УДК 004.056.5

# РЕШЕНИЕ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ КВАНТОВЫХ КОМПЬЮТЕРОВ МЕТОДОМ КРИПТОГРАФИИ НА РЕШЕТКАХ

*Бурчук Д. А.[1], студент гр. 353502, Згирская Д. Д.[2], студент гр.353502*

*Белорусский государственный университет информатики и радиоэлектроники*[1]
*г. Минск, Республика Беларусь*

*Примичева З. Н. – канд. физ.-мат. наук, доцент*

**Аннотация.** Данная работа охватывает краткую историю развития криптографии, дает основные понятия криптографии, описывает метод криптографии на решетках и приводит пример применения данного метода.

**Ключевые слова.** Криптография, криптография на решетках, квантовая криптография, постквантовая криптография, квантовая революция.

## Введение

На протяжении всей истории человечеству было необходимо передавать информацию. Зачастую это приходилось делать тайно: например, при ведении войн преимущество было на стороне тех, у кого были свежие тактические данные. Но все, что может быть перехвачено, будет перехвачено. Это означает, что нет смысла пытаться спрятать само передаваемое сообщение на пути из точки А в точку Б, но есть смысл попытаться скрыть заключенную в него информацию хотя бы на определенное время.

Исходя из этих побуждений, рождается наука криптография. Ее цель заключается в том, чтобы с помощью некоторого алгоритма отправитель смог зашифровать свое сообщение, а получатель с помощью точно такого же алгоритма, но использованного в обратном порядке, расшифровать его.

Зашифровать сообщение можно двумя способами: переставить его символы местами или заменить их другими символами.

В первом, перестановочном методе, число всех возможных перестановок равняется $n!$, где $n$ число букв в сообщении. Если $n$ невелико, то сообщение легко расшифровать. Если же $n$ достаточно большое, то зашифровать, а после расшифровать информацию очень трудоемкий и времязатратный процесс.

Второй метод, называемый методом замены, заключается в том, чтобы заменить одинаковые символы другими одинаковыми символами по определенному алгоритму, что значительно сократит время, затраченное на шифровку и расшифровку информации, в сравнении с методом перестановки (Рисунок 1). Поэтому метод замены стал основной ветвью криптографии еще с древних времен.

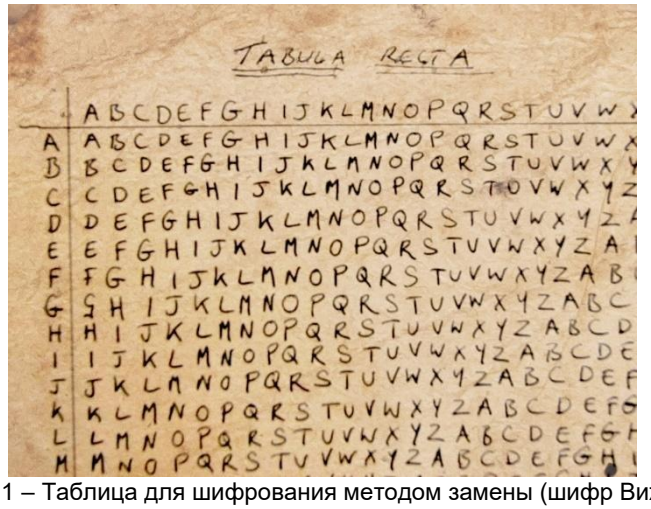

Рисунок 1 – Таблица для шифрования методом замены (шифр Виженера)

Метод замены являлся очень надежным способом шифрования до IX века. Именно тогда арабские ученые заметили интересную деталь: некоторые буквы встречаются в языке чаще, чем остальные. Анализируя таким образом зашифрованные тексты, можно сопоставить наиболее часто встречающиеся символы сообщения с наиболее часто встречающимися буквами языка и таким образом расшифровать послание. Этот метод получил название частотный анализ.

Однако, частотный анализ применим только в том случае, если использовать одинаковый криптографический ключ для шифровки и расшифровки текста, то есть при симметричном

шифровании. Сегодня же существует асимметричное шифрование, которое использует для двух этих целей разные криптографические ключи -— публичный и приватный соответственно (Рисунок 2).

