УДК 519.72+004 DOI 10.31429/vestnik-19-4-20-26

Разработка математических моделей криптосистем на основе NP-полных задач, содержащих диофантовы трудности

В. О. Осипян ✉, **Э. Т. Дж. Альгариб**

Кубанский государственный университет, ул. Ставропольская, 149, Краснодар, 350040, Россия

✉ Осипян Валерий Осипович; ORCID 0000-0001-6558-7998; e-mail: v.osippyan@gmail.com

Аннотация. В рукописи задействована новая область NP-полных задач из диофантова анализа: многостепенные системы диофантовых уравнений типа Тарри–Эскотта. Приводятся математические модели криптосистем на основе известных NP-полных задач с помощью универсального диофантова языка. Описанные модели демонстрируют потенциал применения диофантовых уравнений для разработки СЗИ с высокой степенью надёжностью. Разработана математическая модель алфавитной системы защиты информации, обобщающая принцип построения криптосистем с открытым ключом — так называемую дисимметричную триграммную криптосистему. В ней прямое и обратное преобразования реализовывается по заданному алгоритму на основе многопараметрического решения многостепенной системы диофантовых уравнений.

Ключевые слова: NP-полная задача, многостепенная система диофантовых уравнений, генерация ключей, симметричная (дисимметричная) криптосистема, параметрическое решение, диофантовы трудности.

Финансирование. Исследование не имело спонсорской поддержки.

Цитирование: Осипян В. О., Альгариб Э. Т. Дж. Разработка математических моделей криптосистем на основе NP-полных задач, содержащих диофантовы трудности // Экологический вестник научных центров Черноморского экономического сотрудничества. 2022. Т. 19, № 4. С. 20–26. DOI 10.31429/vestnik-19-4-20-26

Поступила 15 ноября 2022 г. После доработки 21 ноября 2022 г. Принято 22 ноября 2022 г. Публикация 30 ноября 2022 г.

Авторы заявляют об отсутствии конфликта интересов. Авторы внесли одинаковый вклад в подготовку рукописи.

Cryptosystems Mathematical Models Design Based on NP-complete Problems Containing Diophantine Difficulties

V. O. Osipyan ✉, **E. T. J. Al Gharib**

Kuban State University, Stavropolskaya str., 149, Krasnodar, 350040, Russia

✉ Valeriy O. Osipyan; ORCID 0000-0001-6558-7998; e-mail: v.osippyan@gmail.com

Abstract. A new area of NP-complete problems from Diophantine analysis is involved in the manuscript: multistep systems of Tarry-Escott type Diophantine equations. Mathematical models of cryptosystems based on known NP-complete problems using a universal Diophantine language are presented. The described models demonstrate the potential of using Diophantine equations for the development of SPI with a high degree of reliability. A mathematical model of an alphabetic information security system has been developed that generalizes the principle of constructing cryptosystems with a public key – the so-called dissymmetric trigram cryptosystem. In it, forward and reverse transformations are implemented according to a given algorithm based on a multiparametric solution of a multi-stage system of Diophantine equations.

Keywords: NP-complete problem, multi-degree system of Diophantine equations, key generation, symmetric (dissymmetric) cryptosystem, parametric solution, Diophantine difficulties.

Funding. The study did not have sponsorship.

Cite as: Osipyan V. O., Al Gharib E. T. J. Cryptosystems mathematical models design based on NP-complete problems containing Diophantine difficulties. *Ecological Bulletin of Research Centers of the Black Sea Economic Cooperation*, 2022, vol. 19, no. 4, pp. 20–26. DOI 10.31429/vestnik-19-4-20-26

Received 15 November 2022. Revised 21 November 2022. Accepted 22 November 2022. Published 30 November 2022.
The authors declare no competing interests. The authors contributed equally.

Введение

В условиях стремительного развития сетевых и телекоммуникационных технологий, включая технологии мобильной связи, роботизированных систем, интернета вещей, цифровой экономики и технологии распределенного реестра, актуальными становятся задачи теории и практики защиты информации на всех уровнях её хранения, обработки и передачи по открытым каналам связи. Указанный факт стимулируют научные исследования, направленные на совершенствование существующих программно-аппаратных средств обеспечения информационной безопасности и разработку новых систем защиты информации (СЗИ). Поэтому важной фундаментальной научной проблемой исследования является разработка теоретико-числовых методов и алгоритмов, позволяющих построить стойкую и эффективную (с практической точки зрения) математическую модель СЗИ, основанных на новых теоретических результатах.

