УДК 519.72 (075.8)

В. В. Подколзин, В. О. Осипян

О СВОЙСТВАХ РЮКЗАЧНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С ОТКРЫТЫМ КЛЮЧОМ В Z_P

Исследуются свойства последовательностей чисел, выражаемых через компоненты рюкзачного вектора. Анализируются свойства изоморфных и подобных рюкзачных систем защиты информации. Приводятся методы увеличения криптостойкости рюкзачных систем защиты информации с открытым ключом.

Ключевые слова: рюкзачный вектор, изоморфизм, криптоанализ, плотность, инъективность.

Обозначим через Z_p множество натуральных чисел $\{0, 1, \ldots, p-1\}$, а через Z_p^n – множество всех числовых наборов длины n с компонентами из Z_p.

Задача о рюкзаке для заданных $w \in N$ и вектора $A = (a_1, a_2, \ldots, a_n)$, где $a_i \in N$, $i = 1\ldots n$, имеет решение в Z_p, если существует решение уравнения

$$Ax^T = w, x \in Z_p^n. \quad (1)$$

Вектор A уравнения (1) будем называть рюкзачным вектором.

Рюкзачный вектор $A = (a_1, a_2, \ldots, a_n)$ – инъективный, если для любого натурального w уравнение (1) имеет не более одного решения. Рюкзачный вектор, у которого существуют два элемента $a_i = a_j$, $i \neq j$ не является инъективным. Инъективность рюкзачного вектора позволяет говорить об однозначности восстановления исходного текста по криптограмме. Самыми простыми с точки зрения понимания и алгоритмизации инъективными рюкзачными векторами являются сверхрастущие рюкзачные векторы, для компонентов которых в Z_p выполняются соотношения

$$a_j > \sum_{i=1}^{j-1}(p-1)a_i, j = 2\ldots n. \quad (2)$$

Рюкзачный вектор $A = (a_1, a_2, \ldots, a_n)$ – является неубывающим, если его компоненты упорядочены по правилу $a_{i-1} \le a_i$, $i = 2\ldots n$. Соответственно, вектор является возрастающим, если его компоненты упорядочены по правилу $a_{i-1} < a_i$, $i = 2n$.

Определение. Вариацией вектора $A = (a_1, a_2, \ldots, a_n)$ $(a_i \in N, i = 1\ldots n)$ в Z_p назовем вектор $\Delta A = (\delta_1, \delta_2, \ldots, \delta_n)$, для компонентов которого выполняются соотношения

$$\delta_1 = a_1, \ \delta_j = a_j - \sum_{i=1}^{j-1}(p-1)a_i, \ j = 2\ldots n. \quad (3)$$

На основе вектора ΔA можно однозначно определить соответствующий ему рюкзачный вектор A в Z_p:

$$a_1 = \delta_1,$$
$$a_i = \delta_i + (p-1)\sum_{j=1}^{i-1} a_j = \delta_i + (p-1)\sum_{j=1}^{i-1} p^{i-j-1}\delta_j,$$
$$i = 2\ldots n. \quad (4)$$

Обозначим через $\mu(p, A)$ множество различных значений w, для которых уравнение (1) имеет решение. Мощность $\mu(p, A)$ не превышает p^n, так как количество различных векторов в Z_p^n равно p^n. Значение $|\mu(p, A)|$ достигает верхней грани, если

$$\forall x_1, x_2 \in Z_p^n \ x_1 \neq x_2 \Rightarrow Ax_1^T \neq Ax_2^T. \quad (5)$$

Таким образом, мощность $\mu(p, A)$ достигает верхней грани, тогда и только тогда вектор A инъективен. Действительно, если вектор A – инъективный, то выполняются соотношения (5) и различных значений Ax^T $(x \in Z_p^n)$ столько, сколько различных элементов в Z_p^n, т. е. p^n. С другой стороны, если $|\mu(p, A)| = p^n$, то существует взаимнооднозначное соответствие между элементами $\mu(p, A)$ и Z_p^n, а следовательно, имеет место единственность решения уравнения (1) для любого $w \in \mu(p, A)$. Из последнего следует инъективность рюкзачного вектора A.

