Математика

УДК 519.72+004 DOI: 10.31429/vestnik-16-3-6-15

РАЗРАБОТКА МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ МНОГОСТЕПЕННЫХ СИСТЕМ ДИОФАНТОВЫХ УРАВНЕНИЙ

Осипян В. О., Литвинов К. И., Жук А. С.

DEVELOPMENT OF MATHEMATICAL MODELS OF SYSTEMS OF PROTECTION DATA ON THE BASIS OF THE MULTISTAGE SYSTEMS OF DIOPHANTINE EQUATIONS

Osipyan V. O., Litvinov K. I., Zhuk A. S.

Kuban State University, Krasnodar, 350040, Russia
e-mail: lyrik-1994@yandex.ru

Abstract. The objective necessity of improvement of information security systems (SPI) in the conditions of development of information and telecommunication technologies is shown. Theorems which allow to describe the properties of parametric solutions of multistage systems of Diophantine equations necessary for the development of mathematical models of SPI on their basis are given. The theorem generalizing the known Frolov's theorem is presented, and the author's theorem on the basis of which the mathematical model of SPI containing Diophantine difficulties is developed is given.

A new approach to the development of SPI generalizing the principle of construction of public key cryptosystems is proposed. One part of the conditional identity is used for the direct transformation of the original message, and the other part – for the inverse transformation. A new concept of equivalence of ordered sets of numbers or parameters with a given dimension and degree is introduced.

Mathematical models of cryptosystems developed on the basis of two-parameter solutions of multistage systems of Diophantine equations, in particular, – equations of the fifth degree with the number of variables equal to twelve are presented. The described mathematical models demonstrate the potential of using Diophantine equations for the development of SPI with a high degree of reliability. These models allow to build asymmetric GIS, and the system public key. Such systems contain Diophantine difficulties admitting the existence of a countable set of equally probable keys.

Keywords: information technologies, information security system, information encryption, symmetric cryptosystem, public key cryptosystem, multi-level system of Diophantine equations, Diophantine difficulties, Diophantine set, Diophantine representation.

Введение

Для построения моделей эффективных систем защиты информации следует применять сложные математические задачи, требующие от криптоаналитика больших затрат машинного времени и ресурсов на их решение. К таким задачам, следуя К. Шеннону [1], относятся задачи, содержащие диофантовы трудности, применение которых позволяют увеличить множество перебираемых ключей до счётного множества. Новый подход, развиваемый в данной статье, использует многостепенные системы диофантовых уравнений и задачи, находящиеся на стыке теории защиты данных и проблемы Проухета – Тарри – Эскотта [2].

Основная идея данной работы состоит в построении математической модели криптосистемы, содержащей диофантовы трудно-

Осипян Валерий Осипович, д-р физ.-мат. наук, доцент, профессор кафедры информационных технологий Кубанского государственного университета; e-mail: v.osippyan@gmail.com.

Литвинов Кирилл Игоревич, аспирант кафедры информационных технологий Кубанского государственного университета; e-mail: lyrik-1994@yandex.ru.

Жук Арсений Сергеевич, старший преподаватель кафедры вычислительных технологий Кубанского государственного университета; e-mail: arseniyzhuck@mail.ru.

Работа выполнена при финансовой поддержке гранта РФФИ (проект 19-01-00596).

сти. Как отмечал К. Шеннон [1], наибольшей неопределённостью при подборе ключей обладают системы защиты информации (СЗИ), содержащие диофантовы трудности.

В первой части работы приведены основные понятия, определения и теоремы теории диофантовых и систем диофантовых многостепенных уравнений, а также некоторые факты, используемые в дальнейшем при построении математических моделей эффективных СЗИ на их основе. В частности, приведены теоремы, которые позволяют описать свойства параметрических решений таких уравнений. Вводится новое понятие о равносильности параметрических и числовых наборов заданной размерности и степени.

Во второй части работы приведены авторские математические модели алфавитных криптосистем на основе многостепенных систем диофантовых уравнений пятой степени, содержащих диофантовы трудности, как для дисимметричной СЗИ, так и для СЗИ с открытым ключом.

Основные понятия, определения и факты из диофантова анализа

Предварительно приведём некоторые факты, используемые в дальнейшем при построении математической модели систем защиты информации, содержащей диофантовы трудности.

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

$$f(x_1, x_2, \ldots, x_n) = 0, \qquad (1)$$

коэффициенты которого суть целые числа, и решения требуется найти тоже в целых или целых неотрицательных числах. Задача решения диофантова уравнения (1) заключается в поиске параметрических или целочисленных решений этого уравнения или доказательства того, что таких решений нет.