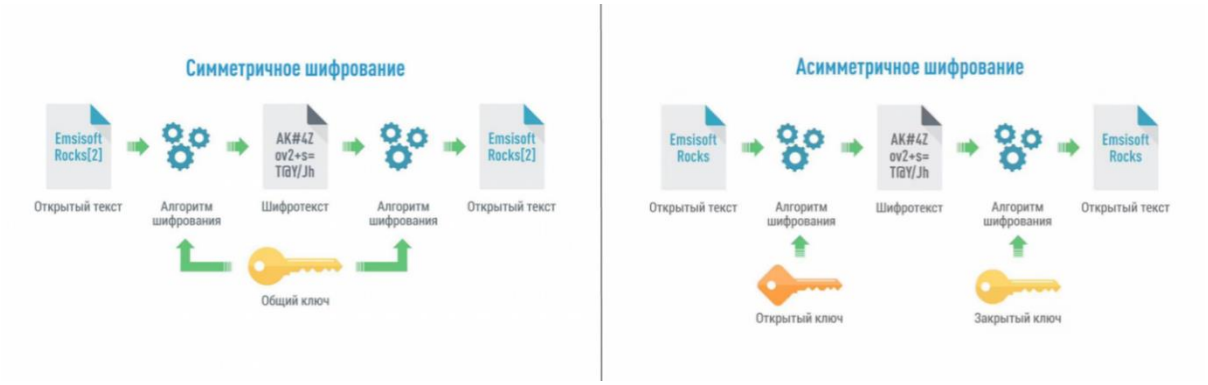


Рисунок 2 – Симметричное и асимметричное шифрование

Вообще, современные методы шифрования информации хорошо работают только на классических компьютерах, имеющих сравнительно небольшие вычислительные мощности. Например, взлом RSA-ключа, состоящего из 1024 бит, займет миллионы лет непрерывных вычислений. Но с такой задачей легко справится квантовый компьютер  устройство, использующее явления квантовой суперпозиции и квантовой запутанности для передачи и обработки данных, и, таким образом, достигающее мощностей во много раз больших мощностей обычного компьютера. Так, приведенная задача будет решена за 10 часов (если предположить, что каждая квантовая операция выполняется 10 нс и что в распоряжении имеется компьютер из достаточного количества логических кубитов).

Несмотря на то, что сегодня еще не существует квантовых компьютеров, способных заниматься подобными задачами, уже сейчас в мире развиваются квантовое и постквантовое шифрование с целью обеспечения защиты информации от квантовой угрозы.

## §1. Методы решения

Существуют два способа защиты данных: квантовая криптография (относится к симметричному шифрованию) и постквантовая криптография (относится к асимметричному шифрованию).

Квантовая криптография берет за основу технологию квантового распределение ключей, которая позволяет двум сторонам обмениваться криптографическими ключами (Рисунок 3).

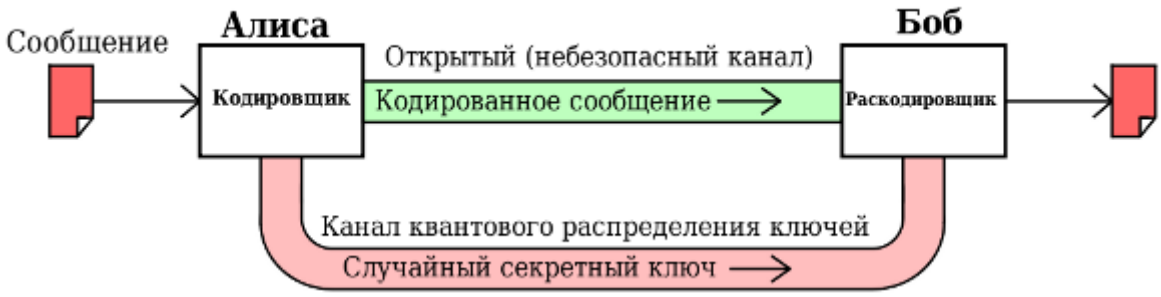


Рисунок 3 – Квантовое шифрование

Как известно, одиночный фотон нельзя разделить, а квантовое состояние нельзя скопировать  это фундаментальное ограничение квантовой механики. На этом принципе  принципе защиты передаваемых данных фундаментальными физическими законами  строятся новые методики шифрования.

