**Лабораторная работа №9-1**

**Исследование протокола скрытого определения k ближайших точек интереса без учета типа POIs.**

**Цель лабораторной работы:**

Практическое применение криптосистемы Пэйе и ее гомоморфных свойств при определении местоположения точек интереса.

**Теоретические сведения:**

POI (*point of interest*) – достопримечательность или другой объект, отмеченный на карте.

Гомоморфное шифрование – это вид шифрования, который позволяет производить вычисления над зашифрованными данными. После расшифровки результат будет таким же, как и проведение идентичных вычислений над открытыми данными. Данный вид шифрования позволяет выполнять пользователю запросы к базе данных (в нашем случае к LBS) в виде зашифрованного текста и получать результаты, не раскрывая при этом информации о самом запросе.

Криптосистема Пэйе является криптосистемой с открытым ключом, обладающей аддитивными гомоморфными свойствами.

**В работе используются следующие обозначения:**

– скрытая область, заранее разделенная на ячеек, для каждой из которых на сервере хранится информация о ближайшей точке интереса;

– местоположение пользователя в ;

информация о ближайшей POI для ячейки (*i, j*) относительно центра данной ячейки, хранящаяся в базе данных сервера. Задается двоичной последоватльностью бит. Первые 3 бита – координата *x,* вторые 3 бита – координата *y*, представленные в двоичном виде. Информация на базе данных сервера хранится в виде целого десятичного числа.

**Описание протокола скрытого определения точек интереса без определения типа POI**

Обозначим:

*–* множество целых чисел по модулю *n*;

*–* множество целых чисел, взаимно простых с *n*;

множество целых чисел, взаимно простых с *n2*;

– Наименьшее общее кратное чисел и .

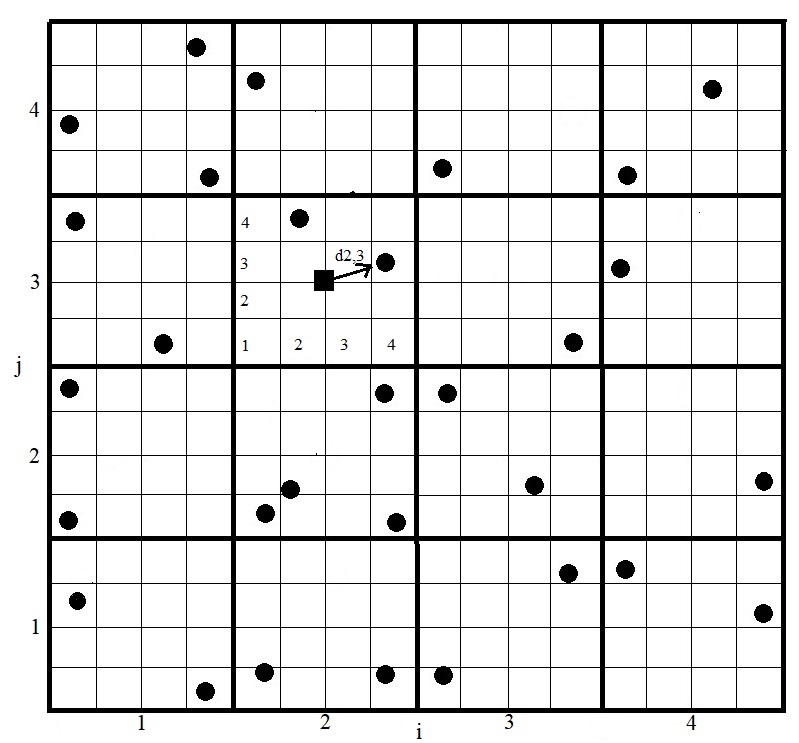


Рис. 3.1 - Координатная сетка с указанными точками интереса.

Предположим, что мобильный пользователь хочет найти ближайшую к своему местоположению точку интереса в области рис. 3.1 предварительно разделенной на ячеек. Пользователь находится в ячейке . Для этого он запускает протокол, состоящий из четырех алгоритмов: генерация ключей, генерация запроса, генерация ответа и получение ответа.

1. Генерация ключей.

Выбирается два простых числа , таких что , где .

Выбирается из .

Способы выбора :

1. Случайно выбирается из множества , удовлетворяющее условию:
2. Случайно выбирается из множества , затем вычисляется:

В этом случае выбранное всегда удовлетворяет условию в пункте 1.