Наряду с отдельными диофантовыми уравнениями вида (1) часто рассматривают также семейства диофантовых уравнений вида [3]

$$F(a_1, a_2, \ldots, a_k, x_1, x_2, \ldots, x_r) = 0, \qquad (2)$$

зависящие от k параметров $a_1, a_2, \ldots, a_k$ и r неизвестных переменных $x_1, x_2, \ldots, x_r$ (такое деление носит условный характер) так, что $k + r = n$ — общее число переменных уравнения (2). Каждое такое семейство определяет некоторое множество D^k упорядоченных наборов из k чисел — множество тех значений параметров $a_1, a_2, \ldots, a_k$, при которых уравнение (2) разрешимо относительно неизвестных переменных $x_1, x_2, \ldots, x_r$ (иногда — в целых неотрицательных числах):

$$D^k = \{(a_1, a_2, \ldots, a_k) \mid F(a_1, a_2, \ldots, a_k, x_1, x_2, \ldots, x_r) = 0\}. \qquad (3)$$

Такое множество (3) называют диофантовым, число k называют его размерностью, а соответствующее уравнение (2) — его диофантовым представлением [3]. Другими словами, множество, имеющее диофантово представление, будем называть диофантовым.

В общем случае, технически достаточно сложно ответить на такой естественный вопрос: диофантово ли заданное множество. В данной статье рассматривается диофантово представление множества числовых эквивалентов элементарных сообщений алфавитных криптосистем, в частности, криптосистемы, построенные на основе многостепенной системы диофантовых уравнений заданной степени и размерности [4–7]. Поэтому приведём также основные понятия, определения теории диофантовых и систем многостепенных диофантовых уравнений, включая некоторые факты [2,8–12], используемые нами в дальнейшем при разработке математических моделей алфавитных криптосистем.

Многостепенные системы диофантовых уравнений: определения и факты

Как известно, с помощью диофантовых и систем многостепенных диофантовых уравнений удается разрешить некоторые чрезвычайно важные в практическом отношении задачи дискретной математики, в частности, задачи теории защиты информации, не разрешимые обычными классическими методами.

В данной статье рассматривается аспект приложения многостепенных систем диофантовых уравнений при моделировании эффективных систем защиты информации, содержащих диофантовы трудности. Особый интерес в этой связи будут представлять многостепенные системы диофантовых уравнений

размерности m степени n вида [2, 8–13]

$$\begin{cases} X_1 + X_2 + \ldots + X_m = \\ \qquad = Y_1 + Y_2 + \ldots + Y_m, \\ X_1^2 + X_2^2 + \ldots + X_m^2 = \\ \qquad = Y_1^2 + Y_2^2 + \ldots + Y_m^2, \\ \qquad \ldots \\ X_1^{n-1} + X_2^{n-1} + \ldots + X_m^{n-1} = \\ \qquad = Y_1^{n-1} + Y_2^{n-1} + \ldots + Y_m^{n-1}, \\ X_1^n + X_2^n + \ldots + X_m^n = \\ \qquad = Y_1^n + Y_2^n + \ldots + Y_m^n \end{cases} \tag{4}$$

или в её компактной записи

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

или в виде

$$X_1, X_2, \ldots, X_m \overset{\text{n}}{=} Y_1, Y_2, \ldots, Y_m.$$

Для краткости, запись (4) представим в виде

$$X \overset{\text{n}}{=} Y,$$

где $X = X_1, X_2, \ldots, X_m, Y = Y_1, Y_2, \ldots, Y_m$, а целое параметрическое решение системы — в виде

$$A \overset{\text{n}}{=} B,$$

где $A = a_1, a_2, \ldots, a_m, B = b_1, b_2, \ldots, b_m$.

Многостепенная система вида

$$X_1, X_2, \ldots, X_{n+1}, X_{n+2} \overset{\text{n}}{=} \\ \overset{\text{n}}{=} Y_1, Y_2, \ldots, Y_{n+1}, Y_{n+2}$$

называется почти идеальной, а система вида

$$X_1, X_2, \ldots, X_{n+1} \overset{\text{n}}{=} Y_1, Y_2, \ldots, Y_{n+1}$$

идеальной или нормальной системой [10, 12].

Так как при $n \geqslant m$ система (4) имеет лишь тривиальные решения (см. теорему Bastien) [11], совокупность $a_1, a_2, \ldots, a_m$ значений переменных $X_1, X_2, \ldots, X_m$ отличается от совокупности $b_1, b_2, \ldots, b_m$ значений переменных $Y_1, Y_2, \ldots, Y_m$ лишь порядком следования значений, т.е. $\{a_1, a_2, \ldots, a_m\} = \{b_1, b_2, \ldots, b_m\}$, то исследуются только параметрическое решение многостепенной системы диофантовых уравнений n-ой степени (4), для которых $n < m$.

