УДК 004.056.5

ДИОФАНТОВЫЕ МОДЕЛИ ДЛЯ СКВОЗНОГО ШИФРОВАНИЯ[1]

Рассохин Д.К. студент, Лукащик Е.П. канд. физ.-мат. наук, доц.
Кубанский Государственный Университет (г. Краснодар)

Ключевые слова: шифрование, криптография, квантовые алгоритмы, диофантовы уравнения, криптосистемы, алгоритм Шора, алгоритм Гровера.

Аннотация

В рамках данной статьи проводится математическое моделирование криптографической системы с использованием диофантовых трудностей, против которой неприменимы популярные квантовые алгоритмы атак, такие как алгоритм Шора и алгоритм Гровера.

Введение. С каждым годом компьютерные технологии развиваются все быстрее. Революцию в технологическом прогрессе произвело и появление квантового компьютера. Однако квантовые вычисления поставили перед криптографией новые проблемы. Так, доказанный ученым Питером Шором [4] факт эффективного решения задач факторизации и дискретного логарифмирования с помощью квантовых компьютеров может сделать многие существующие алгоритмы шифрования в перспективе уязвимыми к атакам. Это заставляет криптографию искать новые математические методы и модели для защиты информации в пост-квантовой эре, устойчивые к успехам технического прогресса.

Одним из возможных решений можно считать разработку криптоалгоритмов на основе теории диофантовых уравнений. Согласно

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-01-00596

работам К. Шеннона [2] не существует алгоритма, позволяющего определить решение произвольного диофантова уравнения. Криптографические системы на основе таких уравнений для нелегального пользователя сокращают возможность уменьшить множество перебираемых ключей и, следовательно, потребуют неограниченного объема вычислительной работы и ресурсов при взломе.

Основные понятия. Диофантовым уравнением называется уравнение вида:

$$D(x_1, \dots, x_n) = 0, \qquad (1)$$

где D – полином с целыми коэффициентами, $x_1, \dots, x_n$ – неизвестные переменные уравнения (1). Стоит отметить, что $x_1, \dots, x_n \in Z$, т.е. решениями считаются только целые числа.

Отметим, что проблема решения уравнений в целых числах решена до конца только для уравнений с одним неизвестным, для уравнений первой степени и для уравнений второй степени с двумя неизвестными. Для уравнений выше второй степени с двумя или более неизвестными достаточно трудной является даже задача определения существования целочисленных решений. Более того, доказано [1], что в принципе не существует единого алгоритма, позволяющего за конечное число шагов решать в целых числах произвольные диофантовы уравнения. Практическая невозможность разрешения произвольного диофантова уравнения делает эту теорию весьма привлекательной для использования в криптографии.

Моделирование алгоритма. Составим математическую модель симметричной биграммной криптосистемы, т.е. криптосистемы, в которой текст разбивается на блоки из 2 элементов – биграммы, а для шифрования и дешифрования используется один секретный ключ.

В качестве основы для алгоритма используем линейное диофантово уравнение 1-й степени:

$$mx + ny = z, \quad (1)$$

где m и n – произвольные целые числа, а x и y – переменные; $x, y \in N$; $m, n, z \in Z$.

Известно, что для случая, когда НОД$(m, n) = 1$, уравнение (1) имеет следующие целые параметрические решения:

$$x_k = x_0 z + nt \quad (2)$$

$$y_k = y_0 z - mt$$

$$t \in Z,$$

(x_0, y_0) – целое решение уравнения $mx + ny = 1$

Для обеспечения единственности решения данной задачи легальным пользователем используем систему линейных диофантовых уравнений:

$$\begin{cases} m_1 x + m_2 y = z_1 \\ n_1 x + n_2 y = z_2 \end{cases}, \quad (3)$$

где m_i и n_i – произвольные целые числа, а x и y – переменные; $x, y \in N$; $m_i, n_i, z_i \in Z$. За секретный ключ примем пары чисел (m_1, n_1) и (m_2, n_2) – коэффициенты системы. Предположим, что (x, y) – известные числовые эквиваленты некоторой биграммы. Тогда, подставляя указанные значения в систему (3), получим пару чисел (z_1, z_2) – зашифрованные числовые эквиваленты этой биграммы.

После получения зашифрованных данных легальному пользователю будут известны все коэффициенты системы из 2 линейных диофантовых уравнений с 2 неизвестными. Для этой системы выполняется теорема Кронекера – Капелли, т.е. система совместна и имеет единственное решение.

