УДК 519.72

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ НЕСТАНДАРТНЫХ МУЛЬТИПЛИКАТИВНЫХ РАНЦЕВЫХ КРИПТОСИСТЕМ

Осипян В. О., Лейман А. В., Чесебиев А. А., Жук А. С., Арутюнян А. Х., Карпенко Ю. А.

MATHEMATICAL MODELING OF NON-STANDARD MULTIPLICATIVE KNAPSACK CRYPTOSYSTEMS

Osipyan V. O.[*], Leyman A. V.[*], Chesebiev A. A.[*], Zhuk A. S.[*], Harutyunyan A. H.[*], Karpenko Y. A.[**]

[*] Kuban State University, Krasnodar, 350040, Russia
[**] Adyghe State University, Krasnodar, 385016, Russia
e-mail: rrwo@mail.ru

Abstract. It investigates the development of mathematical models of alphabet cryptosystems based on the tasks a non-standard multiplicative knapsacks. Mathematical models of the cryptosystems in the form of tuples. Establishes necessary and sufficient conditions under which the generalized multiplicative injective knapsack vector over Z_p, $p \geqslant 2$. Developed mathematical model of the cryptosystem by overlapping scales, in which the algorithm of the inverse transformation of the closed text is reduced to an algorithmically non-solvable problem for the analyst. On the basis of the analysis previously offered a different backpack models are revealed qualitative features of non-standard multiplicative knapsack systems that increase their resistance to known attacks.

We also study the problem of constructing isomorphic additive and multiplication knapsacks. Moreover, in contrast to the standard knapsack-teams, in which when determining the entrance of a knapsack or other components of the knapsack vector are either present or not, and here we consider the case when they can be repeated a specified number of times for a given array for both generic and super generic multiplicative knapsack.

Keywords: alphabetic cryptosystem, mathematical model of cryptosystems, symmetric and asymmetric knapsack system of information protection, non-additive (multiplicative) knapsack, generalized (generalized super) multiplicative knapsack.

Введение

Исходя из теоретических истоков построения стойких и эффективных систем защиты информации [1], следует отметить, что многие математические задачи можно рассмотреть как системы сокрытия и защиты информации с заданными условиями, а сами решения этих задач — правильные ключи. Что же касается вопроса решений, то они соответствуют испытанию или проверке правильного ключа. Следовательно, выбор подходящей задачи позволит строить систему защиты информации на должном уровне, особенно если этот выбор, как отметил ещё К. Шеннон [1], принадлежит классу NP-полных задач.

Как известно [2–11], в основе всех стандартных и нестандартных рюкзачных системах защиты информации (РСЗИ) лежит NP-полная задача об аддитивной или мультипликативной укладке рюкзака (или ранца).

Для построения лёгкого подкласса стандартных рюкзачных систем защиты информации на основе сверхрастущего рюкзака

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

Лейман Антонина Васильевна, преподаватель кафедры информационных технологий Кубанского государственного университета; e-mail: antonina.leyman@gmail.com

Чесебиев Аскер Адамович, соискатель кафедры информационных технологий Кубанского государственного университета; e-mail: kit@fpm.kubsu.ru

Жук Арсений Сергеевич, соискатель кафедры информационных технологий Кубанского государственного университета; e-mail: arseniyzhuck@mail.ru

Арутюнян Ашот Хоренович, преподаватель кафедры прикладной математики Кубанского государственного университета; e-mail: ashotikmail.ru@mail.ru

Карпенко Юрий Александрович, старший преподаватель кафедры алгебры и геометрии Адыгейского государственного университета; e-mail: nart27@gmail.com

Р. Меркль и М. Хеллман [2] предложили «замаскировать» рюкзак с помощью линейного преобразования последнего посредством сильного модульного умножения.

В протоколе Шора–Ривеста [3], в отличие от протокола Меркля–Хеллмана, рюкзак представляет собой набор логарифмов в мультипликативной группе расширенного поля и обладает повышенной плотностью по сравнению с рюкзаком Меркля–Хеллмана.

Хотя после вскрытия с помощью алгоритма полиномиальной сложности [4, 12] оригинальной схемы Меркля–Хеллмана многие эксперты стали скептически относиться к криптостойкости таких систем, одновременно было предложено множество других усложнённых вариантов рюкзачных систем защиты информации [5–11, 13], в частности, рюкзаки Грэм-Шамира, основанные на принципе укладки стандартного рюкзака, среди которых в настоящее время существуют всё ещё не вскрытые рюкзачные системы защиты информации [5].

