**重庆邮电大学《计算机网络》课程报告**

**2024-2025学年第 1 学期**

**题 目 不经意传输协议概述**

**姓 名 叶嘉豪**

**学 号 2022211795**

**专 业 计算机科学与技术**

**班 级 04012202**

**成 绩**

**2024年 12月 18日**

# 不经意传输协议概述

**摘 要：**不经意传输允许发送方将多个消息中的一个或多个安全地传输给接收方，而接收方无法得知未选择的消息内容，同时发送方也不知道接收方选择了哪些消息。报告首先回顾了不经意传输协议的基本概念，接着分析了当前主流的OT协议及其在不同应用场景下的性能和安全性。最后，报告指出了不经意传输协议面临的挑战，为相关领域的研究者和实践者提供了有益的参考。

**关键词：**不经意传输协议，性能，安全性，挑战

## 1基本概念

### 基本定义

不经意传输协议（Oblivious Transfer, OT）：一种密码学协议，允许发送方将多个消息中的一个或多个发送给接收方，而接收方只能得知其选择的那部分消息，发送方则不知道接收方选择了哪些消息。

* 1. 目的
     1. 选择性获取数据

接收方可以根据自己的需求选择性地获取发送方提供的信息中的部分内容，而不是全部信息。

* + 1. 双向匿名

在OT协议中，不仅接收方的选择是私密的，发送方也不知道哪些信息被接收方选中，从而实现了双向匿名。

* + 1. 安全多方计算

OT协议是安全多方计算中的一个重要组件，它允许多方在不泄露各自输入的情况下共同完成计算任务。

* 1. 工作原理

**步骤 1: 发送方准备消息**

* 发送方有N个消息 𝑀1,𝑀2,...,𝑀𝑁*M*1​,*M*2​,...,*MN*​。
* 发送方将每个消息 𝑀𝑖*Mi*​ 加密，得到加密后的消息 𝐸(𝑀1),𝐸(𝑀2),...,𝐸(𝑀𝑁)*E*(*M*1​),*E*(*M*2​),...,*E*(*MN*​)。

**步骤 2: 发送方生成密钥对**

* 发送方为每个消息生成一对公私钥 (𝑃𝐾𝑖,𝑆𝐾𝑖)(*PKi*​,*SKi*​)，其中 𝑃𝐾𝑖*PKi*​ 是公钥，𝑆𝐾𝑖*SKi*​ 是私钥。

**步骤 3: 发送方发送加密消息和公钥**

* 发送方将所有加密后的消息 𝐸(𝑀1),𝐸(𝑀2),...,𝐸(𝑀𝑁)*E*(*M*1​),*E*(*M*2​),...,*E*(*MN*​) 和对应的公钥 𝑃𝐾1,𝑃𝐾2,...,𝑃𝐾𝑁*PK*1​,*PK*2​,...,*PKN*​ 发送给接收方。

**步骤 4: 接收方选择消息**

* 接收方想要选择第 𝑗*j* 个消息 𝑀𝑗*Mj*​，但他不想让发送方知道自己的选择。
* 接收方生成一个随机密钥 𝐾*K* 和 𝑁−1*N*−1 个随机数 𝑟1,𝑟2,...,𝑟𝑗−1,𝑟𝑗+1,...,𝑟𝑁*r*1​,*r*2​,...,*rj*−1​,*rj*+1​,...,*rN*​。

**步骤 5: 接收方构造选择向量**

* 接收方使用自己的选择 𝑗*j* 和随机数构造一个选择向量 𝑉*V*，其中 𝑉𝑗=𝐾*Vj*​=*K*，其他位置为对应的随机数。

**步骤 6: 接收方加密选择向量**

* 接收方使用发送方提供的公钥 𝑃𝐾1,𝑃𝐾2,...,𝑃𝐾𝑁*PK*1​,*PK*2​,...,*PKN*​ 分别加密选择向量中的每个元素，得到加密后的选择向量 𝐸(𝑉1),𝐸(𝑉2),...,𝐸(𝑉𝑁)*E*(*V*1​),*E*(*V*2​),...,*E*(*VN*​)。

**步骤 7: 接收方发送加密的选择向量**

* 接收方将加密后的选择向量发送给发送方。

**步骤 8: 发送方解密并发送结果**

* 发送方使用自己的私钥 𝑆𝐾1,𝑆𝐾2,...,𝑆𝐾𝑁*SK*1​,*SK*2​,...,*SKN*​ 解密接收方发送的加密选择向量。
* 发送方将解密后的 𝑉𝑖*Vi*​ 与原始加密消息 𝐸(𝑀𝑖)*E*(*Mi*​) 使用同态加密的性质进行运算，得到一个新的加密消息 𝐸(𝑀𝑖′)*E*(*Mi*′​)，其中只有 𝐸(𝑀𝑗′)*E*(*Mj*′​) 是有效的加密消息，其他都是无效的。
* 发送方将所有 𝐸(𝑀𝑖′)*E*(*Mi*′​) 发送给接收方。