На основе теоретических истоков построения математических моделей эффективных СЗИ или криптосистем исходят из необходимости использования сложных математических *NP*-полных задач, решение которых потребует от нелегального пользователя больших затрат машинного времени и ресурсов. К таким задачам, следуя К. Шеннону [1], относятся задачи, содержащие диофантовы трудности, позволяющие смоделировать более стойкие математические модели СЗИ.

В работе задействована новая область *NP*-полных задач из диофантова анализа: задача параметрического решения многостепенных систем диофантовых уравнений (МСДУ) типа Тарри – Эскотта [2–4]. Особенность этих МСДУ заключается в том, что неизвестен алгоритм их параметрического решения — на основе отрицательного решения 10-й проблемы Гильберта [3].

Впервые предлагается математическая модель триграммной дисимметричной криптосистемы (ТДК), содержащих диофантовы трудности, обобщающий принцип построения криптосистем с открытым ключом [5, 6].

Описываемые в данной статье математические модели демонстрируют потенциал применения универсального диофантова языка для разработки криптосистем с высокой степенью надёжности.

1. Описание некоторых NP-полных задач с помощью диофантовых уравнений

Как известно [3], под алгебраическим диофантовым уравнением (ДУ) понимают полиномиальное уравнение

$$D(x_1, x_2, \ldots, x_n) = 0, \tag{1.1}$$

коэффициенты которого суть целые числа, и решения требуется найти тоже в целых или целых неотрицательных числах. Задача решения ДУ (1.1) или систем таких уравнений заключается в поиске целочисленных решений или доказательства того, что таких решений не существуют. Как правило, решения уравнения (1.1) задаются в виде тождества, содержащего один, два или более целочисленных параметров [2, 4].

Так, например, полиномиальное диофантово уравнение $47x - 53y = 1$ имеет следующее однопараметрическое решение: $x = 44 + 53n$, $y = 39 + 47n$, где n — целый числовой параметр, и имеет место тождество: $47(44 + 53n) - 53(39 + 47n) = 1$, что выполняется для счётного числа значений n.

Общеизвестное однородное ДУ второй степени

$$x^2 + y^2 = z^2 \tag{1.2}$$

имеет следующее двупараметрическое решение ($a, b \in Z$ — параметры) в виде пифагоровых троек:

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Более того, тождество

$$(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$$

показывает, что однородное ДУ (1.2) имеет бесконечно много решений.

Для практических приложений можно сузить множество числовых значений и для коэффициентов, и для переменных, например, до множества $Z_k = \{0, 1, \cdots, k-1\}$, $k \geqslant 2$ — кольца вычетов по модулю k.

Рассмотрим некоторые трудно вычислимые проблемы и покажем, что каждую такую проблему можно смоделировать с помощью некоторого ДУ вида (1.1). При этом решение такого уравнения позволяет устанавливать шифр соответствующей криптосистемы.

Проблема решения нестандартного аддитивного рюкзака [5]. Пусть имеются множество (рюкзак) $A = \{a_1 a_2, \ldots, a_n\}$, $a_i \in N$, $i = 1, \ldots, n$ и некоторое натуральное число c. Требуется установить существуют ли для заданного c такие значения $x_i \in Z_k = \{0, 1, \ldots, k-1\}$, для которых выполняется линейное ДУ

$$\sum_{i=1}^{n} a_i x_i = \mathrm{c}, \tag{1.3}$$

что соответствует проблеме решения нестандартного аддитивного рюкзака.

Проблема решения нестандартного мультипликативного рюкзака [7]. Аналогично можно рассмотреть проблему решения нестандартного мультипликативного рюкзака на основе следующего экспоненциального ДУ:

$$\prod_{i=1}^{n} a_i^{x_i} = \mathrm{c}. \tag{1.4}$$

Отметим, что указанные равенства (1.3) и (1.4) являются диофантовыми уравнениями над множеством Z_k при известных c(шифр) и $a_i \in N$, $i = 1, \ldots, n$.

Проблема факторизации натуральных чисел [8]. Для данного составного числа n найти натуральные числа $p, q \geqslant 2$, такие, что $n = p * q$. Отметим, что эта задача имеет большую вычислительную сложность, на основе которой построен один из самых популярных методов криптографии с открытым ключом — метод RSA.

