7. *Alshwede R., Cai N., Li S.-Y. R., Yeung R.W.* Network information flow // IEEE Trans. Inf. Theory. – 2000. – Vol. 46. – P. 1204-1216.
8. *Koetter R., Kschischang F.R.* Coding for errors and erasures in random network coding // IEEE Trans. Inf. Theory. – 2008 – Vol. IT-54, № 8. – P. 3579-3591.
9. *Li S.-Y. R., Yeung R. W., Cai N.* Linear network coding // IEEE Trans. Inf. Theory. – 2003. – Vol. 49. – P. 371-381.
10. *Diffie W., Hellman M.E.* New Directions in Cryptography // IEEE Trans. Inf. Theory. – 1976. – Vol. IT-22, № 6. – P. 644-654.
11. *McEliece R.J.* A Public Key Cryptosystem Based o Algebraic Coding Theory // JPL DSN Progress Rep. – 1978. – Vol. 42-44. – P. 114-116.

Статью рекомендовал к опубликованию к.т.н., доцент Н.С. Могилевская.

Михайлова Екатерина Александровна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: mikhailovaekaterina@yandex.ru; 344000, г. Ростов-на-Дону, ул. Красноармейская, 196, кв. 8; тел.: 89185879710; кафедра алгебры и дискретной математики; аспирантка.

Mikhailova Ekaterina Aleksandrovna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: mikhailovaekaterina@yandex.ru; 196, Krasnoarmejskaya street, fl. 8, Rostov-on-Don, 344000, Russia; phone: +79185879710; the department of algebra and discrete mathematics; postgraduate student.

УДК 519.72

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

ДИОФАНТОВЫ ТРУДНОСТИ АТАК НА НЕСТАНДАРТНЫЕ РЮКЗАЧНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Развитие ассиметричной криптографии началось с появления первой рюкзачной системы защиты информации, когда в 1976 году Ральф Меркель и Мартин Хеллман предложили использовать разные ключи для прямого и обратного преобразования данных при шифровании. На данный момент эта модель, как и многие, основанные на ней были скомпрометированы. Как следствие, авторитет рюкзачных систем занижен. Тем не менее, некоторые из них, до сих пор считаются стойкими, например, модель, предложенная в 1988 году Беном Шором и Рональдом Ривестом. В данной работе сформулирована и решена задача аргументации криптографической стойкости нестандартных рюкзачных систем защиты информации, которые допускают повторное использование элементов рюкзака. Обоснованы диофантовы трудности, возникающие при поиске уязвимостей в указанных системах защиты информации. На основе анализа ранее предложенных рюкзачных моделей выявлены качественные особенности нестандартных рюкзачных систем, повышающие их стойкость к известным атакам.

Рюкзачные системы защиты информации; стойкость алгоритма; криптографическая атака, диофантовы трудности; рюкзачный алгоритм; рюкзачный вектор; исходное сообщение; открытый текст; ключ; шифртекст.

V.O. Osipyan, Yu.A. Karpenko, A.S. Zhuck, A.H. Arutyunyan

DIOPHANTINE DIFFICULTIES OF ATTACKS ON NON-STANDARD KNAPSACKS INFORMATION SECURITY SYSTEMS

Development of the asymmetric cryptography started with the appearance of the first knapsack information protection system, when, in 1976, Ralph Merkel and Martin Hellman proposed to use different keys for forward and reverse mapping data for encryption. Now this model, like many based on are considered to be insecure. As a result the authority of knapsack systems was low.

However, some of these systems are still considered persistent, for example, the model proposed in 1988 by Ben Shore and Ronald Rivest. In the article stated and solved the problem of argumentation of cryptographic strength of the non-standard knapsack information security systems. Justified diophantine difficulties that arise in the study of vulnerabilities of the investigated information security systems. Revealed the qualitative features of non-standard knapsack systems that increase their resistance to known attacks.

Knapsack information security system; resistance of algorithm; cryptographic attack; diophantine difficulties; knapsack algorithm; knapsack vector; original message; plain text; key; ciphertext.

