z}_N^*$发送$x^2 \mod N$；Alice计算x的四个平方根并随机返回其中一个y；若$y \neq \pm x$（概率$1/2$），Bob可通过$\gcd(x - y, N)$分解N并解密消息，否则无法获取信息。

3. 阐述零知识证明的涵义

零知识证明（Zero-Knowledge Proof, ZKP）是一种密码学协议，由Goldwasser、Micali和Rackoff在20世纪80年代初提出，其核心在于**证明者（Prover）**能在不泄露任何有用信息的前提下，向**验证者（Verifier）**证明某个命题的真实性。例如，A可通过打开一扇只有特定钥匙才能打开的门并取出某物向B证明自己拥有钥匙，而无需展示钥匙本身。该技术需满足三个关键属性：**正确性**（证明者无法欺骗验证者）、**完备性**（验证者无法欺骗证明者）和**零知识性**（验证者无法获取额外信息）。零知识证明广泛应用于区块链、隐私保护等领域，如ZCash和以太坊通过zk-SNARKs实现隐私交易验证，其本质是概率性证明而非确定性证明，可通过重复交互将误差降至可忽略水平。

4. 简化F-F-S识别体制的实现过程

简化F-F-S（Feige-Fiat-Shamir）识别体制是一种基于零知识证明的身份认证协议，其实现过程如下：首先，可信仲裁者选择一个随机模数m，并为用户A（识别者）生成一对公钥v和私钥s，其中$v \equiv s^2 \mod m$。验证者B随机选择一个挑战数r发送给A，A使用私钥s计算响应$y \equiv s \cdot r \mod m$并返回给B。B通过验证$y^2 \equiv v \cdot r^2 \mod m$是否成立来确认A的身份合法性。整个过程无需泄露私钥s，且重复多次可降低欺骗概率，最终实现“证明者知晓秘密但验证者一无所知”的零知识特性。

5. 基于离散对数的Pedersen 承诺协议

基于离散对数的Pedersen承诺协议是一种密码学承诺方案，其核心思想是允许承诺方（Prover）在不泄露秘密值m的情况下生成一个公开承诺C，后续可通过揭示m和随机盲因子r供验证方

（Verifier）验证。具体实现分为三阶段：

1. **初始化**：选择阶为素数q的乘法群G及两个独立生成元g, h（离散对数关系未知）；
2. **承诺**：承诺方计算$C = g^m h^r \mod p$（p为大素数且$q \mid p-1$），发送C给验证方；
3. **验证**：揭示阶段发送(m, r)，验证方重新计算$C' = g^m h^r$并检查$C' \stackrel{?}{=} C$。

该协议基于离散对数困难问题，满足**完美隐藏性**（r的随机性确保m信息论安全）和**计算绑定性**（无法找到两组(m, r)生成相同C）。其加法同态性（$C_1 \cdot C_2 = g^{m_1+m_2} h^{r_1+r_2}$）使其广泛应用于隐私交易（如门罗币）和零知识证明系统。

6. Paillier加密方案的实现过程并证明为什么其具有加法同态性

Paillier加密方案是一种基于合数剩余类问题的公钥加密算法，其实现过程分为三部分：

1. **密钥生成**：选择两个大素数p和q，计算$n = pq$和$\lambda = \mathrm{lcm}(p-1, q-1)$，随机选取$g \in \mathbb{Z}_{n^2}^*$满足$g^\lambda \equiv 1 \mod n^2$，公钥为$(n, g)$，私钥为$\lambda$。
2. **加密**：对明文$m \in \mathbb{Z}_n$，选择随机数$r \in \mathbb{Z}_n^*$，计算密文$c = g^m \cdot r^n \mod n^2$。
3. **解密**：计算$m = \frac{L(c^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \mod n$，其中$L(x) = \frac{x-1}{n}$。

加法同态性证明：对于密文$c_1 = g^{m_1} r_1^n \mod n^2$和$c_2 = g^{m_2} r_2^n \mod n^2$，其乘积$c_1 c_2 = g^{m_1+m_2} (r_1 r_2)^n \mod n^2$解密后为$m_1 + m_2 \mod n$，即$D(c_1 c_2) = D(c_1) + D(c_2)$，满足同态加法。这一性质源于$g$的指数运算和$r^n$的乘法在模$n^2$下的结合性。