Секретным ключом является: , а открытым ключом:.

1. Генерация запроса.

При шифровании запроса используется алгоритм шифрования криптосистемы Пэйе.

Для каждого выберается случайное целое число и вычисляется:

где 𝑖 – первая координата ячейки, в которой находится пользователь.

Таким образом, пользователь зашифровывается 1, если 𝑙 = 𝑖, и 0 в любом другом случае, используя алгоритм шифрования криптосистемы Пэйе.

Зашифрованный запрос и прикрепленный к нему открытый ключ посылаются на сервер.

1. Генерация ответа сервера.

Получив запрос пользователя и открытый ключ, сервер с помощью открытого ключа зашифровывает инфромацию о ближайших точках интереса для каждой ячейки, таким образом генерируя ответ на посланный запрос.

Для вычисляется :

После того, как сервер сформировал ответ, он отправляет его пользователю.

1. Получение ответа от сервера.

Получив ответ от сервера, пользователь выполняет расшифровку при помощи сгенерированного на первом этапе секретного ключа, используя алгоритм дешифрования криптосистемы Пэйе.

Из вектора пользователь выбирает только , где – вторая координата ячейки, в которой находится пользователь или о которой пользователь запрашивает информацию. Все остальные данные, полученные от сервера пользователь может игнорировать, так как только содержит информацию о k ближайших POIs для ячейки .

Вычисляется:

где алгоритмом дешифрования является алгоритм дешифрования криптосистемы Пэйе:

где

Так как криптосистема Пэйе является аддитивно гомоморфной, то результатом расшифрования произведения криптограмм является сумма их изначальных сообщений. Отсюда следует, что:

Следовательно, так как все множители, кроме равны 0, при расшифровании ответа сервера пользователь получает вектор параметров POI относительно своей ячейки .

После получения целого числа из базы данных сервера следует преобразовать его в двоичный вид и вычислить координаты ближайшей точки интереса для ячейки, в которой находится пользователь.

**Выполнение лабораторной работы**

Вы находитесь в ячейке с координатами согласно номеру варианта.

Каждая ячейка разделена на 4х4 подячеек для определения местоположения точки интереса относительно центра ячейки.

Необходимо определить одну ближайшую точку интереса без раскрытия своего местоположения.

База данных сервера представлена в таблице 1.

База данных сервера о ближайших точках интереса – Таблица 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 11 |  | 33 |  | 36 |  | 27 |
|  | 12 |  | 18 |  | 26 |  | 34 |
|  | 25 |  | 35 |  | 33 |  | 11 |
|  | 10 |  | 11 |  | 9 |  | 27 |

**Порядок выполнения лабораторной работы:**

Для выполнения лабораторной работы удобно использовать сайт [https://wolframalpha.com](https://www.wolframalpha.com/).

1. Выполнить генерацию ключей;
2. Зашифровать данные для дальнейшей отправки на сервер;
3. На стороне сервера сформировать ответ;
4. Выполнить расшифровку ответа, полученного от сервера и вычислить информацию о ближайшей точке интереса;
5. Проверить совпадение результата расшифровки с данными на карте.

**Пример выполнения лабораторной работы:**

Пусть пользователь находится в ячейке .

***Генерация ключей*.**

Выбираем два простых числа и :

Пусть , .

Вычисляем модуль :

.

Максимальная запись на сервере , следовательно простые числа выбраны верно.

Выбираем из множества :

Пусть .

Открытый ключ: ;

Секретный ключ: .

***Шифрование запроса.***

Так как наша область имеет ячеек, то .

Для каждого выбираем случайное число .

Пуcть .

Далее вычисляем для каждого вычисляем:

;

;

;

.

Отправляем на сервер зашифрованный запрос и открытый ключ:

*.*

***Генерация ответа.***

Вычисляем , где :

Сгенерированный ответ сервер отправляет пользователю.

***Получение ответа.***

Расшифровываем криптограмму:

.

Преобразуем полученное число в двоичный вид.

*.* Отсюда выдим, что ближайшая точка интереса для ячейки находится в подячейке .

**Содержание отчета:**

1. Титульный лист с фамилией и номером варианта студента.
2. Цель работы.
3. Исходные данные.
4. Подробные результаты расчетов с пояснениями.
5. Выводы.