Введение. С точки зрения теоретических основ информационной безопасности и разработки эффективных систем защиты информации следует обратить особое внимание на то, что трудно разрешимые математические проблемы могут быть основой для систем сокрытия и защиты информации с требуемыми свойствами, а решения этих задач соответствуют ключам этих систем [1]. В то же время выбор проблемы позволяет получить систему защиты информации требуемого уровня надежности. В частности, согласно К. Шеннону [2], если этот выбор связан с проблемой, содержащей диофантовы трудности, или в целом, относится к классу -полных проблем.

Традиционно, в основе всех стандартных рюкзачных систем защиты информации (РСЗИ) лежит **NP**-полная задача об укладке рюкзака или ранца $\boldsymbol{K_S}$. На сегодняшний день предложены и модели РСЗИ на основе задачи о нестандартном рюкзаке $\boldsymbol{K_N}$ [3]**,** для которого допустимо повторения элементов рюкзака. Наиболее общей из них является модель $\boldsymbol{M_G}$ на основе обобщенно рюкзака. Так же предложены и исследованы [4] модели $\boldsymbol{M_U}$ и $\boldsymbol{M_F}$ на основе задач о универсальном и функциональном рюкзаках соответственно.

Задача $\boldsymbol{K_S}$ (о стандартном рюкзаке).

Дан рюкзачный вектор $\boldsymbol{A = (a_1, \dots, a_n)}$ *с натуральными компонентами* $\boldsymbol{a_i}$, $\boldsymbol{i = \overline{1,n}}$. *По заданному входу* $\boldsymbol{v} \in \mathbb{N}$ *определить такой набор индексов* $\boldsymbol{J \subset \overline{1,n}}$, *для которого имеет место равенство:*

$$\boldsymbol{v = \sum_{j \in J} a_j}. \quad (1)$$

Первые из таких систем были описаны еще в 1978 году Р. Мерклем и М. Хеллманом [5]. Ими была предложена идея линейного преобразования рюкзака посредством сильного модульного умножения. Позднее в протоколе Шора-Ривеста [6], в отличие от протокола Меркеля-Хеллмана, рюкзак представлял собой набор логарифмов в мультипликативной группе поля и обладал повышенной плотностью по сравнению с рюкзаком Меркля-Хеллмана.

Приведем постановки задач о нестандартных рюкзаках.

Задача $\boldsymbol{K_G}$ (об обощенном рюкзаке).

Дан рюкзачный вектор $\boldsymbol{A = (a_1, \dots, a_n)}$ *с натуральными компонентами* $\boldsymbol{a_i}$, $\boldsymbol{i = \overline{1,n}}$, *а также* $\boldsymbol{p} \in \mathbb{N}$ *– ограничение на количество повторений любой из компонент вектора* $\boldsymbol{A}$. *По заданному входу* $\boldsymbol{v} \in \mathbb{N}$ *необходимо найти такой набор коэффициентов повторений* $\boldsymbol{x = (x_1, \dots, x_n)}$, *для которого имеет место равенство:*

$$\boldsymbol{v = \sum_{i=\overline{1,n}} x_i a_i}\,. \quad (2)$$

В отличие от классической задачи $\boldsymbol{K_S}$, *где* i*-ый предмет либо кладется в рюкзак, либо нет, в данной задаче – можно класть в рюкзак несколько экземпляров* i*-го предмета.*

Задача $\boldsymbol{K_U}$ (об универсальном рюкзаке).

Дан рюкзачный вектор $\boldsymbol{A = (a_1, \dots, a_n)}$ *с натуральными компонентами* $\boldsymbol{a_i}$ *, а также ограничения на количество повторений* $\boldsymbol{m = (m_1, \dots, m_n)}$*, то есть число* $\boldsymbol{x_i}$ *вхождений компоненты* $\boldsymbol{a_i}$ *не превосходит* $\boldsymbol{m_i}$ *. По заданному входу* $\boldsymbol{v \in \mathbb{N}}$ *и ограничениям определить такой допустимый набор коэффициентов повторений* $\boldsymbol{x = (x_1, \dots, x_n)}$*, для которого имеет место равенство* (2).

Задача $\boldsymbol{K_F}$ (о функциональном рюкзаке).

