Инженерный вестник Дона, № 6 (2020)
ivdon.ru/ru/magazine/archive/n6y2020/6534

Разработка математической модели дисимметричной биграммной криптосистемы на основе параметрического решения многостепенной системы диофантовых уравнений[1]

В. О. Осипян

Кубанский государственный университет, г. Краснодар, Россия

Аннотация: Показана объективная необходимость совершенствования систем защиты информации в условиях развития информационно-телекоммуникационных технологий. Приведены теоремы, которые описывают свойства параметрических решений многостепенных систем диофантовых уравнений (МСДУ), необходимых для разработки математических моделей систем защиты информации (СЗИ) на их основе. Обобщается теорема Фролова, и приводится авторская теорема, которая позволяет разрабатывать математическую модель СЗИ, содержащих диофантовы трудности. Приводится авторская математическая модель алфавитной криптосистемы в виде кортежа.

Предложен новый подход разработки дисемметричной биграммной криптосистемы (ДБК) на основе двупараметрических решений, обобщающий принцип построения криптосистем с открытым ключом. Предлагается прямое и обратное преобразования реализовать с помощью параметрического решения, предварительно разбив его на две части: одна часть для прямого преобразования, а другая – для обратного. Вводится новое понятие равносильности упорядоченных наборов чисел или параметров с заданной размерности и порядка.

Приводится математическая модель ДБК, построенная на основе двупараметрических решений МСДУ с заданной размерностью и порядком. Описанная математическая модель демонстрирует потенциал применения диофантовых уравнений для разработки СЗИ с высокой степенью надёжности.

Ключевые слова: система защиты информации, симметричная криптосистема, дисимметричная криптосистема, криптосистема с открытым ключом, шифрование информации, дешифрование информации, многостепенная система диофантовых уравнений, параметрическое решение, диофантовы трудности.

1. Введение

На основе теоретических истоков построения математических моделей эффективных криптосистем необходимо использовать сложные математические задачи, решение которых потребует от нелегального пользователя большого объема вычислительной работы и ресурсов. К таким задачам, следуя К. Шеннону [1, 2], относятся задачи, содержащие «диофантовы трудности», использование которых препятствует возможности сократить множество перебираемых ключей.

[1] Работа поддержана грантом РФФИ № 19-01-00596

Предварительно приведём некоторые факты [3–10], используемые нами при построении математической модели систем защиты информации (СЗИ), содержащие диофантовы трудности.

Как известно [3, 11, 12], под алгебраическим диофантовым уравнением 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), как правило, заключается в поиске целочисленных решений заданного уравнения или доказательства того, что таких решений нет [11, 13].

Особый интерес в данной работе будут представлять многостепенные системы диофантовых уравнений (МСДУ) размерности m порядка (или степени) n вида [14,12,15,16, 13,17,18]:

$$X_1^k + X_2^k + \cdots + X_m^k = Y_1^k + Y_2^k + \cdots Y_m^k, \qquad k = 1..n \qquad (2)$$

или в компактной записи:

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

Для краткости эту запись мы представим ещё в виде:

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

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

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

где $A = a_1, a_2, \ldots, a_m$, $B = b_1, b_2, \ldots, b_m$, a_i, b_i – целые числовые параметры.

Многостепенная система (2) называется почти идеальной [4, 16], если $m = n + 2$, и идеальной или нормальной при $m = n + 1$.

Так как при $n \geq m$ система (2) имеет лишь тривиальные решения (см. теорему Bastien) [15]: 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. $\{a_1, a_2, \ldots, a_m\} = \{b_1, b_2, \ldots, b_m\}$, поэтому будем исследовать параметрическое решение (2), для которых $n < m$.

В общем случае, проблемы, связанные с МСДУ (2), трудно решаются [3, 14,12,15,16, 13]: не известны общие не переборные методы их решения для любых m и n (см. Десятую проблему Гильберта о разрешимости диофантова уравнения [3]). В 1900 году была сформулирована Десятая проблема Гильберта, состоящая в нахождении алгоритма решения произвольного алгебраического диофантова уравнения. В 1970 году Ю.В. Матиясевич доказал алгоритмическую неразрешимость этой проблемы [3]. Из этого следует, что гарантированно отсутствует общий алгоритм решения любого диофантова уравнения.