В общем случае проблемы, связанные с системами диофантовых уравнений, трудно решаются [3]: неизвестны общие неперебор-ные методы их решения для любых m и n (см. десятую проблему о разрешимости диофантова уравнения [3]). В то же время некоторые из таких уравнений допускают параметризацию по одному, двум и более параметрам $t_1, t_2, \ldots, t_k$ в виде

$$X_i = X_i(t_1, t_2, \ldots, t_r), Y_i = Y_i(t_1, t_2, \ldots, t_r), \quad i = 1, \ldots, m,$$

из которых можно получить решения в натуральных или целых числах $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m$ таких, что для всех $n < m$ имеют место числовые тождества

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

Теперь рассмотрим некоторые примеры многостепенных систем диофантовых уравнений (4) для различных параметров m и n.

Так, для $m = 4, n = 3$ приведём следующую идеальную или нормальную многостепенную систему диофантовых уравнений третьей степени с четырьмя переменными

$$X_1, X_2, X_3, X_4 \overset{3}{=} Y_1, Y_2, Y_3, Y_4$$

и одно из её взаимно-простых решений

$$1, 8, 10, 17 \overset{3}{=} 2, 5, 13, 16,$$

что означает справедливость следующих равенств для n = 1, 2, 3:

$$1 + 8 + 10 + 17 = 2 + 5 + 13 + 16,$$

$$1^2 + 8^2 + 10^2 + 17^2 = 2^2 + 5^2 + 13^2 + 16^2,$$

$$1^3 + 8^3 + 10^3 + 17^3 = 2^3 + 5^3 + 13^3 + 16^3,$$

причём наибольший общий делитель (НОД) указанного решения — $d = (1, 8, 10, 17, 2, 5, 13, 16) = 1$.

При $m = 6$, $n = 5$ имеем следующую нормальную многостепенную систему диофантовых уравнений пятой степени

$$X_1, X_2, \ldots, X_6 \overset{5}{=} Y_1, Y_2, \ldots, Y_6.$$

и его одно частное решение

$$1, 6, 7, 17, 18, 23 \overset{5}{=} 2, 3, 11, 13, 21, 22.$$

На основе этого решения можно получить следующую систему тождеств (см. Теорему 3) для $n = 1, \ldots, 5$:

$$(a+2b)^n + (6a+3b)^n + (7a+11b)^n + \\ + (17a+13b)^n + (18a+21b)^n + (23a+22b)^n = \\ = (2a+b)^n + (3a+6b)^n + (11a+7b)^n + \\ + (13a+17b)^n + (21a+18b)^n + (22a+23b)^n.$$

Для удобства введём также следующие обозначения и определения. Если

$$A = a_1, a_2, \ldots, a_m, \quad B = b_1, b_2, \ldots, b_m$$

— два числовых упорядоченных набора или наборы параметров размерности m, то для заданных целых чисел a, b, c и d определим:

1. $A^i = a_1, a_2, \ldots, a_i, i \in 1, \ldots, m$;
2. $aA = aa_1, aa_2, \ldots, aa_m$;
3. $A \pm B = a_1 \pm b_1, a_2 \pm b_2, \ldots, a_m \pm b_m$;
4. $A \pm a = a_1 \pm a, a_2 \pm a, \ldots, a_m \pm a$; (5)
5. $A, B = a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m$;
6. $aA \pm c, bB \pm d = aa_1 \pm c, aa_2 \pm c, \ldots,$ $aa_m \pm c, bb_1 \pm d, bb_2 \pm d, \ldots, bb_m \pm d$.

Определение. Два упорядоченных набора чисел или параметров $A = a_1, a_2, \ldots, a_m$ и $B = b_1, b_2, \ldots, b_m$ размерности m равносильны со степенью n, если они удовлетворяют многостепенной системе диофантовых уравнений (4)

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

то есть выполняются равенства для всех значений $1, 2, \ldots, n$:

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

Легко убедиться, что введённое бинарное отношение относительно упорядоченных наборов параметров A и B представляет собой условное алгебраическое тождество, и оно является отношением равносильности, т.к. обладает следующими свойствами:

1. $A \overset{\text{n}}{=} A$ (рефлексивность);

2. Если $A \overset{\text{n}}{=} B$, то $B \overset{\text{n}}{=} A$ (симметричность);

3. Если $A \overset{\text{n}}{=} B, B \overset{\text{n}}{=} C$ то $A \overset{\text{n}}{=} C$ (транзитивность).

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

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

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 m и n имеет место следующие утверждения.