Дан функциональный рюкзачный вектор $\boldsymbol{A = \big(a_1(x), \dots, a_n(x)\big)}$ *с компонентами* $\boldsymbol{a_i(x)}$*,* $\boldsymbol{i = \overline{1,n}}$ *, являющимися целочисленными функциями от переменной* $\boldsymbol{x \in \mathbb{Z}}$ *. Даны также* $\boldsymbol{v(x)}$ *– целочисленная функция от переменной* $\boldsymbol{x}$ *и число* $\boldsymbol{x_0 \in \mathbb{Z}}$ *. По заданному входу* $\boldsymbol{v(x)}$ *и точке* $\boldsymbol{x_0}$ *необходимо найти такой набор коэффициентов повторений* $\boldsymbol{\alpha = (\alpha_1, \dots, \alpha_n)}$*, для которого имеет место равенство:*

$$\boldsymbol{v(x_0) = \sum_{i=\overline{1,n}} \alpha_i a_i(x_0)} \,. \qquad (3)$$

Элементы функционального рюкзака являются не целыми числами, а целочисленными функциями. Все вопросы моделирования универсальных, а следовательно, и обобщённых, и стандартных систем защиты информации с незначительными поправками переносятся в теорию моделирования функциональных систем защиты информации. Исследование функциональных систем защиты информации выход за рамки данной работы.

Исследованию задач о рюкзаке уделено большое внимание в литературе. Широкий спектр таких задач, алгоритмы решения и их реализации описаны, например, С. Мартелло [7]. При решении подобных задач оптимизация основана на поиске верхних и нижних границ для решений. Ограничения выводятся из дополнительного условия на максимизацию или минимизацию некоторой функции. Аналогичные рассуждения теряют смысл при исследовании РСЗИ, ведь все они строятся над конечными полями, а неравенства, имеющие место на множестве целых чисел, теряют смысл в мультипликативных группах полей.

Рассмотрим проблему об атаках на рюкзачные системы и возможности их применения к нестандартным рюкзачным системам, основанным на задаче $\boldsymbol{K_G}$ об универсальном рюкзаке.

Анализ математических моделей $\boldsymbol{M_S}$ стандартных рюкзачных систем защиты информации. Первой системой защиты информации на основе задачи о рюкзаке был протокол Меркеля-Хеллмана [8]. Это ассиметричная модель, которая предполагает двоичное кодирование сообщения как входа для некоторого сверхрастущего рюкзачного вектора $\boldsymbol{A}$**.** Под действием модульного умножения этот вектор «маскируется» вектором $\boldsymbol{B}$:

$$\boldsymbol{B = (b_1, \dots, b_2)}, \text{ где } \boldsymbol{b_i = e \cdot a_i (\mathbf{mod}\, M)}. \qquad (4)$$

Для восстановления полученного сообщения $\boldsymbol{m = x \cdot A^T}$ принимающая сторона использовала векторы $\boldsymbol{B}$, $\boldsymbol{x}$ и пару параметров $\boldsymbol{(d, M)}$, необходимых для обратного модульного умножения.

В 1982 году Шамир [9], ссылаясь на теорему Ленстра о задаче целочисленного программирования с конечным числом переменных, предложил атаку на стандартную рюкзачную систему защиты информации Меркеля-Хеллмана. Согласно предложенному алгоритму для указанных систем удаётся определить новую «лазейку» – наименьшие $\boldsymbol{M'}$ и $\boldsymbol{d'}$, применимые вместо исходных $\boldsymbol{M}$ и $\boldsymbol{d}$**.** При этом, во-первых, вектор $\boldsymbol{\widetilde{A} = d' \cdot B^T (\mathbf{mod}\, M')}$ сверхрастущий, а во-вторых, $\boldsymbol{m = x \cdot \widetilde{A}^T}$**.**

При создании сверхрастущего рюкзачного вектора в системе Меркеля-Хеллмана предполагалось ограничение, согласно которому каждый следующий элемент $\boldsymbol{a_i}$ ограничен снизу суммой всех предыдущих, а сверху – удвоенным значением $\boldsymbol{a_{i-1}}$.

Как отмечает Шамир [9] время для его атаки полиномиально зависит от длины рюкзака и экспоненциально от константы пропорциональности $\boldsymbol{k}$:

$$\boldsymbol{k = \max_i \left\lceil \frac{a_i}{a_{i+1}} \right\rceil = 2}. \quad (5)$$

Подобные оценки приводит и Ленстра [10]. При доказательстве теоремы используется алгоритм поиска решения, полиномиальный по времени, но не от $\boldsymbol{n}$ – количества переменных, а от экспоненты, примененной к $\boldsymbol{n}$.