В отличие от существующих РСЗИ [2–5, 12, 13], основанных на стандартных рюкзаках A_S, в данной работе, во-первых, обобщается классическая задача о рюкзаке K_S и соответствующие ей системы защиты информации, для которых можно применить p-ичный случай зашифрования и расшифрования — взамен двоичного случая, во-вторых, при определении стандартного входа (A_S, V) рассматривается случай, когда компоненты рюкзачного вектора могут повторяться в соответствии с заданными спектрами как для аддитивного, так и для мультипликативного ранца.

Предварительно рассмотрим математическую модель алфавитных криптосистем, в которых в качестве алфавита чаще всего будет выступать либо алфавит некоторого естественного языка (например, английского), либо некоторый числовой алфавит (например, двоичный алфавит) или, например, поле Галуа $GF(p)$, состоящее из p элементов и т.п.

Символически математическую модель алфавитной криптосистемы авторы предлагают представить в виде следующего кортежа:

$$\sum\nolimits_0 = \big\langle M*, S*, E(m), D(s) \mid V(E(m), D(s)) \big\rangle, \quad (1)$$

где M^* — множество всех сообщений $m = m_1, m_2, \ldots, m_k$ (открытых текстов) над буквенным или числовым алфавитом M. Здесь m_i, $i = 1, \ldots, k$ — элементарные сообщения (буквы или конкатенация букв из алфавита M); S^* — множество всех шифртекстов (криптограмм) $s = s_1, s_2, \ldots, s_k$ криптосистемы (1); $E(m)$ — алгоритм прямого преобразования (шифрования) сообщения m в s; $D(s)$ — алгоритм обратного преобразования (дешифрования) шифртекста (криптограммы) s в $m \in M^*$. Следует подчеркнуть, что алгоритмы $E(m)$ и $D(s)$ алфавитной криптосистемы (1) связаны между собой таким образом — $V(E(m), D(s))$, что произвольное сообщение $m = m_1, m_2, \ldots, m_k \in M^*$ всегда однозначно преобразовывается в соответствующую криптограмму (шифртекст) $s = s_1, s_2, \ldots, s_k \in S^*$ и обратно. По криптограмме s всегда однозначно восстанавливается переданное сообщение m.

Альтернативным обозначением алгоритмов $E(m)$ и $D(s)$ для алфавитной криптосистемы (1) является K_E (или F_E) и K_D (или F_D) соответственно, как принято в классической криптографии [1]. Назовём их иначе ключами (или функциями) шифрования и дешифрования соответственно. Авторы не претендует на полноту освещения аналогичных математических моделей (1) алфавитных криптосистем.

Прежде всего, заметим, что прямое преобразование открытого текста m, состоящего из одного элементарного сообщения m_1 или конкатенации таких сообщений $m_1 m_2$, осуществляется путем равномерного увеличения длины ключа этого преобразования. Например, если в качестве элементарного сообщения выступает одна буква $m = *$ с числовым эквивалентом s_1, получаемый на основе стандартного ранца (аддитивного или мультипликативного) длины n, то конкатенации $m = **$ будет соответствовать числовой эквивалент $s_1 s_2$ длины $2 * n$, имеющий блоковую структуру.

1. Математическая модель задачи обобщенного мультипликативного ранца $K_{\mathbf{MG}}$. Обобщенные инъективные мультипликативные ранцы

Известно [2–5, 12, 13], что существующие математические модели аддитивных, мультипликативных рюкзачных систем защиты информации построены на основе двоичных 0-1 рюкзаков (ранцев). Автором [6–8] ранее были предложены различные варианты аддитивных рюкзачных задач и соответствующие им модели симметричных (асимметричных)

систем защиты информации на основе проблемы нестандартного рюкзака над Z_p, $p \geqslant 2$ (так называемые p-рюкзаки).

Рассмотрим вопрос обобщения двоичного мультипликативного ранца и предложим эффективный с точки зрения вычислительной сложности алгоритм построения инъективного мультипликативного обобщенного вектора над Z_p, $p \geqslant 2$. Математическую модель задачи обобщенного мультипликативного ранца K_{MG} представим следующим образом.

1.1. Задача K_{MG} (об обобщенном мультипликативном ранце)

Пусть имеются вектор $\mathbf{B}_{MG} = (b_1, b_2, \ldots, b_n)$ из n натуральных компонент $b_i \in N$, $i = 1, \ldots, n$ (назовем его обобщенным мультипликативным ранцем) и некоторое натуральное число V. Необходимо установить, существуют ли для заданного V такие значения $\alpha_i \in Z_p = \{0, 1, \ldots, p-1\}$, $p \in N$, $p \geqslant 2$, для которых справедливо равенство

$$\prod_{i=1}^{n} b_i^{\alpha_i} = V (\text{или } B_{MG}^{w_v} = V). \qquad (1.1)$$

Здесь $w_v = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha_i \in Z_p$, $p \geqslant 2$ спектр числа V, полученный на основе компонент обобщенно-мультипликативного вектора $\mathbf{B}_{MG}$. Если для заданного V существует подмножество элементов $\mathbf{B}_{MG}$, для которых имеет место равенство (1.1), то говорят, что вход $(\mathbf{B}_{MG}, V)$ обобщенно-мультипликативного ранца обладает решением $w_v = (\alpha_1, \alpha_2, \ldots, \alpha_n), \alpha_i \in Z_p$ и число V порождено спектром w_v на основе обобщенно-мультипликативного ранца $\mathbf{B}_{MG}$, иначе — решения нет.