Сегодня использование диофантовых уравнений для разработки эффективных систем защиты информации становится все интенсивнее [4–10]. Цель данной работы продемонстрировать возможность использования МСДУ для разработки достаточно устойчивых ко взлому систем защиты информации.

Рассмотрим возможность применения семейства МСДУ для математического моделирования алфавитных СЗИ, если установлены условия, при которых МСДУ допускают параметризацию по одному, двум и более параметрам $t_1, t_2, \ldots, t_r$ в виде:

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

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:

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

Для удобства введём также следующие обозначения и определения.

Если

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

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

1. $A_k^i = a_k, a_{k+1}, \ldots, a_i$ в частности, при $k = 1$, $A_k^i = A^i$ для $i \in 1..m$;

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. $A \pm a = a_1 \pm a, a_2 \pm a, \ldots, a_m \pm a$; (3)

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 $A^m = a_1, a_2, \ldots, a_m$ и $B^m = b_1, b_2, \ldots, b_m$ размерности m равносильны со степенью n: $A^m \overset{n}{=} B^m$, если они удовлетворяют МСДУ размерности m порядка n (2):

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

то есть выполняются следующие равенства для всех значений $1..n$:

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

Другими словами, из равносильности $A^m \overset{n}{=} B^m$ следует, что набор A^m, B^m является корнем уравнения порядка n:

$$X^m \overset{n}{=} Y^m$$

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

1. $A^m \overset{n}{=} A^m$ (рефлексивность);
2. Если $A^m \overset{n}{=} B^m$, то $B^m \overset{n}{=} A^m$ (симметричность);
3. Если $A^m \overset{n}{=} B^m$, $B^m \overset{n}{=} C^m$, то $A^m \overset{n}{=} C^m$ (транзитивность).

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

$$19a + b, 15a + 5b, 11a + 9b, 3a + 17b, 2a + 18b \doteq a + 19b, 5a + 15b, 9a + 11b,$$
$$17a + 3b, 18a + 2b.$$

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

Теперь рассмотрим некоторые примеры МСДУ (2) для различных параметров m и n.

Так, для $m = 4$, $n = 3$ имеем следующую идеальную или нормальную МСДУ третьей степени с четырьмя переменными:

$$X^4 \overset{3}{=} Y^4$$

и одно из её взаимно-простых решений:

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

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

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

причём НОД указанного решения – $d = (1, 8, 10, 17, 2, 5, 13, 16) = 1$.

Далее для $m = 4, n = 3$ можно получить следующую цепочку числовых решений:

$3, 50, 82, 129 \overset{3}{=} 10, 33, 99, 122 \overset{3}{=} 14, 27, 105, 118 \overset{3}{=} 6, 41\ 91, 126 \overset{3}{=} 1, 66, 66, 131.$

При $m = 6, n = 5$ можно рассмотреть следующую нормальную МСДУ пятой степени:

$$X^6 \overset{5}{=} Y^6,$$

и его частные решения:

$$1, 6, 7, 17, 18, 23 \overset{5}{=} 2, 3, 11, 13, 21, 22;\ 28, 175, 203, -28, -175, -203 \overset{5}{=}$$

$$\overset{5}{=} 77, 140, 217, -77, -140, -217 \overset{5}{=} 55, 157, 212, -55, -157, -212.$$

На основе этого решения можно получить следующую систему тождеств:

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

$$(28a + 77b)^n + (175a + 140b)^n + (203a + 217b)^n + (-28a - 77b)^n$$
$$+ (-175a - 140b)^n + (-203a - 217b)^n$$
$$= (77a + 28b)^n + (140a + 175b)^n + (217a + 203b)^n + (-77a - 28b)^n$$
$$+ (-140a - 175b)^n + (-217a - 203b)^n$$

т.к. [4] если $A^m \overset{n}{=} B^m$, то $aA^m + bB^m \overset{n}{=} bA^m + aB^m$ для $n = 1..5$.

