ЛИТЕРАТУРА

1. *Stinson D. R.* Cryptography. Theory and Practice. CRC Press, 1995. 434 p.
2. *Menezes A., van Oorshot P., and Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1997. 662 p.
3. *Langelaar G. C.* Real-time Watermarking Techniques for Compressed Video Data. Delft: Delft University of Technology, 2000. 155 p.
4. *Mistry D.* Comparison of digital water marking methods // Intern. J. Comp. Sci. Engin. 2010. V. 2. No. 9. P. 2905–2909.
5. *Анжин В. А.* Метод защиты от нелегального копирования в цифровых видеотрансляциях через внедрение водяных знаков при расшифровании // Прикладная дискретная математика. Приложение. 2014. №. 7. С. 73–74.
6. `https://github.com/anjin-viktor/mpeg2decwtrk/` — Method implementation for MPEG2 Video. 2014.

УДК 004.056.55 DOI 10.17223/2226308X/8/21

ПОСТРОЕНИЕ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ[1]

В. В. Егорова, Д. К. Чечулина

Работа посвящена изучению практической применимости схемы полностью гомоморфного шифрования, созданной в Лаборатории современных компьютерных технологий НИЧ НГУ. Рассмотрено приложение гомоморфного шифрования для построения криптосистемы с открытым ключом, основанной на алгоритме RSA. На примере этой криптосистемы продемонстрирована корректность выполнения арифметических операций над зашифрованными данными, а также отсутствие увеличения размерности зашифрованных сообщений при умножении.

Ключевые слова: *гомоморфное шифрование, криптосистема с открытым ключом, алгоритм RSA.*

В Лаборатории современных компьютерных технологий НИЧ НГУ в рамках проекта «Защищённая база данных» разработана и реализована схема полностью гомоморфного шифрования, позволяющая выполнять операции сложения и умножения над зашифрованными данными. Рассмотрим подробнее эту схему. Пусть требуется шифровать целые числа размера t бит. Для этого необходимо выбрать целое число — модуль m, по которому будут производиться все вычисления в схеме. Модуль является частью секретного ключа. Для того чтобы однозначно восстановить любое зашифрованное число, модуль должен удовлетворять условию $2^t < m$.

Кроме того, для шифрования требуется секретный вектор $k \in \mathbb{Z}^n$, который строится следующим образом. Сгенерируем матрицу W размера $n \times n$, обратимую по модулю m, а также вектор $u \in \mathbb{Z}^n$, компоненты которого по модулю не превосходят m. Вектор k определим как решение системы линейных уравнений

$$(W \cdot k) \bmod m = u,$$

которая всегда разрешима, так как матрица W обратима по модулю m. Таким образом, $k = (W^{-1} \cdot u) \bmod m$. Матрица W и вектор u также являются частью секретного ключа.

Перейдём к описанию алгоритма шифрования. Пусть $p < 2^t < m$ — целое число,

[1]Работа поддержана грантом Минобрнауки РФ, договор № 02.G25.31.0054.

которое требуется зашифровать. Алгоритм гомоморфного шифрования заключается в построении такого вектора $c \in \mathbb{Z}^n$, что

$$(c, k) \bmod m = p. \tag{1}$$

Заметим, что в процессе построения вектора k сформирован набор векторов w_i (строк матрицы W), $i = 1, \ldots, n$, таких, что $(w_i, k) \bmod m = u_i$.

Выберем из этого набора любые s, $s \in \{2, \ldots, n\}$, векторов $w_1, \ldots, w_s$, которые будем использовать для шифрования. Тогда вектор c, являющийся шифртекстом, будем строить как линейную комбинацию этих векторов:

$$c = \sum_{i=1}^{s} \alpha_i \cdot w_i.$$

Коэффициенты α_i найдём из диофантова уравнения

$$u_1\alpha_1 + \ldots + u_s\alpha_s = p.$$

Для того чтобы данное уравнение было разрешимо, необходимо существование как минимум двух взаимно простых компонент вектора u. Сформированный таким образом шифртекст c однозначно расшифровывается согласно формуле (1):

$$(c, k) \bmod m = \left(\sum_{i=1}^{s} \alpha_i w_i, k\right) \bmod m = \sum_{i=1}^{s} \alpha_i (w_i, k) \bmod m = \sum_{i=1}^{s} \alpha_i u_i \bmod m = p.$$