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

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

следует равносильность также следующих наборов (или наборов упорядоченных параметров)

$$a_1, a_2, \ldots, a_m, -b_1, -b_2, \ldots, -b_{m-1} \overset{\text{n}}{=} b_m, \quad (6)$$

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

$$a_1, a_2, \ldots, a_m, -b_1, -b_2, \ldots, -b_{l-1} \overset{\text{n}}{=} \\ \overset{\text{n}}{=} b_l, b_{l+1}, \ldots, b_m. \quad (7)$$

Для удобства перепишем данную теорему в следующем виде

Теорема 1. (Осипян). Если

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

то для любого натурального $i \in 1, \ldots, m$

$$A, -B^i \overset{\text{n}}{=} b_{i+1}, b_{i+2}, \ldots, b_m.$$

Для разработки практических приложений, в частности, криптосистем, нам необходимо будет также следующие теоремы.

Теорема 2. (Фролов, [11]). Если $A \overset{\text{n}}{=} B$, то $aA + b \overset{\text{n}}{=} aB + b$, где $a \neq 0, b$ – – целые числа. В частности, если $a = 1, b = h$, то $A + h \overset{\text{n}}{=} B + h$

Введем также теорему, обобщающую данную теорему Фролова.

Теорема 3. (Осипян). Если $A \overset{n}{=} B$, то $aA + bB \overset{n}{=} bA + aB$.

Приведём также утверждение теоремы Тарри [11], которое позволяет получить решение нормальной многостепенной системы диофантовых уравнений $(n+1)$-ой степени, исходя из соответствующего решения n-ой степени.

Теорема 4. (Тарри [11]). Если $A \overset{n}{=} B$, то $A, B + h \overset{n+1}{=} B, A + h$.

На основе указанных теорем можно доказать следующую основную теорему, позволяющую разрабатывать математические модели СЗИ с заранее заданными критериями на надёжность.

Теорема 5. (Осипян). Пусть имеются две пары равносильных упорядоченных наборов параметров (функциональных ранцев) размерности m степени n, причём первая пара A и B представляет собой произвольное параметрическое решение многостепенной системы диофантовых уравнений n-ой степени размерности m

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

а вторая — C и D любое расширение первой, полученной на основе Теорем 1–4:

1. $(a_1, a_2, \ldots, a_m) \overset{n}{=} (b_1, b_2, \ldots, b_m)$, (или $A \overset{n}{=} B$), $1 \leqslant n < m$;

2. $(c_1, c_2, \ldots, c_k) \overset{n+t}{=} (d_1, d_2, \ldots, d_k)$, (или $C \overset{n+t}{=} D$),$t \geqslant 1, 1 \leqslant n + t < k$.

Тогда первую пару A и B можно взять за основу при разработке математической модели симметричной СЗИ в качестве закрытых ключей, а пару C и D — математической модели асимметричной СЗИ в качестве открытых ключей.

Приведённые Теоремы 2—4 будут необходимы для увеличения размерности m, а также степени n равносильных наборов (числовых или параметрических) при разработке математических моделей СЗИ на основе равносильностей (6)–(7) (см. Теорему 1) совместно с соотношениями (5). При этом указанные равносильности будем использовать для прямого и обратного преобразований обрабатываемой информации следующим образом: предварительно разбиваем их на две части — одну часть будем применять по заданному алгоритму при прямом преобразовании открытого текста, а другую часть — при обратном преобразовании закрытого текста с помощью блоков заданной длины, т.е. количеством параметров соответствующей системы диофантовых уравнений.

Примеры математических моделей систем защиты информации на основе многостепенных систем диофантовых уравнений

Предварительно представим математическую модель алфавитной криптосистемы, разработанной в [4], в виде следующего кортежа:

$$\sum = \langle M^*, Q, C^*, E(m), D(c) \mid V(E(m), D(c)) \rangle. \quad (8)$$

Здесь M^* множество всех сообщений $m = m_1, m_2, \ldots, m_k$ (открытых текстов) над буквенным или числовым алфавитом M, $m_i, i = 1, \ldots, k$ — элементарные сообщения (в частности, буквы или конкатенация букв из алфавита M); Q — множество всех числовых эквивалентов элементарных сообщений m_i из M^*, C^* — множество всех шифртекстов (криптограмм) $c = c_1 c_2 \ldots c_k$ над алфавитом C, в частности, возможно $M = Q = C$. $E(m)$ — алгоритм прямого преобразования (шифрования) сообщения m в c; $D(c)$ — алгоритм обратного преобразования (дешифрования) шифртекста (криптограммы) c в $m \in M^*$. Подчеркнем, что алгоритмы $E(m)$ и $D(c)$ алфавитной криптосистемы (8) связаны между собой таким образом — $V(E(m), D(c))$, что всегда произвольное сообщение $m = m_1 m_2 \ldots m_k \in M^*$ однозначно преобразовывается в соответствующую криптограмму (шифртекст) $c = c_1 c_2 \ldots c_k \in C^*$ и, обратно: по криптограмме c всегда однозначно восстанавливается переданное сообщение m.