На основе техники, предложенной Шамиром, позднее были реализованы атаки и на другие двоичные модификации стандартной РЗСИ.

После атаки Шамира последовала серия новых моделей и идей по улучшению скомпрометированной. Однако, эти предложения объединяла одна общая деталь. Они включали этап, на котором происходила укладка некоторого стандартного рюкзака.

Одна из самых известных стандартных рюкзачных систем защиты информации предложена в 1988 Беном Шором и Рональдом Ривестом. Это была первая система, которая не использовала модульное умножение для того, чтобы скрыть рюкзачный вектор. Вместо этого использовалась арифметика конечных полей Галуа $\mathbb{F}_{p^h}$.

В стандартном случае при $\boldsymbol{p = 197}$ и $\boldsymbol{h = 24}$ в 1998 году Ваундау [11] удалось найти уязвимость в системе Шора-Ривеста. Хотя в скором времени эту уязвимость удалось устранить, применив новые значения параметров $\boldsymbol{p = 409}$ и $\boldsymbol{h = 17}$. Среди прочих особенностей атака использовала малую плотность рюкзака. Так для Шора-Ривеста плотность составляла:

$$\boldsymbol{d = \frac{p}{\log_2(p^h - 2)} \approx \frac{p}{h \log_2 p} = \frac{1}{\beta \log_2 p}}, \text{ где } \boldsymbol{\beta = \frac{h}{p}}. \quad (6)$$

Исследования атаки Вандау и её обобщения [12] показали, что лишь при $\boldsymbol{d \gg 1}$ можно добиться стойкости системы Шора-Ривеста. Для достижения таких значений плотности целесообразно отказаться от ограничений на повторное использование элементов рюкзака, что характерно для нестандартных РСЗИ.

Математические модели $\boldsymbol{M_N}$ нестандартных рюкзачных систем защиты информации. В серии работ [3], [4], [13] и других предложены рюкзачные модели защиты информации, принципиально отличающиеся от всех описанных ранее. Общей их особенностью является то, что в отличие от стандартного случая, допустимы повторения компонент. Сообщение в этой модели сообщение разбивается на буквенные блоки, вместо которых далее рассматриваются их числовые эквиваленты $\boldsymbol{v} \in \mathbb{Z}_M$.

Параметры и преобразования простейшей схемы на основе нестандартного рюкзака можно представить следующим образом:

- *Параметры системы:* основание системы, размер рюкзачных векторов и вектора ограничений на количество повторений элементов рюкзака:
$$\boldsymbol{M \in \mathbb{N}, n \in \mathbb{N}, m = (m_1, \dots, m_n)}. \quad (7)$$
- *Закрытый ключ:* элемент для модульного умножения $\boldsymbol{e \in \mathbb{Z}_M}$, $\boldsymbol{(e, M) = 1}$ и сверхрастущий рюкзачный вектор:
$$\boldsymbol{A = (a_1, \dots, a_n) \ | \ a_i \in \mathbb{Z}_M, \ a_i > \sum_{j=1}^{i-1} m_j a_j}, \quad (8)$$
- *Открытый ключ:*
$$\boldsymbol{d \in \mathbb{Z}_p \mid ed = 1 \ (\mathrm{mod}\, M), \ B = (b_1, \dots, b_n) \mid b_i = e a_i (\mathrm{mod}\, M)}. \quad (9)$$
- *Прямое преобразование:* для входа $\boldsymbol{(A, m)}$ вычисляется спектр $\boldsymbol{x}$:
$$\boldsymbol{x = (x_1, \dots, x_n) \ | \ m = \sum_1^n x_i a_i, \ x_i = \overline{1, m_i}}. \quad (10)$$

- *Обратное преобразование:* спектр входа $\boldsymbol{x}$ применяется к рюкзаку $\boldsymbol{B}$, затем выполняется обратное модульное умножение:

$$\boldsymbol{m'} = \sum_1^n \boldsymbol{x_i b_i} = \sum_1^n \boldsymbol{x_i}(\boldsymbol{e a_i}) = \boldsymbol{e}\sum_1^n \boldsymbol{x_i a_i} = \boldsymbol{em}\ (\mathbf{mod}\ \boldsymbol{M}). \qquad (11)$$
$$\boldsymbol{dm'} = \boldsymbol{m}\ (\mathbf{mod}\ \boldsymbol{M}).$$

Рассмотрим возможность применения атак на системы, заданные условиями (7)–(11). Особый интерес представляют техники, не требующие получения части закрытого ключа.