По уровню ошибок в информационном канале можно узнать, была ли возможность компрометации ключа. Если уровень ошибок ниже критического порога, то можно исправить ошибки и исключить из него потенциально доступную злоумышленнику информацию при помощи классических алгоритмов и, таким образом, сгенерировать финальный секретный ключ. При этом защищаемая информация остается недоступной злоумышленнику.

Главная идея заключается в том, чтобы использовать квантово-распределенные ключи в шифре Вернама, суть которого в следующем: каждый символ в сообщении преобразовывается побитовым XOR с ключом бумажной ленты.

Постквантовая криптография включает в себя новый класс алгоритмов с открытым ключом, которые основаны на задачах, являющихся вычислительно сложными как для классического компьютера, так и для квантового.

Основными направлениями развития постквантовой криптографии являются:

- Криптография, основанная на хэш-функциях;
- Криптография, основанная на кодах исправления ошибок;
- Криптография, основанная на решетках;
- Криптография, основанная на многомерных квадратичных системах;
- Шифрование с секретным ключом;
- Шифрование с использованием суперсингулярной изогении.

Одним из самых надежных и интересных с математической точки зрения методов является метод криптографии на решетках, который мы подробно рассмотрим далее.

## §2. Метод криптографии на решетках

Криптография на решетках (lattice-based cryptography) это метод криптографии, который использует математические структуры, известные как решетки, для создания шифров. Решетки в математике это наборы точек в многомерном пространстве с определенными свойствами.

Данный вид шифрования считается особенно перспективным из-за его потенциальной устойчивости к атакам с помощью квантовых компьютеров, что делает его важным кандидатом для постквантовой криптографии. В отличие от традиционных методов, таких как RSA, основанных на факторизации больших чисел или вычислении дискретных логарифмов, сложность проблем, связанных с решетками, делает их трудными для решения даже для квантовых компьютеров.

### Схема шифрования GGH

Схема шифрования GGH (англ. *Goldreich–Goldwasser–Halevi*) асимметричная криптографическая система, основанная на решетках.

Криптосистема опирается на решения задачи нахождения кратчайшего вектора и задачи нахождения ближайшего вектора. Схема шифрования GGH, опубликованная в 1997 году учёными Oded Goldreich, Shafi Goldwasser и Shai Halevi, использует **односторонюю функцию с потайным входом**, ведь, учитывая любой базис решетки, легко генерировать вектор, близкий к точке решетки. Например, взяв точку решетки и добавив небольшой вектор ошибки. Для возвращения из вектора ошибки в исходную точку решетки необходим специальный базис.

**Односторонняя функция с потайным входом** это односторонняя функция $f$ из множества $X$ в множество $Y$, обладающая свойством (потайным входом, лазейкой), благодаря которому становится возможным найти для любого $y \in Imf,\ x \in X$ такое, что $f(x) = y$, то есть обратить функцию.

### Алгоритм

Метод шифрования GGH основан на трех матрицах: унимодулярной матрице $U$, матрице $B$, задающей $n$-мерную решетку $L$, и $n$-мерной матрице $B' = UB$, задающей ту же решетку, поскольку два разных базиса решетки эквивалентны тогда и только тогда, когда один получен из другого преобразованиями, сохраняющими определитель матрицы исходного базиса (Рисунок 4).

**Унимодулярная матрица** квадратная матрица с целыми коэффициентами, определитель которой равен $+1$ или $-1$, Это в точности те невырожденные матрицы $A$, для которых уравнение $Ax = b$ имеет целочисленное решение для любого целочисленного вектора $b$.

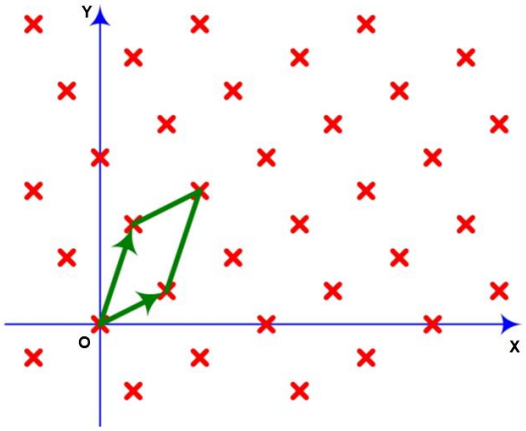


Рисунок 4 – Площадь параллелепипеда, заданного базисными векторами

Матрица $B$ и есть наш закрытый ключ, а матрица $B'$ — открытый.