Отметим, что в данной Задаче K_{MG} натуральное число $p \in \mathrm{N}, p \geqslant 2$ представляет собой так называемое пороговое значение для показателей степеней $\alpha_i \in Z_p$. В частности, если $p = 2$, то имеем двоичный спектр и 0-1 задачу о мультипликативном ранце [2–5, 12]. Для простоты изложения будем считать, что значения компонент ранцевого вектора $\mathbf{B}_{MG}$ расположены в возрастающем порядке и $b_1 \neq 1$, а его плотность $d(\mathbf{B}_{MG})$ определяется как

$$d(B_{MG}) = \frac{n}{\log(\max \mathbf{B}_{MG}; p)}.$$

Например, если $p = 5$, $\mathbf{B}_{MG} = (2, 3, 5, 7)$, то для входа ($\mathbf{B}_{MG}$, 48020) имеем следующий обобщенный спектр w_{548020} = (2,0,1,4), т.к. $V = 48020 = 2^2 * 3^0 * 5^1 * 7^4$. Здесь значение $V = 48020$ порождено спектром $w_{548020} = (2, 0, 1, 4)$ на основе обобщенно-мультипликативного ранца $\mathbf{B}_{MG} = (2, 3, 5, 7)$, а его плотность равна

$$d(\mathbf{B}_{MG}) = \frac{4}{\log(7; 5)} = 3{,}308350.$$

Для сравнения при $p = 2$ имеем

$$d(\mathbf{B}_{MG}) = \frac{4}{\log(7; 2)} = 1{,}424829 < 3{,}308349901.$$

Соответственно имеем следующие диапазоны значений для величины V: $1 \leqslant V \leqslant 1944810000$ и $1 \leqslant V \leqslant 210$.

Предварительно рассмотрим вопрос представления заданного значения V в виде произведения (1.1) компонент вектора $\mathbf{B}_{MG}$ при условии, что его компоненты либо не могут повторяться, как это требуется в известных источниках по построению ранцевых систем защиты информации с открытым ключом [2–5, 12, 13], либо могут повторяться над Z_p, $p \geqslant 2$, как предлагается в данной работе. Причём при моделировании систем защиты информации на основе заданного мультипликативного ранца нас будет интересовать случай, когда имеется не более одного представления для заданного натурального значения V.

Обобщённо-мультипликативный ранцевый вектор $\mathbf{B}_{MG}$ будем называть инъективным, если для произвольного значения V его вход $(\mathbf{B}_{MG}, V)$ обладает не более, чем одним решением. Очевидно, что количество $\mu(B_{MG})$ всех различных числовых входов $(\mathbf{B}_{MG}, V)$ для мультипликативного ранцевого вектора $\mathbf{B}_{MG}$ определяется равенством: $\mu(\mathbf{B}_{MG}) = p^n$. При этом, если для подобного вектора рассматриваются решения с коэффициентами повторений компонент $\mathbf{B}_{MG}$ из Z_p, то этот инъективный вектор будем называть обобщённо-мультипликативным ранцевым вектором и обозначим его через $\tilde{\mathbf{B}}_{MG}$. Так, например, для любого порогового значения p вектор $\tilde{\mathbf{B}}_{MG} = (p_1, p_2, \ldots, p_n)$ инъективен, если p_i, $i = 1, \ldots, n$ — произвольные простые числа. В более общем случае для практических приложений можно воспользоваться следующим утверждением.

Теорема 1. Возрастающий обобщённо-мультипликативный ранцевый вектор

$$\tilde{\mathbf{B}}_{MG} = (b_1, b_2, \ldots, b_n), \quad b_1 \neq 1$$

инъективен над

$$Z_p = \{0,1,\ldots,p-1\}, \quad p \geqslant 2,$$

если для всех индексов i и j, таких что $i \neq j$ компоненты b_i и b_j попарно взаимно просты.

Доказательство. Для простоты изложения рассмотрим случай произвольного порогового значения p и размерности ранца $n = 2$.