Перейдем к анализу математических моделей нестандартных рюкзачных систем защиты информации $\boldsymbol{M_N}$. Классической атака на рюкзачные системы стандартного вида [5] не требует даже частичных знаний о закрытом ключе. Как уже было отмечено выше, атаки такого типа экспоненциально зависят от параметра системы $\boldsymbol{k}$ (5). Для нестандартных РСЗИ эта константа равна одному из основных параметром. Как следствие, для таких систем диофантова аппроксимация не применима.

Еще одним преимуществом использования спектров с повторениями является увеличение множества допустимых значений входа [3]. Для достаточно больших $\boldsymbol{p}$ и даже при $\boldsymbol{n} \leq \mathbf{4}$ это еще больше усложняет определение рюкзака по методу Шамира. Таким образом, плотность рюкзака не уменьшается при увеличении разницы между элементами рюкзака.

В пользу увеличения параметра $\boldsymbol{p}$ говорит и наличие методов компрометирования рюкзачных систем с малым количеством повторяющихся элементов [14]. Например, это касается систем, при моделировании которых используется несколько независимых рюкзаков, множества элементов которых могут пересекаться.

Оценим мощность множество различных значений входа:

Лемма 1.

Для системы (7)-(11) при $\boldsymbol{m_i = p - 1, a_i = p^{i-1}}$ *допустим любой вход* $\boldsymbol{v} \in [\mathbf{1}; \boldsymbol{p^n - 1}]$*, то есть найдется единственный* $\boldsymbol{x}$ *такой, что* $\sum_{i=1}^{n} \boldsymbol{x_i a_i} = \boldsymbol{v}$**.**

Рюкзачный вектор, для которого допустим любой вход от минимального до максимального, называется *плотным*. Данная лемма дает представление о том, каким образом следует задавать параметр $\boldsymbol{M}$:

$$\boldsymbol{M \geq p^n}.$$

Лемма 2.

Для системы (7)-(11) при $\boldsymbol{m_i = p - 1, a_i = p^{i-1} + d_i}$ **,** $\boldsymbol{d_i > p d_{i-1}, d_1 > 0}$**.** *для любого входа* $\boldsymbol{v} \in [\mathbf{1}; \boldsymbol{p^n - 1}]$ *из его допустимости следует единственность соответствующего спектра.*

Доказательство:

Допустим, для входа $\boldsymbol{v}$ нашлись два различных спектра $\boldsymbol{x}$ и $\boldsymbol{y}$:

$$\sum_{i=1}^{n} \boldsymbol{x_i}(\boldsymbol{p^{i-1} + d_i}) = \sum_{i=1}^{n} \boldsymbol{y_i}(\boldsymbol{p^{i-1} + d_i})$$
$$\sum_{i=1}^{n} (\boldsymbol{x_i - y_i})(\boldsymbol{p^{i-1} + d_i}) = \mathbf{0}$$

Пусть $\boldsymbol{j}$ – наибольший индекс, для которого $\boldsymbol{x_i \neq y_i}$. Можно считать, что $\boldsymbol{x_i > y_i}$. Тогда

$$\sum_{i=1}^{n} (\boldsymbol{x_i - y_i})(\boldsymbol{p^{i-1} + d_i}) = \big(\boldsymbol{x_j - y_j}\big)\big(\boldsymbol{p^{j-1} + d_j}\big) + \sum_{i=1}^{j-1} (\boldsymbol{x_i - y_i})(\boldsymbol{p^{i-1} + d_i}) >$$
$$> \boldsymbol{p^{j-1} + d_j} - \sum_{i=1}^{j-1} \boldsymbol{p}(\boldsymbol{p^{i-1} + d_i}) > 0.$$

Использование рюкзачных векторов указанного вида гарантирует однозначность прямого преобразования.