При этом матрица $B$ задает линейно независимые вектора максимально ортогональные друг другу (Рисунок 5), а матрица $B'$ максимально параллельные между собой, поскольку чем меньше угол между ними, тем сложнее выразить требуемую точку с их помощью (Рисунок 6).

Пусть пространство сообщений $M$ состоит из векторов $(m_1, \dots, m_n)$, принадлежащих интервалу

$$-M < m_i < M \tag{1}$$

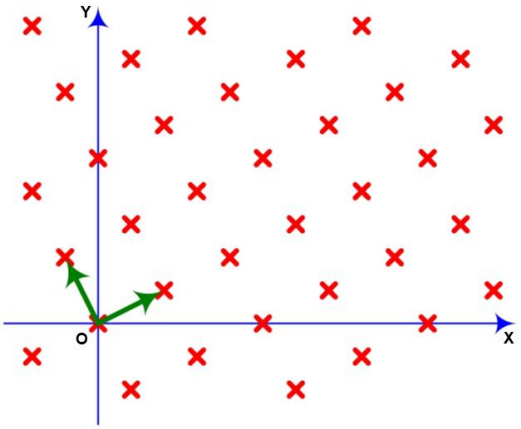


Рисунок 5 – Базис решетки (матрица $B$)

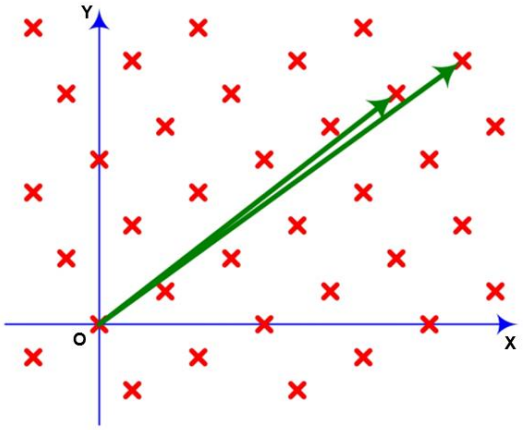


Рисунок 6 – Базис той же решетки (матрица $B'$)

**Шифрование**

Дано сообщение $m = (m_1, \dots, m_n)$, ошибка $e$ и открытый ключ $B'$.

Тогда зашифрованный текст примет вид:

$$c = mB^{'} + e \tag{2}$$

**Расшифровка**

Для расшифровки шифротекста вычисляется:

$$cB^{-1} = \left(mB^{'} + e\right)B^{-1} = mUBB^{-1} + eB^{-1} = mU + eB^{-1} \tag{3}$$

Для удаления $eB^{-1}$, если он достаточно мал, используется округление. Тогда, чтобы получить текст:

$$m = (mU)U^{-1} \tag{4}$$

## §3. Прикладное применение метода

Код писался на языке C++ для увеличения скорости вычисления.

Сначала были разработаны некоторые функции для выполнения базовых операций над матрицами и векторами:

1. Функция перемножения матрицы на матрицу.
2. Функция перемножения вектора на матрицу.
3. Функция нахождения определителя, на ее основе функция нахождения обратной матрицы.
4. Функция генерации унимодулярной матрицы.
5. Функция генерации базис-векторов.
6. Функция генерации случайного шума.