Согласно теореме Лагранжа [8] каждое натуральное число есть сумма не более чем четырёх квадратов, и этот факт равносилен разрешимости ДУ в целых числах

$$n = (x_1 a_1^2 + x_2 a_2^2 + x_3 a_3^2 + x_4 a_4^2)(y_1 b_1^2 + y_2 b_2^2 + y_3 b_3^2 + y_4 b_4^2), \quad a, b \in N_0, \quad x_i, y_j \in \{0, 1\}.$$

Проблема расшифрования по алгоритму RSA [8]. Эта проблема заключается в нахождении вычета $x \in Z_k$, кодирующего исходный текст по его шифру $c = x^e (\mathrm{mod}\, n)$, что равносильно разрешимости ДУ

$$x^e = c + n * y$$

относительно переменных x и y при известных c и n.

Проблема дискретного логарифмирования [8].

Определение. Пусть *GF(p)* — простое поле Галуа порядка p и $a, c \in GF(p)$. Любое целое число x, для которого $a^x = c (\mathrm{mod}\, p)$, называется дискретным логарифмом c по основанию a, что записывается как $x = \log_a c (\mathrm{mod}\, p)$ или

$$x = \log_a c + p * y.$$

Из этого определения следует следующее ДУ относительно переменных x и y:

$$a^x = c + p * y.$$

Заметим, что вычисление дискретного логарифма в $GF(p)$ является трудно вычислимой задачей, когда $p - 1$ имеет большой простой множитель.

Проблема квадратичного вычета в простом поле Галуа $GF(p)$ [8]. Эта трудно вычислимая проблема сводится к разрешимости ДУ относительно переменных x и y при известных a и p:

$$x^2 = a + p * y.$$

Можно рассмотреть и другие, не менее интересные, NP-полные задачи, которые также сводятся либо к ДУ, либо к системе ДУ.

2. Математическое моделирование дисимметричной триграммной криптосистемы, содержащей диофантовы трудности

В предыдущем пункте были рассмотрены различные криптосистемы и приведены соответствующие им ДУ, что можно представить в виде следующего, более общего, диофантово уравнения

$$D(x_1, x_2, \ldots, x_n) = 0,$$

где D — целозначная функция с целозначными аргументами $x_1, x_2, \ldots, x_n$.

Особый интерес в данной работе будут представлять многостепенные системы диофантовых уравнений (МСДУ) размерности m порядка (или степени) n вида

$$X_1^k + X_2^k + \ldots + X_m^k = Y_1^k + Y_2^k + \ldots Y_m^k, \quad k = 1, \ldots, n$$

или в компактной записи

$$X_1, X_2, \ldots, X_m \stackrel{n}{=} Y_1, Y_2, \ldots, Y_m. \tag{2.1}$$

Для краткости эту запись представим ещё в виде

$$X \stackrel{n}{=} Y,$$

где $X = X_1, X_2, \ldots, X_m$, $Y = Y_1, Y_2, \ldots, Y_m$, а её многопараметрическое решение — в виде $A \stackrel{n}{=} B$, где $A = a_1, a_2, \ldots, a_m$, $B = b_1, b_2, \ldots, b_m$, где a_i, b_i — целочисленные параметры.

Определение. Два упорядоченных набора чисел или параметров

$$A = \mathrm{a}_1, a_2, \ldots, a_m \text{ и } B = b_1, b_2, \ldots, b_m$$

размерности m равносильны со степенью n, если они удовлетворяют МСДУ

$$X_1, X_2, \ldots, X_m \stackrel{n}{=} Y_1, Y_2, \ldots, Y_m,$$

то есть выполняются равенства для всех значений 1, 2, . . . , n,

$$a_1, a_2, \ldots, a_m \stackrel{n}{=} b_1, b_2, \ldots, b_m.$$

Так, например, следующие двупараметрические упорядоченные наборы, размерности $m = 5$ равносильны между собой и имеют степень $n = 4$:

$$19a + b,\ 15a + 5b,\ 11a + 9b,\ 3a + 17b,\ 2a + 18b \stackrel{4}{=} a + 19b,\ 5a + 15b,\ 9a + 11b,\ 17a + 3b,\ 18a + 2b.$$

Из этих параметрических равносильностей можно получить сколь угодно много равносильных целых числовых наборов размерности $m = 5$ степени $n = 4$,придав параметрам a и b различные целые или натуральные числовые значения.

Более того, для заданных допустимых значений mи n имеет место следующие утверждения [6].

