

Гомоморфное шифрование в защите информации



Актуальность

Данное исследование является актуальным, поскольку в настоящее время широкое развитие получили технологии облачных вычислений, при этом особое внимание уделяется конфиденциальности и безопасности информации.

Целью данного исследования является изучение различных подходов гомоморфного шифрования, а также разработка прикладного ПО, реализующего один из этих подходов, проверка гомоморфных свойств выбранного для реализации алгоритма шифрования.

Цель

Целью настоящего исследования является изучение различных подходов гомоморфного шифрования, а также разработка прикладного ПО, реализующего один из этих подходов, проверка гомоморфных свойств выбранного для реализации алгоритма шифрования.



Основы гомоморфного шифрования.

Гомоморфное шифрование

- Шифрование – это обратимое преобразование данных с целью сокрытия их от неавторизованных лиц.
- Гомоморфное шифрование (ГШ) – это технология, позволяющая производить вычисления над зашифрованными данными без необходимости их предварительного расшифровывания. Это открывает новые возможности для безопасной работы с данными. Благодаря использованию данной технологии, появляется возможность проведения обработки конфиденциальных данных, используя сторонние вычислительные ресурсы.

История развития гомоморфного шифрования.

Ранние исследования

Концепция гомоморфного шифрования была впервые предложена в 1978 году Рональдом Ривестом, Леонардом Адлеманом и Майклом Дертусосом. Они описали возможность выполнения арифметических операций над зашифрованными данными.

Разработка полностью гомоморфного шифрования

В 2010 году Крэйг Геннаро, Сальваторе Джованни Валенте и Даниэль Вичерс описали первую схему полностью гомоморфного шифрования, которая может выполнять любые вычисления над зашифрованными данными.

1

2

Прорыв в 2009 году

В 2009 году Крэйг Геннаро, Роки Геннаро и Вангее Лу представили первую практическую схему частично гомоморфного шифрования, которая могла эффективно выполнять ограниченные вычисления над зашифрованными данными.

3

Основные типы гомоморфного шифрования

- Полностью гомоморфное шифрование (Fully Homomorphic Encryption, FHE). Данный тип шифрования подразумевает возможность выполнять широкий спектр математических операций над зашифрованными данными, обеспечивает высочайший уровень безопасности и конфиденциальности, поскольку данные могут оставаться зашифрованными на протяжении всего процесса вычислений, однако алгоритмы полностью гомоморфного шифрования обладают высокой вычислительной сложностью, что существенно снижает производительность информационных систем, использующих данный тип шифрования.
- Гомоморфное шифрование с ограниченной полнотой (Somewhat Homomorphic Encryption, SHE). Данный тип шифрования позволяет выполнять ограниченное количество математических операций (сложение и умножение) над зашифрованными данными до накопления определенного уровня шума.
- Частичное гомоморфное шифрование (Partial Homomorphic Encryption). Данный тип шифрования подразумевает возможность выполнять только один тип операции над зашифрованными данными, например, сложение или умножение. Шифрование такого типа осуществляют такие распространенные алгоритмы, как RSA, Криптосистема Голдвассера-Микали, Криптосистема Эль-Гамала, криптосистема Пэйн.

Наиболее распространенными на практике являются частично гомоморфные шифры, допускающие либо сложение, либо умножение, поскольку они обладают более низкой вычислительной сложностью, а так же более просты в реализации.

Криптосистема Пэ́йе

- Криптосистема Пайе (Paillier's cryptosystem) — это асимметричная криптосистема с открытым ключом, разработанная Паскалем Пайе в 1999 году. Она основана на вычислительной сложности задачи факторизации составного числа, являющегося произведением двух простых чисел. Одной из отличительных черт данной системы является возможность выполнения гомоморфных операций сложения над зашифрованными данными.

Давайте рассмотрим данный алгоритм
шифрования.

1. Генерация ключей

- 1. Выбираем два простых числа p и q .
- 2. Вычисляем произведение этих чисел $n = p * q$
- вычисляем $\lambda = \text{lcm}(p-1, q-1)$, где lcm – наименьшее общее кратное.
- Выбираем случайное число g , такое, что $g \in \mathbb{Z}_{n^2}^*$
- Вычисляем μ :
 - $\mu = \left(L(g^\lambda \bmod n^2) \right)^{-1} \bmod n$
 - Где $L(u) = \text{div} \left(\frac{u-1}{n} \right)$
 - Div – целочисленное деление.

Открытым ключом является пара (n, g) , закрытым – (λ, μ) .