Можно рассмотреть также уравнения вида:

$$X^{m_1} \overset{x}{=} Y^{m_2},$$

где x, m_1, m_2 принимают произвольные допустимые натуральные значения.

Так, например, для уравнения

$$X^2 \overset{x}{=} Y^3, x = 1,2,4$$

имеем следующее частное решение:

$$7, -7 \overset{x}{=} 3, 5, -8, \qquad x = 1, 2, 4.$$

Приведём также некоторые частные решения следующего уравнения

$$X^8 \overset{x}{=} Y^8, x = 1,2,4:$$

$$2,3,9,10,11,11,12,16 \overset{x}{=} 4,5,7,7,8,14,14,15, \qquad x = 1,3,9;$$

$$4,5,9,9,9,13,13,17 \overset{x}{=} 6,6,6,8,10,11,16,16, \qquad x = 1,3,9.$$

Можно рассмотреть и другие частные примеры, но мы перейдём к МСДУ более общего вида.

Ниже мы приведём утверждения относительно МСДУ для заданных допустимых значений m и n, позволяющие устанавливать равносильность заданных числовых наборов или наборов упорядоченных параметров.

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

$$A^m \overset{n}{=} B^m$$

следует равносильность также следующих наборов (или наборов упорядоченных параметров)

$$A^m, -B^{m-1} \overset{n}{=} b^m \tag{4}$$

или в более общем случае для любого натурального $i \in 1..m$**:**

$$A^m, -B^{i-1} \overset{n}{=} b^{m_i} \tag{5}$$

Теорема 2. (Фролов, [18]). Если $A^m \overset{n}{=} B^m$, то $aA^m + b \overset{n}{=} aB^m + b$, где $a \neq 0, b$ – целые числа. В частности, если $a = 1, b = h$, то $A^m + h \overset{n}{=} B^m + h$.

Следующая теорема является обобщением указанной теоремы Фролова.

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

Приведём также утверждение теоремы Тарри [18], которое позволяет получить решение нормальной МСДУ $(n+1)$-ой степени, исходя из соответствующего решения n-ой степени.

Теорема 4. (Тарри, [15]). Если $A^m \overset{n}{=} B^m$, то. $A^m, B^m + h \overset{n+1}{=} B^m, A^m + h$.

Следующая теорема позволяет увеличить порядок МСДУ при заданной размерности.

Теорема 5. (Глоден [18]). Пусть

$$a_1, a_2, \dots, a_{n+1} \overset{n}{=} b_1, b_2, \dots, b_{n+1}$$

– нормальная система n -го порядка,

$$S_1 = a_1 + a_2 + \cdots + a_{n+1} = b_1 + b_2 + \cdots + b_{n+1}, \qquad t = -\frac{S_1}{n+1}$$

тогда

$$a_1 + t, a_2 + t, \dots, a_{n+1} + t \overset{x}{=} b_1 + t, b_2 + t, \dots, b_{n+1} + t, x = 1,2, \dots n + 2.$$

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

Теорема 6 (Основная**).** Пусть имеются две пары равносильных упорядоченных наборов параметров (функциональных ранцев) размерности m степени n, причём первая пара A^m и B^m представляет собой произвольное параметрическое решение МСДУ n -ой степени размерности m

$$X^m \overset{n}{=} Y^m$$

а вторая – C^m и D^m любое расширение первой, полученной на основании **Теорем 1 – 5**:

1. $A^m \overset{n}{=} B^m, 1 \leq n < m;$
2. $C^m \overset{n+t}{=} D^m, \ t \geq 1, 1 \leq n + t < k;$

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

Приведённые Теоремы 2–5 нам будут необходимы для увеличения размерности m, а также степени n равносильных наборов (числовых или параметрических) при разработке математических моделей СЗИ на основе равносильностей (4) и (5) (см. Теорему 1) совместно с соотношениями (3). Более того, их можно отождествлять с числовыми и функциональными

ранцами [4,19-25], причём все решения указанных систем, числовые или параметрические, при некоторых ограничениях можно рассмотреть, как числовые или функциональные ранцы, относительно которых можно применить теорию ранцевых СЗИ.