Альтернативным обозначением алгоритмов $E(m)$ и $D(c)$ для алфавитной криптосистемы (8) является K_E (или F_E) и K_D (или F_D) соответственно — как принято считать в классической криптографии [14–17]. Иначе их можно назвать ключами (или функциями) шифрования и дешифрования соответственно, причём авторы не претендуют на полноту освещения аналогичных математических моделей алфавитных криптосистем

(8), преследуя цель формального описания произвольной криптосистемы.

Прежде всего, заметим, что прямое преобразование открытого текста m, состоящего из одного элементарного сообщения m_1 или конкатенации таких сообщений m_1m_2, осуществляется путем равномерного увеличения длины ключа этого преобразования. Так, например, если в качестве элементарного сообщения выступает одна буква $m_i = *$ с числовым эквивалентом q_i, например, получаемый на основе стандартного ранца (аддитивного или мультипликативного) длины n, то конкатенации $m_im_j = **$ будет соответствовать числовой эквивалент q_iq_j длины $2 * n$, имеющий блоковую структуру. Можно указать и другие способы установления размерностей на основании утверждений, приведённых в работе [4].

Теперь перейдём к построению математических моделей СЗИ, исходя из вышеизложенного. Все модели систем защиты информации данного пункта строятся на основании Теорем 1–5.

Дисимметричная биграммная криптосистема на основе решения многостепенного диофантова уравнения пятой степени

Проиллюстрируем предложенный выше подход для построения математической модели алфавитной дисимметричной биграммной криптосистемы на основе двупараметрического (a и b — параметры) решения

$$X_1 = a + 3b, \quad X_2 = 9a + 4b,$$

$$X_3 = 12a + 19b, \quad X_4 = 28a + 21b,$$

$$X_5 = 31a + 36b, \quad X_6 = 39a + 37b,$$

$$X_7 = -4a - 9b, \quad X_8 = -19a - 12b,$$

$$X_9 = -21a - 28b, \quad X_{10} = -36a - 31b,$$

$$X_{11} = -37a - 39b, \quad Y = 3a + b$$

однородного многостепенного диофантова уравнения пятой степени

$$X_1^5 + X_2^5 + \ldots + X_{11}^5 = Y^5, \qquad (9)$$

полученное из числового решения (см. Теорему 3):

$$1, 9, 12, 28, 31, 39 \stackrel{5}{=} 3, 4, 19, 21, 36, 37.$$

Отметим, что данная дисимметричная биграммная криптосистема со сложной степенной гаммой

$$y = 3b, 4b, 19b, 21b, 36b, 37b, \\ - 9b, -12b, -28b, -31b, -39b,$$

составляющей вторые слагаемые решения уравнения (9), где b — закрытый ключ, содержит элементарные сообщения 27-буквеного алфавита, состоящего из заглавных букв английского языка и пробела $M = \{A, B, C, \ldots, Z, \_\}$ с числовыми эквивалентами $Q = \{0, 1, 2, \ldots, 26\}$ в указанном порядке. Числовой эквивалент биграммы (предварительно исходное сообщение m разбиваем на биграммы с добавлением пробела, если m содержит нечётное число элементарных сообщений), состоящей из двух букв m_i и m_{i+1} с числовыми эквивалентами q_i, и $q_{i+1} \in Q$, определяем как целое число

$$27q_i + q_{i+1} \in \{0, 1, \ldots, 728\}.$$

Так, например, биграмме DI соответствует целое число $27 * 3 + 8 = 89$.

Для удобства и простоты изложения пусть исходное сообщение m имеет вид: $m = DIOPHANT$. Алгоритмы $E(m)$ и $D(c)$ математической модели алфавитной дисимметричной биграммной криптосистемы определим на основе модифицированного соотношения (6) (см. Теорему 1)

$$a_1, a_2, \ldots, a_m, -b_1, -b_2, \ldots, -b_{m-1} \stackrel{\text{n}}{=} b_m,$$

предполагая, что n равен, например, только пяти (в самом деле n может принимать значения от 1 до 5).

Примем следующие обозначения:

$$C_L(a, b) = (a + 3b)^5 + (9a + 4b)^5 + \\ (12a + 19b)^5 + (28a + 21b)^5 + \\ + (31a + 36b)^5 + (39a + 37b)^5 - \\ - (4a + 9b)^5 - (19a + 12b)^5 - (21a + 28b)^5 - \\ - (36a + 31b)^5 - (37a + 39b)^5 \qquad (10)$$

— функция прямого преобразования биграммы a с наложенной гаммой y, полученная на основе двупараметрического решения уравнения (9);

$$C_R(a, b) = (3a + b)^5 \qquad (11)$$

— правая часть уравнения (11) и является функцией (закрытый ключ) обратного преобразования; $C_L(m_i, b) = c$ — шифр биграммы m_i с закрытым ключом b. Заметим, что шифрование исходного текста m выполняется функцией $C_L(a, b)$, а дешифруется — другой функцией $C_R(a, b)$.