Определение. Величину

$$d_p(A) = \frac{|\mu(p, A)|}{\sum_{i=1}^{n}(p-1)a_i} \quad (6)$$

назовем плотностью рюкзачного вектора A в Z_p.

Плотность определяет отношение мощности $\mu(p, A)$ к длине отрезка $[0, \sum_{i=1}^{n}(p-1)a_i]$. Очевидно, что $\forall x \in Z_p^n$ значение $Ax^T \in [0, \sum_{i=1}^{n}(p-1)a_i]$. Таким образом, $0 < d_p(A) \le 1$. Причем для инъективных рюкзачных векторов плотность равна 1, тогда и только тогда, когда все компоненты вариации вектора A равны единице [1], а криптоанализ таких рюкзачных систем состоит в нахождении p.

Каждому набору $x = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in Z_p^n$ соответствует $w_x = Ax^T$, $w_x \in \mu(p, A)$. Выпишем последовательность $W_{\mu(p, A)} = (w_0, w_1, w_2, \ldots, w_k)$, где $w_i = Ax_i^T, x_i = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $i = \sum_{i=1}^{n}\alpha_i p^{n-i}$, $i = 0\ldots k, k = p^n - 1$. В случае, если вектор A не является инъективным в $W_{\mu(p, A)}$ существуют два значения $w_i = w_j$, $i \neq j$. Обозначим последовательность $\Delta W_{\mu(p, A)} = (m_1, m_2, \ldots, m_k)$, где $m_i = w_i - w_{i-1}$ $(i = 1\ldots p^n - 1)$.

Последовательность $\Delta W_{\mu(p, A)}$ является симметричной относительно середины и может быть определена рекурсивно относительно размерности рюкзачного вектора A.

Пусть $A_n = (a_1, a_2, \ldots, a_n)$ $(a_i \in N, i = 1\ldots n)$ – рюкзачный вектор. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ получен из A_n добавлением компонента $a_{n+1} \in N$. Тогда

$$\Delta W_{\mu(p, An+1)} = (W_{\mu(p, An)}, \delta_{n+1}, \Delta W_{\mu(p, An)}, \delta_{n+1}, \Delta W_{\mu(p, An)}, \ldots, \delta_{n+1}, \Delta W_{\mu(p, An)}),$$

где $\delta_{n+1}, \Delta W_{\mu(p, An)}$ повторяется p–1 раз.

Последовательность $\Delta W_{\mu(p, A)}$ описывает расстояния между элементами последовательности $W_{\mu(p, A)}$, т. е. ее «разреженность», а следовательно, является характеристикой $\mu(p, A)$.

Из симметричности $\Delta W_{\mu(p, A)}$ следует, что любой $w \in W_{\mu(p, A)}$ может быть представлен двумя способами

$$w = \sum_{j=1}^{n}\alpha_j\alpha_j = \sum_{k=1}^{n}(p-1)\alpha_k - \sum_{i=1}^{n}\beta_i\alpha_i,$$

где $\alpha_i, \beta_i \in Z_p$, $i = 1 \ldots n$. (7)

Лемма 1. $A_n = (a_1, a_2, \ldots, a_n)$ – инъективный рюкзачный вектор, где $a_i \in N$, $I = 1 \ldots n$. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ получен из A_n добавлением компонента $a_{n+1} \in N$, $\Delta A_{n+1} = (\delta_1, \delta_2, \ldots, \delta_n, \delta_{n+1})$ – вариация вектора A_{n+1} и $\delta_{n+1} > 0$. Тогда $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ – инъективный рюкзачный вектор.

Доказательство. Покажем, что $\forall\ w_x \in \mu(p, A_{n+1})$ уравнение (1) имеет единственное решение.

Из принадлежности w_x множеству $\mu(p, A_{n+1})$ следует, что $\exists x = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}) \in Z_p^{n+1}$, для которого выполняется $w_x = A_{n+1} x^T$.

1. Если $\alpha_{n+1} = 0$, то $w_x \in \mu(p, A_n)$, тогда (1) имеет единственное решение в силу инъективности A_n.

2. Пусть $0 < \alpha_{n+1} < p$. Так как $\delta_{n+1} > 0$, то любой элемент $\mu(p, A_n)$ меньше a_{n+1}. Таким образом, существуют единственные α_{n+1} и $w'_x \in \mu(p, A_n)$ такие, что $w_x = \alpha_{n+1} a_{n+1} + w'_x$, а следовательно, уравнение (1) имеет единственное решение.