Кроме того, 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. количества параметров соответствующей системы диофантовых уравнений.

2. Метод двухпараметрического решения систем диофантовых уравнений с помощью целочисленных и целозначных функций

Рассмотрим метод параметризации МСДУ заданной размерности **m** порядка **n:**

$$X^m \overset{n}{=} Y^m, \qquad n < m$$

с помощью введения целочисленных и целозначных функций. Заметим, что данный метод не зависит от конкретных числовых значений **m** и **n**, поэтому для простоты изложения, применим указанный метод для параметризации следующей МСДУ:

$$X^6 \overset{n}{=} Y^6$$

при $m = 6, n = 1, 2, 4, 6.$

Теорема 7. Семейство двупараметрических решений МСДУ

$$X^6 \overset{n}{=} Y^6, n = 1, 2, 4, 6$$

можно найти как:

$$X_1 = 5a + b, X_2 = a - 5b, X_3 = 7a + 5b,$$
$$X_4 = 5a - 7b, X_5 = 2a - 8b, X_6 = 8a - 2b,$$
$$Y_1 = 5a - b, Y_2 = a + 5b, Y_3 = 7a - 5b,$$

$$Y_4 = 5a + 7b, Y_5 = 2a - 8b, Y_6 = 8a + 2b,$$

где a, b – произвольные целые числа.

Доказательство. Введём в рассмотрение следующие две целочисленные и целозначные функции от двух параметров a и b:

$$f_n(a,b) = (5a+b)^n + (a-5b)^n + (7a+5b)^n + (5a-7b)^n + (2a+8b)^n + (8a-2b)^n$$

и

$$g_n(a,b) = (5a-b)^n + (a+5b)^n + (7a-5b)^n + (5a+7b)^n + (2a-8b)^n + (8a+2b)^n,$$

где a, b – произвольные целые числа. Функции $f_n(a,b)$ и $g_n(a,b)$ подобраны таким образом, чтобы выполнялось условие:

$$f_n(a,-b) = g_n(a,b) \text{ или } f_n(a,b) = g_n(a,-b)$$

Определим те значения n, при которых для всех целых значений a и b выполняется равенство:

$$f_n(a,b) = g_n(a,b).$$

Имеем:

$$f_1(a,b) = g_1(a,b) = 28a.$$

$$f_2(a,b) = g_2(a,b) = 168(a^2 + b^2).$$

$$f_3(a,b) = 1114a^3 - 18a^2b + 18ab^2 + 162b^3$$

$$f_4(a,b) = g_4(a,b) = 12(647a^4 + 1506a^2b^2 + 647b^4);$$

$$f_6(a,b) = g_6(a,b) = 411108a^6 + 118708a^4b^2 + 118708a^2b^4 + 411108b^6,$$

т.е.

$$f_n(a,b) = g_n(a,b) \text{ при } n = 1, 2, 4, 6,$$

и таким образом, имеют место следующие тождества:

$$f_n(a,b) = (5a+b)^n + (a-5b)^n + (7a+5b)^n + (5a-7b)^n + (2a+8b)^n$$

$$+(8a-2b)^n \equiv (5a-b)^n + (a+5b)^n + (7a-5b)^n + (5a+7b)^n$$
$$+ (2a-8b)^n + (8a+b)^n = g_n(a,b)$$

при $n = 0,1,2,4,6$, где a и b – произвольные целые числа.

Очевидно, можно подобрать a и b таким образом, чтобы все члены полученного тождества были положительные.

Аналогичным образом можно получить семейство двухпараметрических и трёхпараметрических решений заданной МСДУ.

Так, например, семейство трёхпараметрических решений МСДУ размерности $m = 4$ можно найти на основании следующей теоремы.