Для примера ограничим алфавит до 26 заглавных английских букв A…Z и пробела. Каждому символу в алфавите сопоставим соответствующий номер: A – 1, B – 2, …, Z – 26, <пробел> – 27. Так как алгоритм использует биграммы, перед передачей исходный текст разбиваем на блоки из 2 символов. Если количество символов в биграмме равно 1, то добавим 1 пробел.

Продемонстрируем действие описанного алгоритма на примере исходного сообщения $M = CIPHER$ (таблица 1).

Таблица 1 – таблица числовых эквивалентов для сообщения

C	I	P	H	E	R
3	9	16	8	5	18

Разделим сообщение на биграммы:

$$M_1 = CI \tag{4}$$
$$M_2 = PH$$
$$M_3 = ER$$

Предположим, пользователю А необходимо отправить пользователю Б зашифрованную биграмму M_1. Секретный ключ составят две пары взаимно простых чисел $v = ((m_1, n_1), (m_2, n_2))$. Конкретно, для данного примера выберем ключ $v = ((17, 3), (13, 21))$.

Пользователь А подставляет секретный ключ и числовые эквиваленты биграммы в систему (3) и получает вектор $z = (z_1, z_2)$, который и является зашифрованной биграммой. В нашем случае вектор $z = (511, 483)$, который затем передаем по каналу.

В процессе дешифрования пользователь Б подставляет вектор z и секретный ключ v в систему (3) и получает простую систему линейных диофантовых уравнений, в нашем случае:

$$\begin{cases} 17x + 13y = 511 \\ 3x + 21y = 483 \end{cases} \tag{5}$$

Решая полученную систему Б однозначно определяет числовые эквиваленты x и y: $x = 3$, $y = 9$.

Перед нелегальным пользователем, которому удалось перехватить вектор z, стоит задача решить систему линейных диофантовых уравнений. Так как количество неизвестных превышает количество самих уравнений, то задача имеет бесконечно много решений:

$$\begin{cases} m_1 x + m_2 y = 511 \\ n_1 x + n_2 y = 483 \end{cases} \quad (6)$$

Усложнение алгоритма. Усложним математическую модель, полученную в предыдущем пункте, добавив в нее дополнительные параметры.

В качестве основы оставим систему (3). Заменим x и y на a и b следующим образом:

$$a = x + q_1 \quad (7)$$
$$b = y + q_2,$$

где q_1 и q_2 – произвольные целые числа, $q_i \in Z$.

Тогда система (3) примет вид:

$$\begin{cases} m_1(x + q_1) + m_2(y + q_2) = z_1 \\ n_1(x + q_1) + n_2(y + q_2) = z_2 \end{cases} \quad (8)$$

$$\begin{cases} m_1 a + m_2 b = z_1 \\ n_1 a + n_2 b = z_2 \end{cases}$$

Новым секретным ключом будет вектор $v = ((m_1, n_1, q_1), (m_2, n_2, q_2))$. Так как для легальных пользователей в системе (8) известны все переменные кроме a и b, то система имеет единственное решение и задача сводится к предыдущей с добавлением дополнительного действия для получения числовых эквивалентов биграммы:

$$x = a - q_1 \quad (9)$$
$$y = b - q_2$$

Для нелегального же пользователя задача усложнилась, так как для всех найденных решений системы (8) ему необходимо решить диофантовы уравнения (9).

Дальнейшее усложнение системы можно выполнить путем введения зависимости ключа от свойств шифруемого текста.

Заключение. Приведенная криптосистема использует диофантовы трудности, что делает невозможным применение популярных квантовых алгоритмов для решения проблем факторизации и дискретного

логарифмирования. При выборе достаточно больших значений секретного ключа, перед злоумышленником стоит проблема нахождения всех возможных решений системы диофантовых уравнений, количество которых бесконечно, не имея для этого универсального алгоритма. Приведенная модель может быть использована в механизмах сквозного шифрования различных информационных систем: от мессенджеров до облачных сервисов.

Библиографический список

1. Матиясевич Ю. В. Диофантовы множества // Успехи мат. наук. 1972. Т. 27, вып. 5. С. 185–222

2. Shannon C. Communication theory of secrecy systems, Bell System Techn. J. 28, № 4 – 1949. P. 656–715

3. Osipyan V.O. Mathematical modelling of cryptosystems based on Diophantine problem with gamma superposition method // SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks ACM, 2015. pp 338-341

4. Shor P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on — IEEE, 1994. — P. 124–134