Пусть НОД$(b_1, b_2) = 1$. Очевидно, для любого $w_v = (\alpha_1, \alpha_2)$, $\alpha_i \in Z_p$ и $V = \tilde{B}_{MG}^{w_v} = (b_1)^{\alpha 1} * (b_2)^{\alpha 2}$ мультипликативный вход $(\tilde{\mathbf{B}}_{MG}, V)$ определяется однозначно. И наоборот, если НОД$(b_1, b_2) = 1$, то также однозначно определяется $w_v = (\alpha_1, \alpha_2), \alpha_i \in Z_p$ для заданногоV, т.к. из условия НОД$(b_1, b_2) = 1$ следует НОД$(b_1^{\alpha 1}, b_2^{\alpha 2}) = 1$. □

Следствие (Оператор L). Если обобщённо-мультипликативный ранцевый вектор

$$\tilde{\mathbf{B}}_{MG} = (b_1, b_2, \ldots, b_n)$$

инъективен над $Z_p = \{0,1,\ldots,p-1\}$, $p \geqslant 2$, то для любого натурального числа L вектор

$$\tilde{\mathbf{B}}_{MG}^{L} = (b_1^L, b_2^L, \ldots, b_n^L)$$

также инъективен, причем их мультипликативные входы определяются однозначно, т.е. $(\tilde{\mathbf{B}}_{MG}, V) = (\tilde{\mathbf{B}}_{MG}^{L}, V)$.

Аналогично доказывается следующая теорема относительно инъективности обобщённо-мультипликативного ранцевого вектора $\tilde{\mathbf{B}}_{MG}$.

Теорема 2. Возрастающий обобщённо-мультипликативный ранцевый вектор

$$\tilde{\mathbf{B}}_{MG} = (b_1, b_2, \ldots, b_n), \quad b_1 \neq 1$$

инъективен над

$$Z_p = \{0,1,\ldots,p-1\}, \quad p \geqslant 2$$

тогда и только тогда, когда каждый его компонент не является произведением других — с учётом их степеней.

Указанные *Теоремы* и *Следствие* позволяют разработать математические модели алфавитных криптосистем вида (1), стойкость которых можно увеличить за счёт применения изоморфных ранцев. Для произвольного порогового значения $p \geqslant 2$ и практических приложений приведём алгоритм построения инъективного обобщенно-мультипликативного ранцевого вектора.

Рассмотрим последовательность

$$\begin{gathered} b_1 = b \neq 1, \\ b_2 = b_1 + 1, \quad b_3 = b_1 b_2 + 1, \ldots, \\ b_n = b_1 b_2 \ldots b_{n-1} + 1, \end{gathered} \quad (1.2)$$

где $b \neq 1$ — произвольное натуральное число. Инъективность обобщённо-мультипликативного ранцевого вектора

$$\tilde{\mathbf{B}}_{MG} = (b_1, b_2, \ldots, b_n), \quad b_1 = b \neq 1,$$

с компонентами последовательности (1.2) следует из *Теоремы 2*.

Например, если $b = 2$, $n = 5$, то для произвольного порогового значения $p \geqslant 2$ имеем следующий инъективный обобщенно-мультипликативный ранцевый вектор $\tilde{\mathbf{B}}_{MG} = (2, 3, 7, 43, 1807, 3263443)$.

Приведём также математическую модель новой супер обобщенной мультипликативной задачи о ранце K_{MU}, обобщающей известную — стандартную K_{MS}.

1.2. Задача K_{MU} (о супер обобщенном мультипликативном ранце)

Пусть имеются вектор $\mathbf{B}_{MU} = (b_1, b_2, \ldots, b_n)$, состоящий из n натуральных компонентов b_i, $b_i \in N$, $b_1 \neq 1$, $i = 1, \ldots, n$ (назовем его супер обобщенным мультипликативным ранцем) и некоторое натуральное число V. Пусть далее

$$\begin{gathered} ZK_t = \{k_1, k_2, \ldots, k_t\}, \quad k_1 + k_2 + \ldots + k_t = n, \\ t \leqslant n, \\ ZC_p = \{m_1, m_2, \ldots, m_n\}, \\ 0 \leqslant m_i \leqslant p-1, \quad i = 1, \ldots, n \end{gathered} \quad (1.3)$$

— упорядоченные множества коэффициентов повторений компонент супер обобщенного мультипликативного ранца и его входа $(\mathbf{B}_{MU}, V)$ соответственно. В соотношениях (1.3) элемент k_i, $k_i \geqslant 1$, $i = 1, \ldots, t$, указывает количество повторений компонентов ранга натурального числа b_i в рюкзаке $\mathbf{B}_{MU}$ (здесь t — количество различных компонент ранца B_{MU}), а элемент $m_i \in ZC_p$, $i = 1, \ldots, n$ указывает максимальное значение коэффициента повтора при b_i, $i = 1, \ldots, n$ для определения супер обобщенного мультипликативного входа (B_{MU}, V), причём $p \geqslant 2$, $p \in N$ — некоторое пороговое числовое значение.