Рассмотрим возможность применения атаки типа Шамира на систему (7)–(11), удовлетворяющую условиями **Леммы 2.** Без ограничения общности можно считать, что компоненты вектора $\boldsymbol{A}$ представлены в порядке убывания. Напомним, что целью атаки является поиск такого модуля $\boldsymbol{M'}$, не обязательно равного $\boldsymbol{M}$, и сверхрастущего вектора $\widetilde{\boldsymbol{A}} = \boldsymbol{d'} \cdot \boldsymbol{B^T} (\mathbf{mod}\, \boldsymbol{M'})$, для которых:

$$\widetilde{\boldsymbol{m}} = \boldsymbol{x} \cdot \widetilde{\boldsymbol{A}}^{\boldsymbol{T}} = \boldsymbol{x} \cdot \boldsymbol{A}^{\boldsymbol{T}} = \boldsymbol{m}.$$

В качестве ограничения на $\boldsymbol{M'}$ можно взять $\boldsymbol{b_1} \cdot \log_{\boldsymbol{n}} \boldsymbol{b_1}$. Для поиска $\boldsymbol{d'}$ следует рассмотреть все $\boldsymbol{0} \le \boldsymbol{d} \le \boldsymbol{M'}$ и исследовать графики функции $\boldsymbol{da_i} (\mathbf{mod}\, \boldsymbol{M'})$ при неизвестном $\boldsymbol{d}$. Эти графики имеет форму пилы с расстоянием между минимумами $\boldsymbol{M'/a_i}$ (рис. 1).

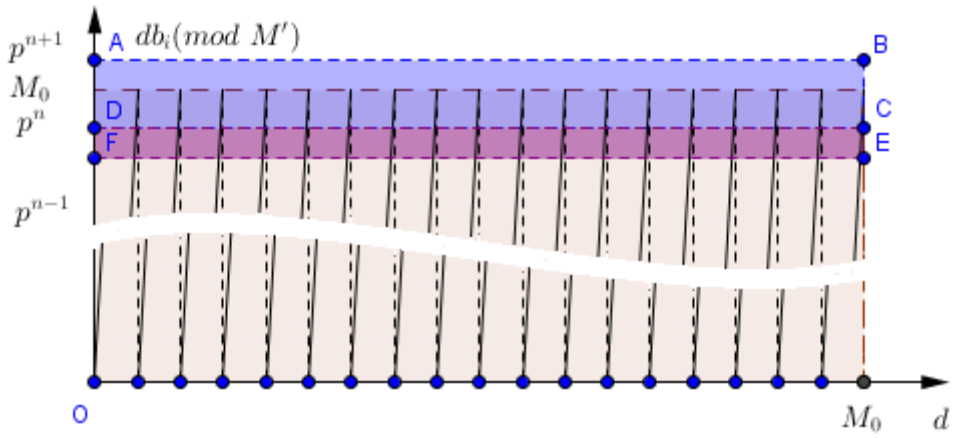

Рис. 1

Из ограничений на наибольший элемент сверхрастущего рюкзачного вектора $\boldsymbol{p^{n-1}} < \boldsymbol{a_1} < \boldsymbol{p^n}$ и $\boldsymbol{a_1} = \boldsymbol{db_1} (\mathbf{mod}\, \boldsymbol{M})$ следует, что $\boldsymbol{d}$ должен быть достаточно близок одному из минимумов функции $\boldsymbol{db_1} (\mathbf{mod}\, \boldsymbol{M})$.

Эти минимумы можно искать в виде $\boldsymbol{jM'/b_i}$, где $\boldsymbol{j}$ – номер минимума графика $\boldsymbol{db_i} (\mathbf{mod}\, \boldsymbol{M'})$. Множитель $\boldsymbol{d}$ попадает в пересечение промежутков для различных $\boldsymbol{b_i}$. Так как значение $\boldsymbol{M'}$ не известно, то использование модели, изображенной на рис. 1 сопряжено с трудностями. Шамир предложил заменить $\boldsymbol{M'}$ единицей, ведь интерес представляют точки скопления минимумов для различных $\boldsymbol{i}$. Шамир свел поиск таких точек к системе двойных неравенств:

$$\begin{array}{ll} \boldsymbol{p, q, r, \ldots} \in \mathbb{N}, & \\ -\boldsymbol{\delta_2} \le \boldsymbol{pb_2} - \boldsymbol{qb_1} \le \boldsymbol{\delta_2} & \boldsymbol{1} \le \boldsymbol{p} \le \boldsymbol{b_1} - \boldsymbol{1}, \\ -\boldsymbol{\delta_3} \le \boldsymbol{pb_3} - \boldsymbol{rb_1} \le \boldsymbol{\delta_3} & \boldsymbol{1} \le \boldsymbol{q} \le \boldsymbol{b_2} - \boldsymbol{1}, \\ \ldots & \boldsymbol{1} \le \boldsymbol{r} \le \boldsymbol{b_3} - \boldsymbol{1}, \\ & \ldots \end{array} \qquad (12)$$

Таким образом, поиск значения $\boldsymbol{d}$, задающего обратное модульное умножение, сводится к приближенному решению системы диофантовых уравнений. При решении системы (12) для обеспечения эффективности требуются корректные значения $\boldsymbol{\delta_i}$. Верхнюю границу на значения таких параметров $\boldsymbol{\delta_i}$ в случае стандартных рюкзачных систем были предложены в работе [9]:

Теорема 1.

Для $\boldsymbol{l}$ кривых и $\mathbf{max}_{\boldsymbol{i}=\overline{\boldsymbol{1,l}}}\, \boldsymbol{\delta_i} = \boldsymbol{\delta} \le \sqrt{\boldsymbol{b_1/2}}$ условная вероятность получения не менее чем $\boldsymbol{k}$ точек скопления, при условии наличия всего одной не превосходит:

$$\left(\frac{1}{\lceil k/2 \rceil}\right)^{l-1}. \quad (13)$$

Если количество точек не более чем k, и k имеет порядок n, то сложность атаки останется полиномиальной от n. В противном случае атака признается не эффективной. **Теорема 1** оценивает вероятность неудачи при проведении эффективной атаки по методу Шамира [9].

Как заметил Шамир, полученное обоснование эффективности диофантовой аппроксимации теряет силу, если отношение модуля M и элемента a_1 превосходит **2**. Как следует из **Леммы 2**, для рюкзачных систем нестандартного типа это отношение равно $p > 2$.

Заключение. Таким образом, рассмотрены особенности атак на исследуемые рюкзачные системы защиты информации и выявлены особенности, позволяющие применять известные в литературе атаки. На основе проделанного анализа были уточнены значения параметров для нестандартных РЗСИ, гарантирующих их стойкость. Выявлен набор атак, применимых для нестандартного случая. Среди них выявлена наиболее универсальная – атака типа Шамира, которая использует только открытый ключ. На основе проведенного обзора классических рюкзачных систем в целом и рюкзачных систем на основе нестандартного рюкзака в частности, показано, что подобная техника приближенного решения диофантовых уравнений не приводит к успеху в обобщенном случае, даже при $n \geq 4$ и $p = \log T$, где T – предполагаемое время атаки.

Итак, наряду с системой Шора-Ривеста, в семействе рюкзачных систем защиты информации по праву безопасными являются РСЗИ, основанные на задаче о нестандартном рюкзаке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Саломаа А.* Криптография с открытым ключом. – М.: Мир, 1995.
2. *Шеннон К.* Работы по теории информации и кибернетики. – М. 1963. – 832 с.
3. *Осипян В.О.* О системе защиты информации на основе проблемы рюкзака // Известия Томского политехнического университета. – 2006. – Т. 309, № 2.
4. *Осипян В.О.* Моделирование систем защиты информации содержащих диофантовы трудности. LAP LAMBERT Academic Publishing, 2012.
5. Diffie W., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. – 1976. – Vol. 22. – P. 644-654.
6. *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, № 5. – P. 901-909.
7. *Martello S. T.P.* Knapsack problems : algorithms and computer implementations // Chichester: JOHN WILEY & SONS. – 1990. – P. 137-138.
8. *Merkle R.C., Hellman M.E. Hiding* Information and Signatures in Trapdook Knapsacks. – 1978. – № 24. – P. 525-530.
9. *Shamir A.* A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem // Information Theory, IEEE Transactions. – 1984. – Vol. 30, № 5. – P. 699-704.
10. *Lenstra, Jr. H.W.* Integer Programming with a Fixed Number of Variables // Mathematics of Operations Research. – 1983. – Vol. 8, № 4. – P. 538-548.
11. *Vaudenay S.* Cryptanalysis of the Chor-Rivest cryptosystem // CRYPTO. – 1998. – P. 243-256.
12. *Izu T., Kogure J., Koshiba T., and Shimoyama T.* Low-density attack revisited // Design, Codes and Cryptography. – 2007. – Vol. 43, № 1. – P. 47-59.
13. *Осипян В.О., Спирина С.Г., Арутюнян А.С., Подколзин В.В.* Труды VII Международной конференции "Алгебра и теория чисел: современные проблемы и приложения", посвященной памяти профессора А.А. Карацубы // Моделирование ранцевых криптосистем, содержащих диофантову трудность. – 2010. – Т. 11. – С. 209-216.