Теорема 8. Пусть целые числа a, b и c удовлетворяют диофантому уравнению

$$a^2 + ab + b^2 = 7c^2.$$

Тогда семейство трёхпараметрических решений МСДУ размерности $m = 4$:

$$X^4 \overset{n}{=} Y^4, \qquad n = 2,4,6$$

можно найти как:

$$X_1 = a-7c, \quad X_2 = 3a+c, \quad X_3 = a-2b+c, \quad X_4 = 3a+2b+c;$$
$$Y_1 = a+7c, \quad Y_2 = 3a-c, \quad Y_3 = a-2b-c, \quad Y_4 = 3a+2b-c,$$

где a, b, c – произвольные целые числа.

Указанный выше метод имеет широкое применение при моделировании эффективных криптосистем.

3. Моделирование дисимметричной биграммной криптосистемы на основе двухпараметрического решения заданной многостепенной системы диофантовых уравнений

Предварительно представим математическую модель алфавитной криптосистемы, разработанной автором, в виде следующего кортежа:

$$\sum\nolimits_0 = \langle M^*, Q, C^*, E(m), D(c) | V(E(m), D(c)) \rangle, \quad (6)$$

где M^* множество всех сообщений $m = m_1 m_2 .. m_k$ (открытых текстов) над буквенным или числовым алфавитом M. Здесь $m_i, i = 1..k$ – 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) $c = c_1 c_2 .. c_k$ 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 (6) связаны между собой таким образом – $V(E(m), D(c))$, что всегда произвольное сообщение $m = m_1 m_2 .. m_k \in M^*$ однозначно преобразовывается в соответствующую криптограмму (шифртекст) $c = c_1 c_2 .. c_k \in C^*$ и, обратно: по криптограмме c всегда однозначно восстанавливается переданное сообщение m.

Альтернативным обозначением алгоритмов $E(m)$ и $D(c)$ для алфавитной криптосистемы (6) является K_E (или F_E) и K_D (или F_D) соответственно – как принято считать в классической криптографии [1, 2, 19, 20, 22]. Мы их иначе назовём ключами (или функциями) шифрования и дешифрования соответственно, причём автор не претендует на полноту освещения аналогичных математических моделей алфавитных криптосистем (6), единственная его цель – формально описать произвольную криптосистему.

Теперь перейдём к разработке математической модели дисимметричной биграммной криптосистемы (ДБК), исходя из вышеизложенного (некоторые несущественные детали мы опускаем, т.к. они широко освещены в литературе). Алгоритмы $E(m)$ и $D(c)$ математической

модели алфавитной ДБК определим на основе модифицированного соотношения (5) (см. Теорему 1).

Проиллюстрируем предложенный автором подход для построения математической модели алфавитной ДБК на основе двупараметрического решения заданной МСДУ (для наглядности и понимания мы упрощаем многие процедуры). Прежде всего, на основании Теорем 2–5 необходимо определить размерность l и порядок k МСДУ:

$$X_1, X_2, \dots, X_l \overset{k}{=} Y_1, Y_2, \dots, Y_l \text{ или } X^i \overset{k}{=} Y^i \qquad (7)$$

а затем и её двупараметричское решение:

$$X_i = v_i(a,b) = v_i, \qquad i = 1..l,$$
$$Y_i = v_j(a,b) = v_j, \qquad j = (l+1)..2l$$

Для простоты и удобства её двупараметрическое решение представим в виде следующего упорядоченного набора:

$$V^{2l} = v_1, v_2, \dots, v_{2l}$$

для которого выполняются следующие равенства для всех значений $1..k$:

$$v_1, v_2, \dots, v_l \overset{k}{=} v_{l+1}, v_{l+2}, \dots, v_{2l}.$$

В соответствии с условием (5) при фиксированной степени $d, 1 \le d \le k$ сгенерируем функцию прямого преобразования по заданному алгоритму как:

$$E(m_i) = C_L(a,b) = v_1^d + v_2^d + \dots + v_r^d, \qquad r < 2l$$

считая, что a шифр элементарного сообщения биграммы $m_i m_{i+1}, b$ – некоторый закрытый ключ. Соответственно функцию обратного преобразования определим как

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

Заметим, что количество слагаемых для функции шифрования $C_R(a,b)$ можно довести до минимума, например, до одного слагаемого, как это представлено в (4). Для наглядности и простоты изложения рассмотрим следующий учебный пример.