Упорядоченные множества ZK_t и ZC_p назовём спектрами коэффициентов супер обобщенного мультипликативного ранца $\mathbf{B}_{MU}$ и

его входа $(\mathbf{B}_{MU}, V)$ соответственно. Значения множества ZC_p иначе назовём каскадными значениями.

Например, если $t = 4$, $p = 3$ и

$$\mathbf{B}_{MU} = (1, 2, 5, 5, 13, 13, 13),$$

$$ZC_3 = \{1, 1, 1, 2, 2, 2, 1\},$$

то спектр коэффициентов рюкзака имеет вид

$$ZK_4 = \{1, 1, 2, 3\},$$

$$k_1 = 1, k_2 = 1, \quad k_5 = 2, \quad k_{13} = 3,$$

а спектр входа задан как ZC_3, для которого каскадные значения заданы как

$$m_1 \leqslant 1, \quad m_2 \leqslant 1, \quad m_3 \leqslant 1, m_4 \leqslant 2,$$

$$m_5 \leqslant 2, \quad m_6 \leqslant 2, \quad m_7 \leqslant= 1.$$

Супер обобщенный мультипликативный ранец $\mathbf{B}_{MU}$ при $t = n$ превращается в обобщенно-мультипликативный ранец $\mathbf{B}_{MG}$, если каскадные значения для его входа (B_{MU}, V) достигают своего порогового значения $p - 1$, т.е. когда спектр коэффициентов его входа имеет вид $ZC_p = \{p - 1, p - 1, \ldots, p - 1\}$, а спектр коэффициентов повторений компонент равен $ZK_n = \{1, 1, \ldots, 1\}$.

В частности, если $p = 2$ и $t = n$, то супер обобщенный мультипликативный ранец $\mathbf{B}_{MU}$ совпадает со стандартным мультипликативным ранцем $\mathbf{B}_{MS}$, а супер обобщенная мультипликативная задача о ранце K_{MU} — со стандартной задачей о рюкзаке K_{MS}. Для простоты изложения в данной работе опускаем рассмотрение случая ранца с повторениями и поэтому всюду ниже считаем, что $t = n$, т. е. ранец $\mathbf{B}_{MU}$ без повторений. Кроме того, известные факты, понятия и обозначения теории стандартных рюкзачных систем защиты информации [2,5] нетрудно перенести в теорию супер обобщенных мультипликативных ранцевых систем защиты информации, потому здесь они опущены.

2. Изоморфные аддитивные и мультипликативные ранцы

Пусть

$$A^n(N) = \{(a_1, a_2, \ldots, a_n) \,|\, a_k \in N\}$$

— множество всех ранцев первой степени размерности n над множеством N натуральных чисел. Соответственно,

$$A^n(N^i) = \{(a_1^i, a_2^i, \ldots, a_n^i) \,|\, a_k^i \in N\}$$

— множество всех ранцев степени i размерности n,

$$A^{n+1}(N) = \{(a_1, a_2, \ldots, a_n, a_{n+1}) \,|\, a_k \in N\}$$

— множество всех ранцев первой степени размерности $n + 1$.

Очевидно, что все инъективные обобщенно-мультипликативные ранцевые вектора $\tilde{\mathbf{B}}_{MG}$ размерности n также принадлежат множеству $A^n(N)$. Более того, можно доказать, что из инъективности ранца степени один $\tilde{\mathbf{B}}_{MG}$ = (2, 3, 5, 7, 11, 13) вытекает инъективность следующих ранцев более высоких степеней:

$\tilde{\mathbf{B}}^2_{MG}$ = (4, 9, 25, 49, 121, 169);

$\tilde{\mathbf{B}}^3_{MG}$ = (8, 27, 125, 343, 1331, 2197);

$\tilde{\mathbf{B}}^4_{MG}$ = (16, 81, 625, 1029, 14641, 28561);

$\tilde{\mathbf{B}}^5_{MG}$ = (32, 243, 3125, 16807, 161051, 371293) и т.д.

Заметим также, что все данные ранцы являются изоморфными ранцами, т.к. из равенства двух произвольных наборов $w_v^1 = w_v^2, \alpha_i^1 = \alpha_i^2$, т.е.

$$w_v^1 = (\alpha_1^1, \alpha_2^1, \ldots, \alpha_n^1), w_v^2 = \\ = (\alpha_1^2, \alpha_2^2, \ldots, \alpha_n^2), \alpha_i^1, \alpha_i^2 \in Z_p,$$

следует взаимно однозначное соответствие значений $V^1 \leftrightarrow V^2$, порожденными наборами w_v^1 и w_v^2.