**步骤 9: 接收方解密所选消息**

* 接收方使用密钥 𝐾*K* 解密 𝐸(𝑀𝑗′)*E*(*Mj*′​)，得到所选择的消息 𝑀𝑗*Mj*​。
* 接收方无法解密其他 𝐸(𝑀𝑖′)*E*(*Mi*′​)，因为这些加密消息与接收方的密钥不匹配。

1. 协议种类及安全性与性能分析

[2]此处主要分析基于不经意传输的数字产品交易协议、基于不经意传输的LBS隐私保护协议、基于不经意传输的区块链数据保密查询协议三种协议之间的对比。

* 基于不经意传输的数字产品交易协议
* 初始化

我们先设定一个用于加密的特殊数学系统，基于一种叫做椭圆曲线的东西。这个系统里有一个基础的点G，可以生成一个有q个成员的群（q是一个很大的素数），我们在这个群里进行数学运算。

消费者在这个系统中随机选择一个私钥SB，并基于这个私钥生成一个公钥KB。这个公钥是用来加密信息的。

销售商有两种数字产品，我们假设它们的价格都是m。消费者想要选择其中一种产品，记为gk，k可以是1或者2。

* 信息交互

销售商随机选择一些数字t0, r1, r2，并确保r1和r2是不同的。然后，销售商用这些数字和消费者的公钥KB来加密商品信息，得到两组加密数据C1和C2，并将这些加密数据放在一个公开的网站上。

消费者从网站上下载这些加密数据，然后根据自己的选择（比如选择第一个或第二个商品），随机选择一个数字ai，并计算出Di发送给销售商。

销售商收到Di后，计算出两个新的数据R和D’，并将它们发送给消费者。

* 获取信息

消费者收到R和D’后，使用自己的私钥SB和之前选择的数字ai，进行一些计算，最终解密出自己选择的数字产品信息gk。

* 基于不经意传输的LBS隐私保护协议
* 初始化

我们使用一种叫做椭圆曲线的技术来设置一些基础的安全工具。用户会随机生成一个私钥（就像密码一样），并用它来创建一个公钥。服务器有很多地点信息，用户想要查询的是其中的一个。

* 信息交互

用户修改原本的查询请求，使其不会泄露自己的真实位置和查询意图，而是用一些替代信息来发送给服务器。

服务器随机生成一些数字，然后用这些数字和用户的公钥来加密地点信息，最后把加密后的信息发送给用户。

用户收到这些加密信息后，再随机选择一些数字，根据自己的查询需求进行一些计算，然后把结果发送给服务器。

服务器再次进行计算，然后把计算结果发送给用户。

* 获取信息

用户最后使用自己的私钥和一些收到的信息进行计算，这样就能得到自己想要查询的地点信息，而服务器完全不知道用户查询的是哪个地点。

* 基于不经意传输的区块链数据保密查询协议
* 初始化

创建加密工具：我们使用一个特殊的数学工具——椭圆曲线，在这个曲线上有一个特殊的点𝐺G，它可以帮助我们生成一个加密用的群体𝐺𝐵GB​。这个群体的大小由一个大素数𝑞q决定。

生成钥匙：存储者和查询者各自生成一对钥匙，包括公钥和私钥。存储者的钥匙是𝐾𝐴KA​和𝑠𝐴sA​，查询者的钥匙是𝐾𝐵KB​和𝑠𝐵sB​。

准备数据：存储者拥有一些重要的数据ℎ1,ℎ2,ℎ3,...,ℎ𝑛h1​,h2​,h3​,...,hn​，他想要将这些数据安全地存储起来。

* 信息交互

数据加密：存储者首先将原始数据ℎ1,ℎ2,ℎ3,...,ℎ𝑛h1​,h2​,h3​,...,hn​转换成椭圆曲线上的点𝐻1,𝐻2,...,𝐻𝑛H1​,H2​,...,Hn​。然后，他选择一些随机的数字𝑟0,𝑟1,...,𝑟𝑛r0​,r1​,...,rn​，并使用这些数字和查询者的公钥𝐾𝐵KB​来加密数据，生成加密信息𝐶𝑖Ci​。

查询者准备查询：查询者决定他想要查看哪些数据，比如ℎ1,ℎ2,...,ℎ𝑘h1​,h2​,...,hk​。他随机选择一些数字𝑎1,𝑎2,...,𝑎𝑘a1​,a2​,...,ak​，并计算出一些新的东西𝐷𝑖Di​，这些新东西是基于他想要查看的数据的加密信息。