Пусть задана степень d МСДУ и открытый текст сообщения:

$$m = DIOPHANTINE\ DIFFICULTY\ AND\ SMG$$

над алфавитом M заглавных букв английского 27-буквенного алфавита от A до Z и пробела с множеством Q всех числовых эквивалентов q биграмм элементарных сообщений m_i из M^* с числовыми эквивалентами от 0 до 26. Заметим, что шифрование исходного текста m выполняется функцией $C_L(a,b)$, а дешифрование – другой функцией$C_R(a,b)$.

Числовой эквивалент q биграммы (предварительно исходное сообщение m разбиваем на биграммы $m_i m_{i+1}$с добавлением пробела, если m содержит нечётное число элементарных сообщений: у нас всего 15 биграмм), 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 MG соответствует числовой эквивалент $q = 27 * 13 + 7 = 358$, а результат прямого преобразования в явном виде можно представить как:

$$C_L(358, b) = v_1(358, b)^d + v_2(358, b)^d + \cdots + v_r(358, b)^d.$$

Рассмотрим оптимальный вариант прямого преобразования $E(MG)$ для легального пользователя при $r = 2l - 1$.

Имеем:

$$E(MG) = C_L(358, b) = v_1(358, b)^d + v_2(358, b)^d + \cdots + v_{2l-1}(358, b)^d \quad (8)$$

Перед нелегальном пользователем предстоит трудно вычислимая задача – найти параметрическое решение МСДУ, для которой имеет место равенство (8).

Задача определения легальным пользователем того же значения a сводится к решению следующего уравнения:

$$D(c_i) = C_R(358, b) = v_{2l}(358, b)^d = c \quad (9)$$

Заметим, что прямое преобразование исходного текста m выполняется функцией $C_L(a,b)$, а обратное преобразование – другой функцией $C_R(a,b)$.

Очевидно, затраты у легального и нелегального пользователей не соизмеримы: легальный пользователь решает простое уравнение (9), а нелегальный – многовариативное МСДУ размерности l порядка k. Отметим также, что фактически функция прямого преобразования $C_L(a,b)$ биграммы a с закрытым ключом b представляет часть двупараметрического решения уравнения (7) и содержит диофантовы трудности.

4. Заключение

Таким образом, для практических приложений следует выбрать подходящую МСДУ и соответствующие модифицированные соотношения (4), (5) на основе Теоремы 1 с учётом степеней равносильностей. В рассмотренном выше примере ДБК мы выбрали простой вариант функции прямого преобразования, в самом же деле можно предложить сложный алгоритм для выбора указанной функции с соответствующими равносильностями. В дальнейшем их можно отождествлять с числовыми и функциональными ранцами [4], причём все решения системы (7), числовые или параметрические, при некоторых ограничениях можно рассмотреть, как числовые или функциональные ранцы, относительно которых следует применить теорию ранцевых СЗИ.

Итак, нами разработан математическая модель ДБК, содержащих диофантовы трудности при решении МСДУ заданной размерности и порядка. Как отмечено выше, для определения числовых эквивалентов элементарных сообщений легальный пользователь решает простое уравнение заданной степени, а нелегальный – многовариативную МСДУ заданной размерности и порядка.

Предложен новый подход разработки ДБК на основе параметрического решения МСДУ, обобщающий принцип построения криптосистем с открытым ключом: для прямого и обратного преобразований обрабатываемой информации параметрическое решение МСДУ предварительно разбивается на две части – одна часть применяется по заданному алгоритму при прямом преобразовании открытого текста, а другая часть – при обратном преобразовании закрытого текста с помощью блоков заданной длины, например, биграмм.