Определение. Два ранца $\mathbf{A}$ и $\mathbf{B}$ из $A^n(N)$ назовём изоморфными ранцами $\mathbf{A} \cong \mathbf{B}$, если для каждого значения V_A, порожденного набором $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, существует единственное значение V_B — также порожденное этим же набором $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ и наоборот.

Отметим, что все сверхрастущие аддитивные рюкзаки одинаковой размерности изоморфны между собой [11]. Количество входов таких рюкзаков зависит только от их размерностей. Например, для $p = 3$ вектор $\tilde{\mathbf{B}}_{MG} = (2, 3, 5, 7, 11, 13)$ является инъективным обобщённо-мультипликативным ранцевым вектором размерности 6, содержащих $\mu(\tilde{\mathbf{B}}_{MG}) = 3^6 = 729$ входов — против 64 для двоичного стандартного случая.

3. Математическая модель криптосистемы на основе обобщенно-мультипликативного ранца

Рассмотрим простой пример алфавитной симметричной криптосистемы (1) на основе обобщенно-мультипликативного ранцевого вектора $\tilde{\mathbf{B}}_{MG} = (2, 3, 5, 7, 11, 13)$ размерности $n = 6$ над $Z_{11} = \{0, 1, 2, 3, \ldots, 10\}$.

Пусть исходный открытый текст $m =$ КАО представлен заглавными буквами русского алфавита, а буквам K, A и O соответствуют следующие обобщенные спектры:

$w_K = (1,\ 3,\ 0,\ 5,\ 8,\ 0)$,
$w_A = (0,\ 6,\ 0,\ 8,\ 8,\ 4)$,
$w_O = (1,\ 4,\ 0,\ 4,\ 9,\ 0)$.

Тогда соответствующие шифры s_1, s_2 и s_3 симметричной криптосистемы (1) определяются как функции от w_v вида $F_E(w_v) = \tilde{B}_{MG}^{w_V}$:

$$s_1 = F_E(1,3,0,5,8,0) = \tilde{B}_{MG}^{w_K} = 2^1 * 3^3 * 5^0 * 7^5 * 11^8 * 13^0 = 194547404500218,$$

$$s_2 = F_E(0,6,0,8,8,4) = \tilde{B}_{MG}^{w_A} = 2^0 * 3^6 * 5^0 * 7^8 * 11^8 * 13^4 = 25729227018489228122889,$$

$$s_3 = F_E(1,4,0,4,9,0) = \tilde{B}_{MG}^{w_O} = 2^1 * 3^4 * 5^0 * 7^4 * 11^9 * 13^0 = 917152049786742.$$

Таким образом, открытому тексту $m =$ КАО соответствует следующий шифртекст

$$s = s_1 s_2 s_3 = 194547404500218 * 25729227018489228122889 * 917152049786742,$$

где $*$ — символ разделитель.

Рассмотрим теперь алгоритм дешифрования $D(s)$ для указанного примера и определим обобщенный спектр, например, относительно следующего шифра $s_1 = 194547404500218$, на основе заданного обобщенно-мультипликативного ранцевого вектора $\tilde{\mathbf{B}}_{MG} = (2, 3, 5, 7, 11, 13)$.

Найдем первое частное от деления $s_1 = 194547404500218$ на максимальную степень наибольшего компонента $b_6 = 13$ ранца $\tilde{\mathbf{B}}_{MG}$

$$s_1 = 194547404500218 = 194547404500218 * 13^0,$$

затем полученное частное 194547404500218 делим на максимальную степень следующего компонента $b_5 = 11$ ранца $\tilde{\mathbf{B}}_{MG}$ и т.д.

Имеем

$$s_1 = 194547404500218 * 13^0 = 907578 * 11^8 * 13^0 = 54 * 7^5 * 11^8 * 13^0 = 54 * 5^0 * 7^5 * 11^8 * 13^0 = 2^1 * 3^3 * 5^0 * 7^5 * 11^8 * 13^0,$$

что позволяет однозначно выписывать спектр $w_K = (1, 3, 0, 5, 8, 0)$ и соответствующее ему первое элементарное сообщение $m_1 = K$. Аналогично поступаем относительно других шифров s_2, s_3 и устанавливаем соответствующие им элементарные сообщения $m_2 = A$, $m_3 = O$.

Отметим, что приведённый способ восстановления открытого текста справедлив лишь для инъективных векторов, определённых в *Теоремах 1, 2*, в общем случае существуют такие инъективные рюкзачные векторы, что решения задачи об обобщенно-мультипликативном рюкзаке возможно лишь с помощью переборного алгоритма экспоненциальной сложности.