Теорема 1. Из равносильности двух целых числовых упорядоченных наборов (или наборов упорядоченных параметров) размерности m степени n

$$a_1, a_2, \ldots, a_m \stackrel{n}{=} b_1, b_2, \ldots b_m$$

следует равносильность также следующих наборов (или наборов упорядоченных параметров)

$$a_1, a_2, \dots, a_m, -b_1, -b_2, \dots, -b_{m-1} \overset{n}{=} b_m$$

или в более общем случае для любого натурального $i \in 1, \dots, m$

$$a_1, a_2, \dots, a_m, -b_1, -b_2, \dots, -b_{l-1} \overset{n}{=} b_l, b_{l+1}, \dots, b_m.$$

Для удобства перепишем эту теорему ещё в виде

Теорема 1. Если $a_1, a_2, \dots, a_m \overset{n}{=} b_1, b_2, \dots, b_m$, то для любого натурального числа $i \in 1, \dots, m$ имеет место соотношение $A, -B^i \overset{n}{=} b_{i+1}, b_{i+2}, \dots, b_m$.

Как уже было отмечено выше, особенность МСДУ заключается в том, что неизвестны общие не переборные методы их решения для любых m и n [3]. В то же время для отдельных значений m и n они допускают параметризацию по одному, двум и более параметрам, из которых можно получить конкретные решения в целых или натуральных числах $a_1, a_2, \dots, a_m, b_1, b_2, \dots, b_m$ таких, что выполняются равенства [7]

$$a_1, a_2, \dots, a_m \overset{n}{=} b_1, b_2, \dots, b_m. \tag{2.2}$$

Заметим, что по найденному решению (2.2) МСДУ восстановить числовые значения её параметров за приемлемое время не представляется возможным. Кроме того, на практике вычисления производятся для достаточно больших натуральных чисел, так что стандартные средства вычислений зачастую неприменимы. Поэтому для разработки эффективной СЗИ на основе параметрических решений МСДУ необходимо в зависимости от размерности m и степени n учитывать либо сложность решения системы (2.1), либо сами решения, либо и то, и другое одновременно. Необходимые определения и факты можно найти в работе [9].

Как известно [9], математическую модель произвольной алфавитной криптосистемы можно представить в виде следующего кортежа:

$$\sum_0 = \langle M^*, Q, C^*, E(m), D(c) | V(E(m), D(c)) \rangle,$$

где M^* – множество всех сообщений $m = m_1 m_2 \dots m_k$ (открытых текстов) над алфавитом M; Q — множество всех числовых эквивалентов элементарных сообщений m_i (в частности буквы или конкатенация букв из алфавита M); C^* — множество всех криптограмм $c = c_1 c_2 \dots c_k$ над алфавитом C; $E(m)$ — алгоритм прямого преобразования открытого текста $m = m_1 m_2 \dots m_k$; $D(c)$ — алгоритм обратного преобразования криптограммы $c = c_1 c_2 \dots c_k$; $V\,(E(m), D(c))$ — связь однозначности между алгоритмами $E(m)$ и $D(c)$.

Приведём математическую модель алфавитной дисимметричной криптосистемы (ДК), элементарными сообщениями которой суть триграммы: $m_{2i-1} m_{2i} m_{2i+1}$. Пусть для определённости открытый текст $m = m_1 m_2 \dots m_k$ состоит из заглавных букв английского 27-буквенного алфавита от A до Z и пробела со множеством всех числовых эквивалентов $q \in Q = \{0, 1, \dots, 26\}$ элементарных сообщений $m_i \in M^*$.

Числовой эквивалент $\tilde{q}_i$ триграммы $m_{2i-1} m_{2i} m_{2i+1}$ сообщения m определим как трёхзначное число по основанию 27 (предварительно исходное сообщение m разбиваем на триграммы с добавлением пробелов таким образом, чтобы каждый блок содержал три буквы)

$$\tilde{q}_i = 27^2 q_{2i-1} + 27 q_{2i} + q_{2i+1} \in \{0, 1, \dots, 19682\}.$$

Допустим, определены следующие равносильные векторы:

$$A^l = (a_1, \dots, a_l), \quad B^l = (b_1, \dots, b_l), \quad A^l \overset{k}{=} B^l, \quad 1 < k < l.$$

На их основе построим параметрическое решение МСДУ (2.1) с параметрами a и b по следующему правилу:

$$v_i = \begin{cases} a_i a + b_i b, & i = 1, \ldots, l, \\ b_{i-l} a + a_{i-l} b, & i = (l+1), \ldots, 2l. \end{cases}$$

С помощью этого параметрического решения определим функции прямого преобразования $C_L(ab)$ открытого текста m и обратного преобразования $C_R(ab)$ криптограммы c, считая, что a — триграммный шифр, а b — закрытый ключ: для фиксированной степени d, $1 \leqslant d \leqslant k$ генерируем функции прямого и обратного преобразований как

$$E\left(m_{2i-1} m_{2i} m_{2i+1}\right) = C_L(a,b) = v_1^d + v_2^d + \ldots + v_r^d = c_i, \quad r < 2l,$$

$$C_R(a,b) = v_{r+1}^d + v_{r+2}^d + \ldots + v_{2l}^d = c_i,$$

причём $D(c_i)$ — решение уравнения $v_{r+1}^d + v_{r+2}^d + \ldots + v_{2l}^d = c_i$, $1 < d \leqslant k$.