В заключение отметим, что в общем случае проблемы, связанные с системами диофантовых уравнений, трудно решаются [3], и не известны общие не переборные методы их решения для любых диофантовых уравнений заранее заданной степени и сложности. Поэтому, следуя К. Шеннону, эти проблемы можно взять за основу при разработке аналогичных ДБК.

Литература

1. Алферов А. П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии . – 2-е изд., испр. и доп. – Москва: Гелиос АРВ, 2002. – 480 с.

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

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 (41). – 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: управление и высокие технологии. – 2019. – № 1 (45), с. 164-172.

7. Osipyan V. O., Litvinov K. I., Bagdasaryan R. Kh., Lukashchik E. P., Sinitsa S. G., Zhuk A. S. Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems / SIN '19 Proceedings of the 12th International Conference on Security of Information and Networks/ ACM Press, 2019, pp.1-8.

8. 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 т.3, №16 / Кубанский государственный университет (Краснодар), 2019, с.6-15.

9. Осипян В.О., Синица С.Г., Имитационное моделирование алгоритмов криптосистем. Симметричное шифрования на основе диофантова уравнения первой степени // Математические методы и информационно-технические средства: материалы XV Всерос. науч.-практ.конф., 21 июня 2019 г. / Краснодар: Краснодарский университет МВД России, 2019, с.140-145.

10. Осипян В. О., Спирина С.Г., Арутюнян А.С., Подколзи В.В. Моделирование ранцевых криптосистем, содержащих диофантовую трудность // Чебышевский сборник. – 2010.Т. 11, вып. 1. – С. 209–217.

11. Серпинский В. О решении уравнений в целых числах / пер. с польск. К. Г. Мельникова. – Москва: Физматлит, 1961. – 88 с.

12. Cassels J. W. S. On a Diophantine Equation // Acta Arithmetica. – 1960. – Vol. 6. – pp. 47–52.

13. Dickson L. E. History of the Theory of Numbers. – New York, 1971. – Vol. 2. Diophantine Analysis.

14. Alpers A., Tijdeman R. The two-dimensional Prouhet–Tarry–Escott problem // Journal of Number Theory, 123(2), pp. 403-412.

15. Carmichael R. D. The Theory of Numbers and Diophantine Analysis. – New York, 1959. – 118 p.

16. Chernick J. Ideal solutions of the Tarry-Escott problem //Amer. Monthly, 1937, 5, 44n.10, 626-633.

17. Dorwart, H.L. and Brown O. E. The Tarry-Escott problem, Amer. Math. Monthly 44 (1937), pp. 613–626.

18. Gloden A. Mehgradige Gleichungen. – Groningen, 1944. – P. 104.

19. Саломаа А. Криптография с открытым ключом. – Москва: Мир, 1995. – 318 с.

20. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си: пер. с англ. – Москва: Триумф, 2002. – 816 с.

21. Chor B., Rivest R. A knapsack-type public key cryptoystem based on arithmetic in finite fields // IEEE Transactions on Information Theory. – 1988. – Vol. IT-34. – pp. 901–909.

22. Koblitz N. A Course in Number Theory and Cryptography. – New York: Springer-Verlag, 1987. – 235 p.

23. Lenstra A. K., Lenstra H. W., Lovasz L. Factoring polynomials with rational coefficients // Mathematische annalen. – 1982. – Vol. 261. – pp. 515–534.

24. Lin C. H., Chang C. C., Lee R. C. T. A new public-key cipher system based upon the Diophantine equations // IEEE Transactions on Computers. – 1995, Jan. – Vol. 44, issue 1.

25. Merkle R., Hellman M. Hiding information and signatures in trapdoor knapsacks // IEEE Transactions on Information Theory. – 1978. – Vol. IT-24. – pp. 525–530.

References

1. Alferov A. P., Zubov A. Yu., Kuzmin A. S., Cheremushkin A. V. Osnovy kriptografii [Bases of cryptography]. 2nd ed. Moskva, Gelios ARV Publ., 2002. 480 p.