Аналогично можно разработать алфавитную асимметричную криптосистему (1) на основе соответствующего изоморфного обобщенно-мультипликативного ранцевого вектора $\tilde{B}_{MG}$.

В более общем случае имеет место следующая теорема.

Теорема 3. Пусть $\tilde{\mathbf{A}}_{MG} = (a_1, a_2, \ldots, a_n)$ и $\tilde{\mathbf{B}}_{MG} = (b_1, b_2, \ldots, b_n)$, $a_1 \neq 1$, $b_1 \neq 1$ — два инъективных обобщённо-мультипликативных ранца над $GF(p)$ размерности n, $n \geqslant 3$, $b_i = \log_g a_i^L (\mathrm{mod}\ p)$, g — примитивный элемент поля $GF(p)$.

Тогда решения задач об обобщённо-мультипликативных ранцах $\tilde{\mathbf{A}}_{MP}$ и $\tilde{\mathbf{B}}_{MP}$ над $GF(p)$ изоморфны.

Доказательство. Некоторые несущественные детали опустим и лишь докажем, что для произвольного шифра инъективные обобщённо-мультипликативные ранцы $\tilde{\mathbf{A}}_{MP}$ и $\tilde{\mathbf{B}}_{MP}$ над $GF(p)$ изоморфны между собой.

В самом деле, для произвольного шифра **s** имеем

$$s = V_B = b_{i_1} + b_{i_2} + \ldots + b_{i_r} = \\ = g^{\log_g a_{i_1}^L + \log_g^{a_{i_2}^L} + \ldots + \log_g^{a_{i_r}^L}} = \\ = a_{i_1}^L * a_{i_2}^L * \ldots * a_{i_r}^L = \\ = (a_{i_1} * a_{i_2} * \ldots * a_{i_r})^L = V_A,$$

– что подтверждает изоморфность двух обобщённо-мультипликативных ранцев $\tilde{\mathbf{A}}_{MP}$ и $\tilde{\mathbf{B}}_{MP}$ над $GF(p)$. Очевидно, значение L заранее определяется. □

Здесь следует сделать следующее замечание: процедура восстановления открытого текста в целом не зависит от самих компонент ранцевого вектора, она зависит только от размера самого ранца, значения L и способа первоначального кодирования букв открытого текста. Данное замечание относится ко всем существующим открытым ранцевым системам.

Заключение

Изучается вопрос разработки математических моделей алфавитных криптосистем в виде кортежа, в которых в качестве алфавита чаще всего выступает либо алфавит некоторого естественного языка (например, английского), либо некоторый числовой алфавит (например, двоичный алфавит) или, например, поле Галуа $GF(p)$, состоящее из p элементов и т.п.

Рассмотрена задача построения изоморфных аддитивных и мультипликативных ранцев и предложена математическая модель криптосистемы на основе обобщенно-мультипликативного ранца, стойкость которой можно увеличить за счёт применения изоморфных ранцев (Теорема 3). Установлены необходимые и достаточные условия на основе Теорем 1, 2, при которых обобщённо-мультипликативный ранцевый вектор $\tilde{B}_{MP}$ инъективен над Z_p, $p \geqslant 2$. При этом в отличие от существующих математических моделей аддитивных или мультипликативных ранцевых систем, здесь рассмотрен и случай, когда коэффициенты входа могут повторяться заданное число раз из заданных множеств Z_p или ZC_p. Криптостойкость таких систем для больших значений параметров ранцевых векторов выше и обладает повышенной плотностью по сравнению с известными ранцами.

Аналогично можно рассмотреть супер обобщенные мультипликативные ранцы и их математические модели систем защиты информации, разрабатываемые совершенно идентично.