Количество слагаемых в правой части функции обратного преобразования $C_R(a,b)$ можно довести до минимума, например, до одного слагаемого (см. теорему 1): $C_R(a,b) = v_{2l}^d$, $1 < d \leqslant k$.

Заключение

Для практических приложений следует выбрать подходящую МСДУ и соответствующие им соотношения (см. теорему 1). В рассмотренном выше примере ТДК выбран простой вариант функции прямого преобразования, а для практических приложений можно предложить сложный алгоритм для выбора указанной функции.

В рукописи разработана математическая модель триграммной ДК, содержащих диофантовы трудности. Как следует из сказанного выше, для определения числовых эквивалентов элементарных сообщений легальный пользователь решает простое уравнение заданной степени, а нелегальный — многовариативную МСДУ заданной размерности и порядка.

Решение поставленных в рукописи задач позволит получить научно-технический задел для разработки и дальнейшей реализации стойких и эффективных математических моделей алфавитных СЗИ, а также дать новый импульс в развитии математического моделирования криптосистем, содержащих диофантовы трудности.

Литература [References]

1. Shannon, C., Communication theory of secrecy systems. *Bell System Techn. J.*, 1949, vol. 28, iss. 4., pp. 656–715.
2. Dorwart, H.L., Brown, O.E., The Tarry-Escott problem. *Amer. Math. Monthly*, 1937, vol. 44, iss. 10, pp. 613–626.
3. Матиясевич, Ю.В., *Десятая проблема Гильберта*. Наука, Москва, 1993. [Matiyasevich, Yu.V., *Desyataya problema Gil'berta = Hilbert's tenth problem*. Nauka, Moscow, 1993.]
4. Carmichael, R.D., *The theory of numbers and diophantine analysis*. New York, 1959.
5. Саломаа, А., *Криптография с открытым ключом*. Мир, Москва, 1995. [Salomaa, A., *Kriptografiya s otkrytym klyuchom = Public key cryptography*. Mir, Moscow, 1995. (in Russian)]
6. Осипян, В.О., Разработка математической модели дисимметричной биграммной криптосистемы на основе параметрического решения многостепенной системы диофантовых уравнений. *Сетевой научный журнал «Инженерный вестник Дона»*, 2020, № 6. [Osipyan, V.O., Development of a mathematical model of a dissymmetric bigram cryptosystem based on the parametric solution of a multi-degree system of Diophantine equations. *Setevoy nauchnyy zhurnal "Inzhenernyy vestnik Dona" = Web Scientific Journal "Engineering Bulletin of the Don"*, 2020, no. 6. (in Russian)] URL: http://ivdon.ru/ru/magazine/archive/N6y2020/6534
7. Осипян, В.О., *Разработка математических моделей систем защиты информации, содержащих диофантовы трудности*. Кубанский гос. ун-т, Краснодар, 2021. [Osipyan, V.O., *Razrabotka matematicheskikh modeley sistem zashchity informatsii, soderzhashchikh diofantovy trudnosti = Development of mathematical models of information security systems containing Diophantine difficulties*. Kuban State University, Krasnodar, 2021. (in Russian)]

8. Koblitz, N.A., *Course in number theory and cryptography*. Springer-Verlag, New York, 1987.
9. Осипян, В.О., Литвинов, К.И., Жук, А.С., Разработка математических моделей систем защиты информации на основе многостепенных систем диофантовых уравнений. *Экологический вестник научных центров Черноморского экономического сотрудничества*, 2019, т. 16, № 3, с. 6–15. [Osipyan, V.O., Litvinov, K.I., Zhuk, A.S., Development of mathematical models of information security systems based on multi-degree systems of Diophantine equations. *Ekologicheskiy vestnik nauchnykh tsentrov Chernomorskogo ekonomicheskogo sotrudnichestva = Ecological Bulletin of Research Centers of the Black Sea Economic Cooperation*, 2019, vol. 16, no. 3, pp. 6–15. (in Russian)] DOI 10.31429/vestnik-16-3-6-15