Описанная схема шифрования является гомоморфной по сложению и умножению в силу свойств скалярного произведения и модулярной арифметики [1]. Рассмотрим подробнее операцию умножения. Найдём шифртекст для произведения чисел p_1 и p_2, которым соответствуют шифротексты a и b:

$$\begin{gathered} p_1 \cdot p_2 (\bmod\ m) = (a, k)(b, k) = (a_1k_1 + \ldots + a_nk_n)(b_1k_1 + \ldots + b_nk_n) = \\ = a_1b_1k_1k_1 + a_1b_2k_1k_2 + \ldots + a_nb_{n-1}k_nk_{n-1} + a_nb_nk_nk_n = \\ = (a_1b_1, a_1b_2, \ldots, a_nb_{n-1}, a_nb_n)(k_1k_1, k_1k_2, \ldots, k_nk_{n-1}, k_nk_n). \end{gathered}$$

Таким образом, в результате умножения двух шифртекстов длины n получается шифртекст длины n^2:

$$c = a \cdot b = (a_1b_1, a_1b_2, \ldots, a_nb_{n-1}, a_nb_n) \in \mathbb{Z}^{n^2}.$$

Для решения этой проблемы предлагается использовать специальную таблицу умножения — матрицу (γ_{ijk}). С её помощью компоненты вектора $c = (c_1, \ldots, c_n)$ — результата произведения двух шифртекстов — вычисляются следующим образом:

$$c_k = \sum_i \sum_j \gamma_{ijk} \cdot a_i \cdot b_j, \ k = 1, \ldots, n.$$

Если таблица умножения несимметрична, то для операции умножения шифртекстов не выполняются свойства коммутативности и ассоциативности. За счёт этого гомоморфное шифрование является недетерминированным. Таблица умножения не является секретной и предъявляется в открытом виде недоверенной стороне, на которой выполняются вычисления над зашифрованными данными.

Далее рассмотрим применение гомоморфного шифрования для построения криптосистемы с открытым ключом, с помощью которой проверяется корректность вычисления полиномиальных функций над зашифрованными данными.

Описываемая криптосистема формируется на основе некоторого аналога известного алгоритма RSA [2], в котором модуль объявляется секретом. К сожалению, такая криптосистема является нестойкой, однако её можно модифицировать за счёт использования гомоморфного шифрования. Таким образом, предлагается возводить в степень предварительно зашифрованное исходное число.

Секретным ключом назовем модуль m и вектор k, которые используются в гомоморфном шифровании. В качестве открытого ключа возьмем векторы w_1, w_2 и соответствующие им взаимно простые числа u_1, u_2: $(w_i, k) \bmod m = u_i$, $i = 1, 2$, и, кроме того, выберем целое число e, обратимое по модулю $\phi(m)$, где $\phi(x)$ — функция Эйлера. В открытом ключе хранится также таблица умножения (γ_{ijk}).

Предположим, что требуется зашифровать целое число $p < 2^t < m$. Для этого сначала применим к p алгоритм гомоморфного шифрования, в результате чего получим шифртекст c. Затем подействуем на вектор c полиномиальной функцией $F(x) = x^e$:

$$F(c) = c^e = z.$$

Обратим внимание на то, что функцию F можно вычислять различными способами. Так как операция умножения шифртекстов не коммутативна и не ассоциативна, результат возведения шифртекста c в степень e определяется расстановкой скобок при выполнении умножения, например, $c{\cdot}(c{\cdot}\ldots{\cdot}c) \neq (c{\cdot}\ldots{\cdot}c){\cdot}c$. Благодаря этому алгоритм шифрования является недетерминированным.

При расшифровании необходимо сначала найти скалярное произведение (z, k) по модулю m:

$$(z, k) \bmod m = (c^e, k) \bmod m = p^e \bmod m.$$

Кроме этого, отметим, что так как вектор c получен с помощью гомоморфного шифрования, вычисление функции $F(c)$ эквивалентно вычислению функции $F(p)$. Далее для восстановления исходного числа, аналогично алгоритму RSA, результат скалярного произведения $(z, k) \bmod m$ возводится в степень $d = e^{-1} \bmod \phi(m)$:

$$(p^e \bmod m)^d = p^{ed} \bmod m = p.$$

Приведённую криптосистему с открытым ключом можно модифицировать за счёт использования более сложных полиномиальных функций, функций от нескольких переменных или за счёт операции замены переменных.

Помимо рассмотренной криптосистемы, исследована криптосистема с открытым ключом, построенная на основе шифра Хилла с использованием гомоморфного шифрования. Однако такая система сводится к описанной выше, если заменить линейное преобразование на полиномиальное и применить предложенные модификации. Поэтому в работе описан только полиномиальный вариант, который является более общим.

ЛИТЕРАТУРА

1. *Knuth D.* The Art of Computer Programming. V. 2. Seminumerical Algorithms. Addison-Wesley Pub. Co., 1981.
2. *Shamir A.* A polynomial time algorithm for breaking the basic Merkle — Hellman cryptosystem // Adv. Cryptology. 1983. P. 279–288.