2. Shannon C. Bell System Techn. J., 1949, vol. 28, no. 4, pp. 656–715.

3. Matiyasevich, Yu. B. Matiyasevich Yu. B. Desyataya problema Gil'berta. [Hilbert's tenth problem]. Izdatel'skaya firma “Fiziko-matematicheskaya literature”. VO Nauka. 1993. 224p.

4. Osipyan V. O. Modelirovaniye sistem zashchity informatsii soderzhashchikh diofantovy trudnosti. Razrabotka metodov resheniy mnogostepennykh sistem diofantovykh uravneniy. Razrabotka nestandartnykh ryukzachnykh kriptosistem: monografiya [Modeling of systems of protection of information containing the Diophantine difficulties. Development of methods for solving multi-stage systems of Diophantine equations. Development of non-standard knapsack cryptosystems]. Lambert Academic Publishing, 2012, 344 p.

5. Osipyan V. O. Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii, 2018, no. 1 (41), pp. 151–160.

6. Osipyan VO, Grigoryan E.S. Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii. 2019. № 1 (45), pp. 164-172.

7. Osipyan V. O., Litvinov K. I., Bagdasaryan R. Kh., Lukashchik E. P., Sinitsa S. G., Zhuk A. S. SIN '19 Proceedings of the 12th International Conference on Security of Information and Networks. ACM Press, 2019, pp.1-8.

8. Osipyan V. O., Litvinov K. I., Zhuk A. S. Ekologicheskij vestnik nauchnyh centrov chernomorskogo ekonomicheskogo sotrudnichestva t.3, №16. Kubanskij gosudarstvennyj universitet (Krasnodar), 2019, pp.6-15.

9. Osipyan V. O., Sinitsa S. G., Matematicheskie metody i informacionno-tekhnicheskie sredstva: materialy XV Vseros. nauch.-prakt.konf., 21 iyunya 2019 g. Krasnodar: Krasnodarskij universitet MVD Rossii, 2019, pp.140-145.

10. Osipyan V. O., Spirina S. G., Arutyunyan A. S., Podkolzin V. V. Chebyshevskiy sbornik, 2010, vol. 11, № 1, pp. 209–216.

11. Serpinsky W. O reshenii uravneniy v tselykh chislakh [On solving equations in integers]. Moskva, Fizmatlit Publ., 1961, 88 p.

12. Cassels J. W. S. Acta Arithmetica. 1960. Vol. 6. pp. 47–52.

13. Dickson L. E. History of the Theory of Numbers. New York, 1971, vol. 2: Diophantine Analysis.

14. Alpers A., Tijdeman R. Journal of Number Theory, 123(2), pp. 403-412.

15. Carmichael R. D. Theory of numbers and Diophantine Analysis. New York, 1959. 118 p.

16. Chernick J. Amer. Monthly, 1937, 5, 44n.10, pp.626-633.

17. Dorwart, H.L. and Brown O. E. Amer. Math. Monthly 44 (1937), pp.613–626.

18. Gloden A. Mehgradige Gleichungen. Groningen, 1944. P. 104.

19. Salomaa A. Kriptografiya s otkrytym klyuchom [Cryptography with a public key]. Moskva, Mir Publ., 1995, 318 p.

20. Schneier B. Prikladnaya kriptografiya: Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Applied cryptography: Protocols, algorithms, source texts in C]. Moskva, Triumph Publ., 2002, 816 p.

21. Chor B., Rivest R. IEEE Transactions on Information Theory. 1988. Vol. IT-34. pp. 901–909.

22. Koblitz N. A Course in Number Theory and Cryptography. New York: Springer-Verlag, 1987. 235 p.

23. Lenstra A. K., Lenstra H. W., Lovasz L. Mathematische annalen. 1982. Vol. 261. pp. 515–534.

24. Lin C. H., Chang C. C., Lee R. C. T. IEEE Transactions on Computers. 1995, Jan. Vol. 44, issue 1.

25. Merkle R., Hellman M. IEEE Transactions on Information Theory. 1978. Vol. IT-24. pp. 525–530.