14. *Odlyzhko A.O.* Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme // IEEE Transactions on Information Theory. – Jul 1984. – Vol. IT-30, № 4. – P. 594-601.

Статью рекомендовал к опубликованию д.т.н., профессор Р.З. Камалян.

Осипян Валерий Осипович – Кубанский государственный университет; e-mail: rrwo@mail.ru; 350040, г. Краснодар, ул. Ставропольская, 149; тел.: 89184651399; кафедра информационный технологий; д.ф.-м.н.; профессор.

Жук Арсений Сергеевич – e-mail: arseniyzhuck@mail.ru; тел.: 89654620300; аспирант.

Арутюнян Ашот Хоренович – e-mail: ashotax@gmail.com; тел.: 89180319557; аспирант.

Карпенко Юрий Александрович – Адыгейский государственный университет; e-mail: rrwo@mail.ru; 385000, г. Майкоп, ул. Свободы, 233, кв. 71; тел.: 89184651399; аспирант.

Osipyan Valeriy Osipovich –Kuban State University; e-mail: rrwo@mail.ru; 149, Stavropol'skaya street, Krasnodar, 350040, Russia; phone: +79184651399; the department of information technology; dr. of phis.-math. sc.; professor.

Karpenko Yuriy Aleksandrovich – Adyghe State University; e-mail: rrwo@mail.ru; 233 / 71, Svobody street, Maikop, 385000; phone: +79184651399; postgraduate student.

Zhuck Arseniy Sergeevich – mail: arseniyzhuck@mail.ru; phone: +79654620300; postgraduate student.

Arutyunyan Ashot Horenovich – e-mail: ashotax@gmail.com; phone: +79180319557; postgraduate student.

УДК 681.03.245

Л.К. Бабенко, Е.А. Ищукова

ФИНАЛИСТЫ КОНКУРСА SHA-3 И ОСНОВНЫЕ СВЕДЕНИЯ ОБ ИХ АНАЛИЗЕ*

В последние годы в научном мире наблюдается повышенный интерес к проектированию и анализу алгоритмов хэширования. Наряду с анализом уже существующих функций хэширования, предлагаются новые, заявляемые авторами как более надежные. Кроме того, предлагаются новые методы анализа, которые, как правило, рассчитаны на довольно широкий класс алгоритмов хэширования. Подтверждением тому служит конкурс на принятие нового стандарта хэширования SHA-3, недавно завершенный Национальным институтом стандартов и технологий США. В настоящей статье рассматриваются основы построения функций хэширования, которые явились финалистами конкурса SHA-3. Рассматриваются следующие хэш-функции: BLAKE, Skein, JH, Keccak, Grostl. Для каждой функции рассматриваются основные шаги преобразования и составляющие компоненты. Так, в частности, в составе функции хэширования Skein описывается новый блочный алгоритм шифрования Threefish. Также в статье приводятся основные сведения, известные на данный момент, об основных результатах анализа рассматриваемых функций хэширования.

Криптграфия; анализ; функция хэширования; надежность; стойкость; шифр.

* Работа выполнена при поддержке грантов РФФИ №12-07-31120_мол_а, №12-07-33007_мол_а_вед, № 12-07-00037-а.