2. Шифрование

- 1. Пусть m будет шифруемым сообщением, где $m \in \mathbb{Z}_n$.
- 2. Выбор случайного числа r , $r \in \mathbb{Z}_n^*$
- 3. Вычисление шифротекста c :
 - $c = g^n * r^n \bmod n^2$

3. Расшифровка

- 1. Принимаем зашифрованное сообщение $c \in \mathbb{Z}_{n^2}^*$, открытый (n, g) и закрытый (λ, μ) ключи.
- 2. Вычисляем исходное сообщение по формуле:
- $$m = (L(c^\lambda \bmod n^2) * \mu) \bmod n$$

Результаты проведенной мною реализации
данной криптографической системы

Демонстрация созданной программы

Зашифровать строку в последовательность чисел

Зашифрованные числа: 15632

Открытый ключ (n, g): 145 19244

Закрытый ключ (lambda, mu): 28 28

Расшифровать последовательность чисел

Расшифровать строку из последовательности чисел

Расшифрованные числа/строка: 15

Paillier's cryptographic system

Числа для шифрования (через пробел): 5 10

Зашифровать последовательность чисел

Зашифровать строку в последовательность чисел

Зашифрованные числа: 14807 4826

Открытый ключ (n, g): 145 19244

Закрытый ключ (lambda, mu): 28 28

Расшифровать последовательность чисел

Расшифровать строку из последовательности чисел

Расшифрованные числа/строка:

Умножение чисел по модулю n^2

Введите первое число: 14807

Введите второе число: 4826

Введите число n: 145

Результат умножения по модулю n^2 : 15632

Умножить

Сложение чисел

Введите первое число: 5

Введите второе число: 10

Результат сложения: 15

Сложить

Демонстрация созданной программы

Зашифровать строку в последовательность чисел

Зашифрованные числа: 4868843

Открытый ключ (n, g): 4531 11043083

Закрытый ключ (lambda, mu): 2156 4308

Расшифровать последовательность чисел

Расшифровать строку из последовательности чисел

Расшифрованные числа/строка: 80

Paillier's cryptographic system

Числа для шифрования (через пробел): 30 50

Зашифровать последовательность чисел

Зашифровать строку в последовательность чисел

Зашифрованные числа: 2066627 17426628

Открытый ключ (n, g): 4531 11043083

Закрытый ключ (lambda, mu): 2156 4308

Расшифровать последовательность чисел

Расшифровать строку из последовательности чисел

Расшифрованные числа/строка: 15

Умножение чисел по модулю n^2

Введите первое число: 2066627

Введите второе число: 17426628

Введите число n: 4531

Результат умножения по модулю n^2 : 4868843

Умножить

Сложение чисел

Введите первое число: 30

Введите второе число: 50

Результат сложения: 80

Сложить

Демонстрация созданной программы

Зашифровать строку в последовательность чисел

Зашифрованные числа: 448013403

Открытый ключ (n, g): 24221 402035907

Закрытый ключ (lambda, mu): 5928 14359

Расшифровать последовательность чисел

Расшифровать строку из последовательности чисел

Расшифрованные числа/строка: 123

Paillier's cryptographic system

Числа для шифрования (через пробел): 49 74

Зашифровать последовательность чисел

Зашифровать строку в последовательность чисел

Зашифрованные числа: 218785913 139854355

Открытый ключ (n, g): 24221 402035907

Закрытый ключ (lambda, mu): 5928 14359

Расшифровать последовательность чисел

Расшифровать строку из последовательности чисел

Расшифрованные числа/строка: 80

Умножение чисел по модулю n^2

Введите первое число: 218785913

Введите второе число: 139854355

Введите число n: 24221

Результат умножения по модулю n^2 : 448013403

Умножить

Сложение чисел

Введите первое число: 49

Введите второе число: 74

Результат сложения: 123

Сложить

Демонстрация созданной программы

Paillier's cryptographic system

Числа для шифрования (через пробел):

Зашифрованные числа:

Открытый ключ (n, g):

Закрытый ключ (lambda, mu):

Расшифрованные числа/строка:

Умножение чисел по модулю n^2

Введите первое число:

Введите второе число:

Введите число n:

Результат умножения по модулю n^2 :

Сложение чисел

Введите первое число:

Введите второе число:

Результат сложения:

Заключение

- Гомоморфное шифрование – это перспективная технология, открывающая новые возможности для безопасной обработки данных. Несмотря на текущие проблемы с производительностью, активные исследования и разработки в данной области позволяют надеяться на широкое применение этой технологии в будущем. Обеспечение конфиденциальности данных становится все более важным в современном мире, и гомоморфное шифрование может сыграть ключевую роль в решении этой проблемы

Спасибо за внимание!