Так, например, шифр с первой биграммы $m_1 = DI$ исходного сообщения m при закрытом ключе b, например, $b = 9$ определяем на основе (10) как числовое значение $C_L(a, b)$ при $a = 89$ (числовой эквивалент биграммы $m_1 = DI$).

Имеем

$$c = C_L(89, 9) = 1601568101376.$$

Перед нелегальном пользователем предстоит трудно вычислимая задача — найти параметрическое решение уравнения (9), для которого

$$c = 1601568101376,$$

и установить значение числового эквивалента биграммы a, т.е. решить уравнение

$$X_1^5 + X_2^5 + \ldots + X_{11}^5 = 1601568101376.$$

Задача определения легальным пользователем того же значения a сводиться в соответствии с (11) к решению следующего простого линейного диофантова уравнения

$$m_1 = C_R(a, 9) = y^5 = (3a + 9)^5 = \\ = 1601568101376$$

или

$$y = 3a + 9 = (1601568101376)^{1/5} = 276,$$

откуда $3a = 267$, $a = 89$, т.е. было передано $m_1 = DI$. Аналогично поступаем и для других биграмм исходного открытого текста $m : m_2 = OP, m_3 = HA, m_4 = NT$.

Очевидно, затраты у легального и нелегального пользователей не соизмеримы: легальный пользователь решает линейное диофантово уравнение, а нелегальный — многовариативное многостепенное диофантово уравнение пятой степени. Отметим также особо: фактически функция прямого преобразования $C_L(a, b)$ биграммы a с закрытым ключом b представляет часть двупараметрического решения уравнения (9) и содержит сложную степенную гамму y, состоящую из последовательности: $3b, 4b, 19b, 21b, 36b, 37b, -9b, -12b, -28b, -31b, -39b$, где b закрытый ключ. Поэтому установить правую часть по левой, не зная наложенную гамму y, является трудновычислимой для криптоаналитика задачей.

Асимметричная криптосистема на основе многостепенного диофантова уравнения пятой степени

Для удобства и простоты изложения рассмотрим математическую модель асимметричной криптосистемы на основе двупараметрического решения того же уравнения (9)

$$X_1^5 + X_2^5 + \ldots + X_{11}^5 = y^5.$$

Вначале определим значение модуля $U = U(q_a, q_b)$ как число большее, чем $y^5 = (3q_a + q_b)^5$, например, $y^5 + 1$ для двух наибольших числовых эквивалентов q_a и q_b для букв a и b заданного открытого текста m (в самом деле для практического приложения можно применить более эффективное распределение секрета). Затем определим открытый ($OK = w$) и закрытый ($PK = v$) ключи таким образом, чтобы выполнялось условие:

$$(w, v) \equiv 1 \pmod{U}.$$

Далее определим функции прямого и обратного преобразований данной асимметричной криптосистемы как $C_L(a, b, w)$ и $C_R(a, b, v)$ соответственно (здесь b, как и для дисимметричной биграммной криптосистемы, закрытый ключ):

$$C_L(a, b, w) = w^5 * ((a + 3b)^5 + \\ + (9a + 4b)^5 + (12a + 19b)^5 + (28a + 21b)^5 + \\ + (31a + 36b)^5 + (39a + 37b)^5 - (4a + 9b)^5 - \\ - (19a + 12b)^5 - (21a + 28b)^5 - (36a + 31b)^5 - \\ - (37a + 39b)^5) \pmod{U} = \\ = w^5 * C_L(a, b) \pmod{U}; \quad (12)$$

$$C_R(a, b, v) = v^5 * C_L(a, b, w) \pmod{U}.$$

Очевидно, т.к. $(w, v) = 1 \pmod{U}$, то при обратном преобразовании закрытого текста с легальный пользователь будет исходить из

того, что

$$C_R(a,b,v) = v^5 * C_L(a,b,w) \pmod U = \\ = v^5 * w^5 * C_L(a,b) \pmod U = \\ = C_L(a,b) \pmod U = \\ = C_R(a,b) \pmod U. \quad (13)$$

Рассмотрим математическую модель криптосистемы с открытым ключом на том же примере, который был рассмотрен выше для математической модели алфавитной дисимметричной биграммной криптосистемы. Пусть имеем тот же открытый текст $m = DIOPHANT$, состоящий из четырёх биграмм: $m_1 = DI$, $m_2 = OP$, $m_3 = HA$, $m_4 = NT$. Здесь наибольшие числовые эквиваленты имеют буквы P и T, для которых они соответственно равны $q_P = 15$, $q_T = 19$, поэтому модуль U определим как

$$U = U(q_P, q_T) = (3q_P + q_T)^5 + 1 \text{ или}$$
$$U(15,19)+1 = (3*15+19)^5+1 = 1073741825.$$