Изначально генерируется три почти перпендикулярных базис-вектора, задающих решётку в трехмерном пространстве (Рисунок 7). Далее создается унимодулярная матрица, используемая для преобразования базис-векторов без изменения начальной решетки (Рисунок 8). После у пользователя запрашивают ввод сообщения, которое посимвольно записывается в вектора для дальнейшего шифрования.

```
long double** B = new long double*[nDimention];

for (int i = 0; i < nDimention; i++)
{
    B[i] = new long double[nDimention]{};
}

for (int i = 0; i < nDimention; i++)
{
    for (int j = 0; j < nDimention; j++)
    {
        B[i][j] = rand() % 5 - 2;
    }
}

for (int j = 0; j < nDimention; j++)
{
    B[j][j] = rand() % 10 + 30;
}
```

Рисунок 7 – Создание матрицы $B$, задающей решетку в трехмерном пространстве

```
long double** unimodularMatrix = new long double*[nDimention];
for (int i = 0; i < nDimention; i++)
{
    unimodularMatrix[i] = new long double[nDimention];
}

long double n = rand() % 3 + 3;

unimodularMatrix[0][0] = 8 * n * (n + 1);

unimodularMatrix[0][1] = 2 * n + 1;

unimodularMatrix[0][2] = 4 * n;

unimodularMatrix[1][0] = 4 * n * (n + 1);

unimodularMatrix[1][1] = n + 1;

unimodularMatrix[1][2] = 2 * n + 1;

unimodularMatrix[2][0] = 4 * n * (n + 1) + 1;

unimodularMatrix[2][1] = n;

unimodularMatrix[2][2] = 2 * n - 1;
```

Рисунок 8 – Создание унимодулярной матрицы

Далее мы перемножаем унимодулярную матрицу на наш базис-вектор, генерируя тем самым открытый ключ. После этого каждый вектор символов мы обрабатываем с помощью случайного шума,

увеличивая значение на 1000 и прибавляя случайное значение от 0 до 255. Затем перемножаем каждый вектор на полученный ранее открытый ключ и распределяем случайную ошибку. Таким образом, мы получаем некоторое количество векторов-сообщений в числовом формате.

После этого следует расшифровка. Мы находим две матрицы: первая обратная унимодулярной матрице, а вторая исходному базису пространства. Перемножаем их последовательно в обратном порядке и получаем приближенные значения. Делим на 1000 и округляем по правилам математического округления (Рисунок 9). На выходе мы получаем наше сообщение плюс n % 3 пробела в конце, нужных для заполнения векторов. Значения являются приближенными. Хотя и происходит нормализация ошибки, потери данных не исключены, так что возможны опечатки в некоторых символах (0.1%).

```
for (int i = 0; i < length; i++)
{
    c[i] = multiplication( first: 1,  second: 3, c[i], B1);
}

for (int i = 0; i < length; i++)
{
    c[i] = multiplication( first: 1,  second: 3, c[i], U1);
}

for (int i = 0; i < length; i++)
{
    for (int j = 0; j < nDimention; j++)
    {
        c[i][j] /= 1000;
        c[i][j] = roundl(c[i][j]);
    }
}
```

Рисунок 9 – Расшифровка сообщения

## Пример

**Шифрование**

Попробуем зашифровать классическое сообщение “Hello World!”
Преобразованное сообщение $m$:

$$(72183.000000 \quad 101154.000000 \quad 108146.000000)$$

$$(108181.000000 \quad 111088.000000 \quad 32188.000000)$$

$$(87086.000000 \quad 111043.000000 \quad 114238.000000)$$

$$(108074.000000 \quad 100250.000000 \quad 33147.000000)$$

Базис $B$:

$$\begin{matrix} 30.000000 & 0.000000 & 0.000000 \\ -1.000000 & 34.000000 & 2.000000 \\ 0.000000 & 1.000000 & 31.000000 \end{matrix}$$

Унимодулярная матрица $U$:

$$\begin{matrix} 240.000000 & 11.000000 & 20.000000 \\ 120.000000 & 6.000000 & 11.000000 \\ 121.000000 & 5.000000 & 9.000000 \end{matrix}$$

Открытый (плохой) базис $B'$:

$$\begin{matrix} 7189.000000 & 394.000000 & 642.000000 \\ 3594.000000 & 215.000000 & 353.000000 \\ 3625.000000 & 179.000000 & 289.000000 \end{matrix}$$