传递查询请求：查询者将计算出的新东西𝐷1,𝐷2,...,𝐷𝑘D1​,D2​,...,Dk​发送给存储者，这就像是一个加密的查询请求。

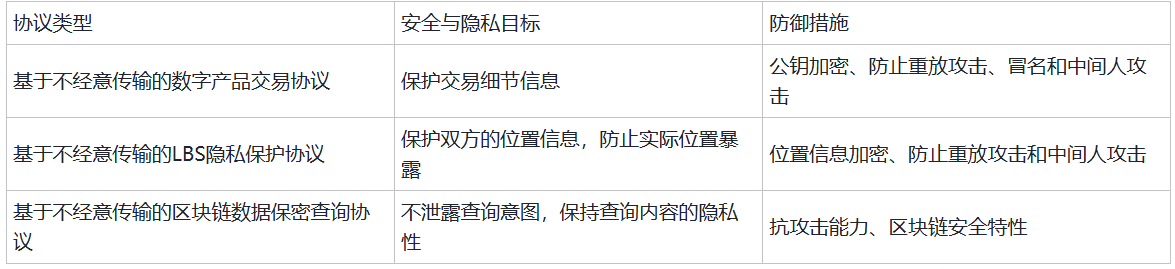
* 获取信息

存储者响应：存储者收到查询者的请求后，进行一些计算，生成结果𝑅R和修改后的新东西𝐷𝑖′Di′​，然后将它们发送给查询者。

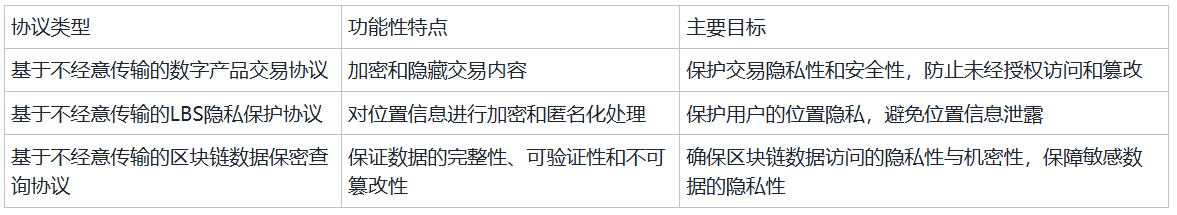
查询者解密数据：查询者使用自己的私钥𝑠𝐵sB​和他之前选择的随机数字𝑎1,𝑎2,...,𝑎𝑘a1​,a2​,...,ak​，以及从存储者那里收到的信息，进行最后的计算。通过这个过程，查询者能够解密出他想要的数据ℎ1,ℎ2,...,ℎ𝑘h1​,h2​,...,hk​。

获取原始数据：查询者使用译码函数将解密后的信息转换回原始数据形式，这样他就成功地在不泄露查询细节的情况下获取了所需的信息。

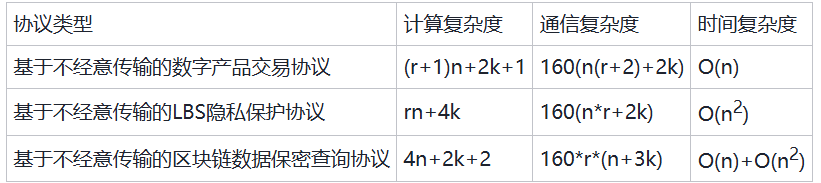
* 1. 安全性对比分析



* 1. 功能性对比分析



* 1. 性能对比分析



1. 挑战
   1. 效率和扩展性

**计算和通信开销**：传统的 OT 协议通常涉及复杂的计算和大量的通信。在处理大量数据或多方参与者时，这些开销成为瓶颈。

**可扩展性**：现有的 OT 协议往往难以扩展到大量用户或大量数据的情况。

* 1. 安全性

**隐私泄露**：即使是最先进的 OT 协议也可能存在隐私泄露的风险，尤其是在面对恶意攻击者时。

**理论模型与实际应用**：理论上的安全模型可能与现实世界中的应用场景不完全匹配，导致实际应用中的安全性问题。

* 1. 实用性和互操作性

**实现复杂性**：OT 协议的实现往往非常复杂，这使得在实际系统中部署 OT 变得困难。

**互操作性**：不同的 OT 协议可能不兼容，这限制了它们在不同系统间的互操作性。

### 参考文献

1. 李晓东,朱晓鹏,张健毅,等.基于密文混淆的不经意传输协议[J/OL].计算机工程,1-11[2024-12-18].https://doi.org/10.19678/j.issn.1000-3428.0069792.
2. 李春平,满子琪,张艳硕,等.基于不经意传输的密码方案设计与对比分析[J].北京电子科技学院学报,2024,32(03):67-81.