Далее, определим w и v таким образом, чтобы выполнялось условие

$$(w,v) \equiv 1 \pmod{1073741825}.$$

Для значений $w = 378967703$, $v = 17$, указанное условие выполняется, т.е.

$$(378967703, 17) \equiv 1 \pmod{1073741825}.$$

Теперь перейдём к прямому преобразованию исходного сообщения $m = DIOPHANT$. Так, например, шифр с первой биграммы $m_1 = DI$ исходного сообщения m при закрытом ключе b, например, $b = 9$ определяем на основе (12) как числовое значение

$$c = C_L(89, 9, 378967703) = \\ = 3789677035^5 * C_L(a,b) \pmod{1073741825} = \\ = 3789677035^5 * 1601568101376 \\ \pmod{1073741825}.$$

Очевидно, для обратного преобразования закрытого текста нелегальный пользователь, не зная секретных ключей $b = 9$, $v = 17$, должен исходить из шифра c, полученный на основе левой части уравнения (9) с заданной гаммой y

$$C_L(a,b,w) = w^5 * C_L(a,b) \pmod{1073741825}$$

— что является трудоёмкой задачей.

Легальный пользователь для решения той же задачи предварительно на основе (13) и секретных ключей $b = 9, v = 17$ вычисляет

$$C_R(a,b,v) = C_L(a,b) \pmod{1073741825} = \\ = 1601568101376 \pmod{1073741825},$$

а затем применяет тот же алгоритм, что и для дисимметричной криптосистемы, рассмотренный выше, и определяет значение $a = 89$, соответствующее биграмме $m_1 = DI$.

Аналогично он поступает и для других биграмм открытого текста $m = DIOPHANT$.

Отметим особо, что затраты у легального и нелегального пользователей не соизмеримы: легальный пользователь, применяя секретные ключи решает линейное диофантово уравнение, а нелегальный много вариативное многостепенное диофантово уравнение пятой степени.

Заключение

Таким образом, для практических приложений следует выбрать подходящую многостепенную систему диофантовых уравнений и соответствующие соотношения с учётом степени равносильностей. В рассмотренных выше примерах криптосистем, выбран простой вариант равносильности (7) степени один (см. Теорему 1). В дальнейшем они отождествляются с числовыми или функциональными ранцами [4], причём все решения системы (4), числовые или параметрические, при некоторых ограничениях можно рассмотреть, как числовые или функциональные ранцы [4], относительно которых можно применить теорию ранцевых СЗИ.

Итак, авторами разработаны математические модели криптосистем, содержащих диофантовы трудности при решении многостепенной системы диофантовых уравнений заданной размерности и степени. Как отмечено выше, для определения числовых эквивалентов элементарных сообщений легальный пользователь решает диофантово уравнение первой степени, а нелегальный — многовариативную многостепенную систему диофантовых уравнений пятой степени.

В заключение ещё раз отметим, что в общем случае проблемы, связанные с системами диофантовых уравнений, трудно решаются и общие непереборные методы их решения

для любых диофантовых уравнений заранее заданной степени и сложности неизвестны. Поэтому, следуя К. Шеннону, эти проблемы можно взять за основу при построении аналогичных криптосистем.

Литература

1. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28. Iss. 4. P. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x
2. *Alpers A., Tijdeman R.* The two-dimensional Prouhet–Tarry–Escott problem // J. of Number Theory. 2007. Vol. 123. Iss. 2. P. 403–412. DOI: 10.1016/j.jnt.2006.07.001.
3. *Матиясевич Ю. В.* Десятая проблема Гильберта. М.: Издательская фирма «Физико-математическая литература», ВО Наука, 1993. 224 с.
4. *Осипян В. О.* Моделирование систем защиты информации содержащих диофантовы трудности. Разработка методов решений многостепенных систем диофантовых уравнений. Разработка нестандартных рюкзачных криптосистем. LAMBERT Academic Publishing. 2012. 344 с.
5. *Осипян В. О.* Математическое моделирование систем защиты данных на основе диофантовых уравнений // Прикаспийский журнал: управление и высокие технологии. 2018. № 1. С. 151–160.
6. *Осипян В. О., Григорян Э. С.* Метод параметризации диофантовых уравнений и математическое моделирование систем защиты данных на их основе // Прикаспийский журнал. 2019. № 1. С. 164–172.
7. *Осипян В. О., Спирина С. Г., Арутюнян А. С., Подколзин В. В.* Моделирование ранцевых криптосистем, содержащих диофантовую трудность // Чебышевский сборник. 2010. Т. 11. № 1. С. 209–216.
8. *Cassels J. W. S.* On a Diophantine Equation // Acta Arithmetica. 1960. Vol. 6. Iss. 1. P. 47–52. DOI: 10.4064/aa-6-1-47-52
9. *Carmichael R. D.* The Theory of Numbers and Diophantine Analysis. New York, 1959. 118 p.
10. *Chernick J.* Ideal solutions of the Tarry-Escott problem // The American Mathematical Monthly. 1937. Vol. 44. Iss. 10. P. 626–633. DOI: 10.2307/2301481
11. *Dickson L. E.* History of the Theory of Numbers. New York, 1971.
12. *Dorwart H. L., Brown O. E.* The Tarry-Escott problem // Amer. Math. Monthly. 1937. Vol. 44. Iss. 10. P. 613–626. DOI: 10.2307/2301480
13. *Gloden A.* Mehgradige Gleichungen // Groningen. 1944. pp. 104.
14. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.
15. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995. 318 с.
16. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002. 816 с.
17. *Koblitz N.* A Course in Number Theory and Cryptography. New York: Springer-Verlag, 1987. 235 p.