Зашифрованное сообщение $c$:

$$(1274500312.000000 \quad 69546345.000000 \quad 113303041.000000)$$

$$(1293644980.000000 \quad 72268885.000000 \quad 117968597.000000)$$

$$(1439262545.000000 \quad 78634730.000000 \quad 128122172.000000)$$

$$(1257400360.000000 \quad 70068218.000000 \quad 114351240.000000)$$

**Расшифровка**

Матрица, обратная базису $B^{-1}$:

$$\begin{matrix} 0.033333 & 0.000000 & 0.000000 \\ 0.000982 & 0.029468 & -0.001901 \\ -0.000032 & -0.000951 & 0.032319 \end{matrix}$$

Матрица, обратная унимодулярной матрице $U^{-1}$:

$$\begin{matrix} -1.000000 & 1.000000 & 1.000000 \\ 251.000000 & -260.000000 & -240.000000 \\ -126.000000 & 131.000000 & 120.000000 \end{matrix}$$

Расшифрованное сообщение в кодировке ASCII:

$$(72.000000 \quad 101.000000 \quad 108.000000)$$

$$(108.000000 \quad 111.000000 \quad 32.000000)$$

$$(87.000000 \quad 111.000000 \quad 114.000000)$$

$$(108.000000 \quad 100.000000 \quad 33.000000)$$

Расшифрованное сообщение: Hello World!

## Заключение

В результате проделанной работы выяснено, какие существуют методы шифрования информации, выявлена уязвимость используемых методов для взлома квантовыми компьютерами и рассмотрены способы решения данной проблемы.

Подробно изучены шифрование на решетках, в частности, алгоритм шифрования GGH и написана программа, с помощью которой можно зашифровать и расшифровать текстовое сообщение.

На основе полученных данных, можно сделать несколько важных выводов:

1. Криптография на решетках остается безопасной даже при использовании квантовых компьютеров, поскольку алгоритмы, основанные на задачах нахождения кратчайших векторов в решетках, не имеют эффективных квантовых алгоритмов решения.
2. Производительность криптографии на решетках сопоставима с современными алгоритмами шифрования, что позволяет применять ее на практике без существенной потери производительности.
3. Метод шифрования, основанный на решетках, может быть применен в различных областях, включая шифрование данных, электронные подписи, протоколы аутентификации, телевидение, компьютеры, интернет-технологии, программирование, банковскую деятельность, радиосвязь и прочие коммуникации.

Таким образом, на протяжении всей истории для людей существовала необходимость передавать информацию. Для этих целей они научились ее шифровать. С течением времени методы шифрования становились все более сложными и продвинутыми, и в настоящее время используются различные методы шифрования информации, но в скором времени они станут устаревшими и легко взламываемыми.

Одним из способов решения этой проблемы является метод шифрования на решетках. На данный момент ни один квантовый алгоритм не способен справится с расшифровкой сообщения, зашифрованного таким образом, лучше обычного процессора. Считаем рассматриваемый метод крайне эффективным из-за высокой криптостойкости и поэтому думаем, что в ближайшем будущем весь мир будет широко использовать шифрование, основанное на криптографии на решетках.

***Список использованных источников:***
*1. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/sandbox/163505/*
*2. [Электронный ресурс]. – Режим доступа: https://www.ispras.ru/courses/book-lattice-cryptography.pdf*
*3. [Электронный ресурс]. – Режим доступа: https://dzen.ru/a/ZR_HOiQpoAgwA7fT*
*4. [Электронный ресурс]. – Режим доступа: https://new.ras.ru/upload/iblock/07e/0jcrq8npgpu208o8qlssforcyeky5dxl.pdf*

UDC 004.056.5

# SOLUTION TO THE PROBLEM OF INFORMATION FROM QUANTUM COMPUTERS USING YHE MOTHOD OF CRYPTOGRAPHY ON LATTICES

*Burchuk D. A.*[1], *Zgirskaya D. D.*[2]

*Belarusian State University of Informatics and Radioelectronics*[1], *Minsk, Republic of Belarus*

*Primicheva Z.N. – Ph.D. physics and mathematics Sciences, Associate Professor*

**Annotation.** This work covers a brief history of the development of cryptography, gives the basic concepts of cryptography, describes the method of lattice cryptography, and gives an example of the application of this method.

**Keywords.** Cryptography, lattice cryptography, quantum cryptography, post-quantum cryptography, quantum revolution.