



Private Set Intersection

安全多方计算应用

作者：牛午甲 & 潘云石 & 石磊鑫 & 孙霄鹏 & 陈昊

组织：USTC

时间：April 25, 2023

版本：0.1

:



注意：本模板自 2023 年 1 月 1 日开始，不再更新和维护！

目录

第 0 章 数学基础	1
0.1 数论基础	1
0.1.1 中国剩余定理	1
0.2 抽象代数基础	1
第 1 章 基础知识介绍	2
1.1 不经意传输 (Oblivious transfer, OT)	2
1.1.1 Rabin 不经意传输协议	2
1.1.2 1-2 不经意传输	3
第一章 练习	3

第零章 数学基础

0.1 数论基础

内容提要

- 中国剩余定理 0.1
- Fubini 定理 1.1
- 最优性原理 1.1
- 柯西列性质 1.1.2
- 韦达定理

0.1.1 中国剩余定理

定理 0.1 (中国剩余定理, Chinese Remainder Theorem, CRT)

设 m_1, m_2, \dots, m_k 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, 记 $m = m_i M_i (i = 1, 2, \dots, k)$, 则同余式组

$$x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \dots, x \equiv b_k \pmod{m_k}$$

有唯一解

$$x \equiv M'_1 M_1 b_1 + M'_2 M_2 b_2 + \cdots + M'_k M_k b_k \pmod{m}$$

其中 $M'_i M_i \equiv 1 \pmod{m_i} (i = 1, 2, \dots, k)$.

推论 0.1

设 m_1, m_2, \dots, m_k 是 k 个两两互素的正整数, $m = m_1 m_2 \cdots m_k$, 则同余式 $f(x) \equiv 0 \pmod{m}$ 有解的充分必要条件是同余式 $f(x) \equiv 0 \pmod{m_i} (i = 1, 2, \dots, k)$ 每一个都有解, 并且若用 T_i 表示 $f(x) \equiv 0 \pmod{m_i}$ 的解数, T 表示 $f(x) \equiv 0 \pmod{m}$ 的解数, 则 $T = T_1 T_2 \cdots T_k$.

0.2 抽象代数基础

第一章 基础知识介绍

内容提要

- ❑ Rabin 不经意传输协议 1.1
- ❑ Fubini 定理 1.1
- ❑ 最优性原理 1.1
- ❑ 柯西列性质 1.1.2
- ❑ 韦达定理

1.1 不经意传输 (Oblivious transfer, OT)

不经意传输 (Oblivious transfer, OT) 是密码学中的一类协议, 实现了发送方将潜在的许多信息中的一个传递给接收方, 但事后对发送了哪一条消息给接收方保持未知状态。

1.1.1 Rabin 不经意传输协议

不经意传输最早由 Michael O. Rabin 在 1981 年提出。在这种形式下, 发送方以 $\frac{1}{2}$ 的概率向接收方发送一个信息, 而发送方不知道接收方是否收到该信息, 只有接收方能确信地知道自己是否收到了消息。Rabin 的方案是基于 RSA 的。在介绍 Rabin 的方案之前, 需要介绍几个模平方根相关的引理。

引理 1.1

若 m_1, m_2, \dots, m_k 是 k 个

定义 1.1 (Rabin's oblivious transfer protocol)

准备工作: Alice 按照 RSA 算法生成模数 $N = pq$ (这里 p, q 是大素数)、指数 e (要保证 e 和 $r = (p-1)(q-1)$ 互素)。

1. Alice 发送 $N, e, m^e \bmod N$ 给 Bob;
2. Bob 选择随机数 x , 将 $x^2 \bmod N$ 发给 Alice;
3. Alice 求解 $x^2 \bmod N$ 的四个平方根, 选择其中一个 (记作 y) 发给 Bob;

如果 Bob 发现 $y \bmod N$ 既不等于 $x \bmod N$ 也不等于 $-x \bmod N$, 那么 Bob 就可以对 N 进行素因子分解得到 p, q , 从而求得 r 。然后 Bob 求解 $ed \equiv 1 \bmod r$ 得到 d , 再解密 $m^{ed} \bmod N$ 获得 m 的明文。然而, 如果 $y \bmod N$ 是 $x \bmod N$ 和 $-x \bmod N$ 中的一个, 那么 Bob 就无法分解 N , 从而不能解密得到明文。

注 对上述协议需要做几点说明:

1. 在协议第 2. 步中, 由于 N 的素因子只有 p, q , 并且 N 非常大, 因此认为 x 和 N 互素, 从而 $x^2 \bmod N$ 有四个平方根。
- 2.

推论 1.1 (推论名称)

推论内容

1.1.2 1-2 不经意传输

定义 1.2 (定义名称)

定义内容

(1.1)



练习 1.1 练习

解 解

注 注

证明 证明

定理 1.1 (定理名称)

定理内容



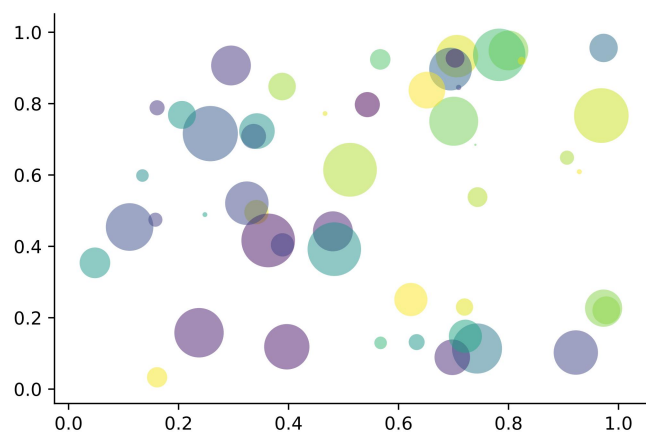
笔记 笔记

命题 1.1 (命题名称)

命题内容



图片

图 1.1: 散点图示例 $\hat{y} = a + bx$

性质 性质

1. 条目 1

2. 条目 2

结论 结论

例题 1.1 例题

第一章 练习

1. 练习 1

2. 练习 2

3. 练习 3