Литература

1. *Shannon C.* Communication theory of secrecy systems // Bell System Techn. J. 1949. Vol. 28. No. 4. P. 656–715.
2. *Merkle R., Hellman M.* Hiding information and signatures in trapdoor knapsacks // IEEE Transactions on Information Theory. 1978. Vol. IT-24. P. 525–530.
3. *Rivest R.L., Chor B.* A knapsack-type public key cryptosystem based on arithmetic in finite fields // IEEE Transactions on Information Theory. 1988. Vol. 34. No. 5. P. 901–909.
4. *Shamir A.* A polynomial-time algorithm for breaking the basic Merkle–Hellman cryptosystem // IEEE Transactions on Information Theory. 1984. Vol. 30. No. 5. P. 699–704.
5. *Koblitz N.* A Course in Number Theory and Cryptography. New York, Springer-Verlag, 1987.
6. *Осипян В.О.* Об одном обобщении рюкзачной криптосистемы // Известия вузов. Сев.-Кавк. регион. Техн. науки. 2003. Прил. № 5. С. 18–25.
7. *Осипян В.О.* О системе защиты информации на основе функционального рюкзака // Вопросы защиты информации. 2004. № 4. С. 16–18.
8. *Осипян В.О.* О системе защиты информации на основе проблемы рюкзака // Известия Томского политехнического университета. 2006. Т. 309. № 2. С. 209–212.
9. *Осипян В.О., Арутюнян А.С., Спирина С.Г.* Моделирование ранцевых криптосистем, содержащих диофантовую трудность // Чебышевский сборник. 2010. Т. XI. Вып. 1. С. 209–217.
10. *Осипян В.О., Карпенко Ю.А., Жук А.С., Арутюнян А.Х.* Диофантовы трудности атак на нестандартные рюкзачные системы защиты информации // Известия ЮФУ. Технические науки. 2013. № 12. С. 209–215.
11. *Osipyan V.O.* Information protection systems based on universal knapsack problem // SIN'13 Proceedings of the 6th International Conference on Security of Information and Networks, ACM, 2013. P. 343–346.
12. *Lenstra, Jr. H.W.* Integer Programming with a Fixed Number of Variables // Mathematics of Operations Research. 1983. Vol. 8. No. 4. pp. 538–548.
13. *Vaudenay S.* Cryptanalysis of the Chor-Rivest cryptosystem. Advances in Cryptology - CRYPTO '98: Proc. of 18th Annual International Cryptology Conference Santa

Barbara, California, USA August 23–27, 1998. P. 243–256. DOI: 10.1007/BFb0055732

References

1. Shannon C. Communication theory of secrecy systems. *Bell System Techn. J.*, 1949, vol. 28, no. 4, pp. 656–715.
2. Merkle R., Hellman M. Hiding information and signatures in trapdoor knapsacks. *IEEE Transactions on Information Theory*, 1978, vol. IT–24, pp. 525–530.
3. Rivest R.L., Chor B. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 1988, vol. 34, no. 5, pp. 901–909.
4. Shamir A. A polynomial-time algorithm for breaking the basic Merkle–Hellman cryptosystem // Information Theory, IEEE Transactions. 1984. Vol. 30. No. 5. pp. 699–704.
5. Koblitz N. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1987.
6. Osipyan V.O. Ob odnom obobshchenii rukzachnoi kriptosistemi [On a generalization of a knapsack cryptosystem]. *Izv. vuzov Sev.-Kavk. reg.* [Bulletin of the Universities of the Nord Caucasus region], 2003, no. 5, pp. 18–25.
7. Osipyan V.O. O sisteme zashchity informatcii na osnove funktcional'nogo rukzaka [On a security system based on functional knapsack]. *Voprosy zashchity informatcii* [Question of information's security], 2004, no. 4, pp. 16–18.
8. Osipyan V.O. O sisteme zashchity informatcii na osnove problemy rukzaka [On a security system based on knapsack's problem]. *Izvestiya Tomskogo Politekhnicheskogo universiteta* [Bulletin of Tomsk politechnical University], 2006, vol. 309, no 2, pp. 209–212.
9. Osipyan V.O., Harutunyan A.S., Spirina C.G. Modelirovanie rantcevyh kriptosistem, sodergashchikh diophantovuyu trudnost' [Modelling of knapsack cryptosystem Diophantine difficulty contains]. *Chebyshevskii sbornik* [Chebyshev's digest], 2010, vol. XI, no. 1, pp. 209–217.
10. Osipyan V.O., Kerpenko Y.A., Zhuk A.S., Harutunyan A.H. Diofantovy trudnosti atak na nestandartnye rukzachnye sistemy zashchity informatcii [Diophantine difficulties of attacks on non-standard knapsack security systems]. *Izvestiya UFU. Tekhnicheskie nauki* [Bulletin of South Federal University. Technical sciences]. 2013, no. 12, pp. 209–215.
11. Osipyan V. O. Information protection systems based on universal knapsack problem. *SIN'13: Proc. of the 6th International Conference on Security of Information and Networks, ACM, 2013*, pp. 343–346.
12. Lenstra, Jr. H.W. Integer Programming with a Fixed Number of Variables. *Mathematics of Operations Research*, 1983, vol. 8, no. 4, pp. 538–548.
13. Vaudenay S. Cryptanalysis of the Chor-Rivest cryptosystem. *Advances in Cryptology - CRYPTO '98: Proc. of 18th Annual International Cryptology Conference Santa Barbara, California, USA August 23–27, 1998*, pp. 243–256. DOI: 10.1007/BFb0055732

Статья поступила 18 апреля 2017 г.