References

1. Shannon, C. Communication theory of secrecy systems. *Bell System Techn. J.*, 1949, vol. 28, iss. 4, pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x
2. Alpers, A., Tijdeman, R. The two-dimensional Prouhet–Tarry–Escott problem. *J. of Number Theory*, 2007, vol. 123. Iss. 2. P. 403–412. DOI: 10.1016/j.jnt.2006.07.001
3. Matiyasevich, Yu.V. *Desyataya problema Gil'berta* [Hilbert's tenth problem]. Fiziko-matematicheskaya literatura, Moscow, 1993. (In Russian)
4. Osipyan, V.O. *Modelirovanie sistem zashchity informatsii soderzhashchikh diofantovy trudnosti. Razrabotka metodov resheniy mnogostepennykh sistem diofantovykh uravneniy. Razrabotka nestandartnykh ryukzachnykh kriptosistem* [Modeling information security systems containing Diophantine difficulties. Development of methods for solving multi-degree systems of diophantine equations. Development of custom backpack cryptosystems]. LAMBERT Academic Publishing, Moscow, 2012. (In Russian)
5. Osipyan, V. O. Matematicheskoe modelirovanie sistem zashchity dannykh na osnove diofantovykh uravneniy [Mathematical modeling of data protection systems based on diophantine equations]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Pre-Caspian J.: Management and High Technologies], 2018, no. 1, pp. 151–160. (In Russian)
6. Osipyan, V. O., Grigoryan, E. S. Metod parametrizatsii diofantovykh uravneniy i matematicheskoe modelirovanie sistem zashchity dannykh na ikh osnove [The method of parameterization of diophantine equations and mathematical modeling of data protection systems based on them]. *Prikaspiyskiy zhurnal* [Pre-Caspian J.], 2019, no. 1, pp. 164–172. (In Russian)
7. Osipyan, V. O., Spirina, S. G., Arutyunyan, A. S., Podkolzin, V. V. Modelirovanie rantsevykh kriptosistem, soderzhashchikh diofantovuyu trudnost' [Modeling knapsack cryptosystems containing diophantine difficulty]. *Cheby-*

shevskiy sbornik [Chebyshevskii Sbornik], 2010, vol. 11, no. 1, pp. 209–216. (In Russian)
8. Cassels, J. W. S. On a Diophantine Equation. *Acta Arithmetica*, 1960, vol. 6, iss. 1, pp. 47–52. DOI: 10.4064/aa-6-1-47-52
9. Carmichael, R. D. *The Theory of Numbers and Diophantine Analysis*. New York, 1959.
10. Chernick, J. Ideal solutions of the Tarry-Escott problem. *Amer. Math. Monthly*, 1937, vol. 44, iss. 10, pp. 626–633. DOI: 10.2307/2301481
11. Dickson, L. E. *History of the Theory of Numbers*. New York, 1971.
12. Dorwart H. L., Brown O. E. The Tarry-Escott problem. *Amer. Math. Monthly*, 1937, vol. 44, iss. 10, pp. 613–626. DOI: 10.2307/2301480
13. Gloden, A. Mehgradige Gleichungen. *Groningen*, 1944, pp. 104.
14. Alferov, A. P., Zubov, A. Yu., Kuz'min, A. S., Cheremushkin, A. V. *Osnovy kriptografii* [Cryptography Basics]. Gelios ARV, Moscow, 2002. (In Russian)
15. Salomaa, A. *Kriptografiya s otkrytym klyuchom* [Public key cryptography]. Mir, Moscow, 1995. (In Russian)
16. Shnayer, B. *Prikladnaya kriptografiya: Protokoly, algoritmy, iskhodnye teksty na yazyke Si* [Applied Cryptography: Protocols, Algorithms, C Source Texts]. Triumf, Moscow, 2002. (In Russian)
17. Koblitz, N. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1987.

Статья поступила 22 августа 2019 г.