Из произвольности $w_x \in \mu(p, A_{n+1})$ следует, что A_{n+1} является инъективным рюкзачным вектором.

Лемма 2. $A_n = (a_1, a_2, \ldots, a_n)$ – инъективный возрастающий рюкзачный вектор, где $a_i \in N$, $i = 1 \ldots n$. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ получен из A_n добавлением компонента $a_{n+1} \in N$, $A_{n+1} = (\delta_1, \delta_2, \ldots, \delta_n, \delta_{n+1})$ – вариация вектора A_{n+1} и $\delta_{n+1} < 0$.

Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ является инъективным возрастающим рюкзачным, если выполняется

$$(a_n - \sum_{j=1}^{n} (p-1) a_j < \delta_{n+1}) \ \&\ (|\delta_{n+1}| \notin W_{\mu(2p-1,\, An)}).$$

Доказательство. Прежде всего определим условие, при котором A_{n+1} будет возрастающим. Так как A_n – возрастающий вектор, то необходимо выполнение условия

$$a_n < a_{n+1} = \sum_{j=1}^{n} (p-1) a_j + \delta_{n+1}.$$

Следовательно

$$a_n - \sum_{j=1}^{n} (p-1) a_j < \delta_{n+1}.$$

Пусть $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ является возрастающим, но не является инъективным вектором, т. е. существует $\omega_x \in \mu(p, A_{n+1})$, т. е. уравнение (1) имеет не единственное решение. Из инъективности A_n и свойств последовательностей $W_{\mu(p,\, An)}$ и $W_{\mu(p,\, An+1)}$ следует, что все такие ω_x принадлежат отрезкам $[a_{n+1} + k\ a_{n+1},\ \sum_{j=1}^{n} (p-1) a_j + k\ a_{n+1}]$, где $k = 0 \ldots p-2$.

Также если

$$a_{n+1} = \sum_{j=1}^{n} (p-1) a_j + \delta_{n+1} \le \omega_x \le \sum_{j=1}^{n} (p-1) a_j \qquad (8)$$

и для ω_x уравнение (1) имеет более одного решения, то для $\omega_x + k\, a_{n+1}$, где $k = 0 \ldots p-2$, уравнение (1) также имеет более одного решения, и наоборот.

На основании вышеизложенного рассмотрим ω_x, удовлетворяющее (8), тогда $\omega_x \in \mu(p, A_n)$ и $\omega_x \in \mu(p, A_{n+1})$.

Из принадлежности ω_x множеству $\mu(p, A_{n+1})$ имеем следующее

$$\omega_x = a_{n+1} + \sum_{j=1}^{n} \beta_j a_j = \left(\sum_{k=1}^{n} (p-1) a_k + \delta_{n+1} \right) + \sum_{j=1}^{n} \beta_j a_j,$$

где $\beta_i \in Z_p$, $I = 1 \ldots n$, $0 < \alpha < p-1$.

Из принадлежности ω_x множеству $\mu(p, A_n)$ и справедливости (7) имеем

$$\omega_x = \sum_{j=1}^{n} \gamma_j a_j = \sum_{k=1}^{n} (p-1) a_k - \sum_{j=1}^{n} \varphi_j a_j, \text{ где } \gamma_i, \varphi_i \in Z_p,\ i = 1 \ldots n.$$

Таким образом, имеет место равенство

$$\sum_{k=1}^{n} (p-1) a_k - \sum_{j=1}^{n} \varphi_j a_j = \sum_{k=1}^{n} (p-1) a_k + \delta_{n+1} + \sum_{j=1}^{n} \beta_j a_j -$$

$$- \delta_{n+1} = \sum_{j=1}^{n} (\beta_j + \varphi_j) a_j.$$

Из последнего равенства следует $-\delta_{n+1} \in W_{\mu(2p-1,\, An)}$. Следовательно, для инъективности A_{n+1} необходимо $|\delta_{n+1}| \notin W_{\mu(2p-1,\, An)}$.

На множестве $\mu(p, A)$ рюкзачного вектора $A = (a_1, a_2, \ldots, a_n)$ определим операцию сложения $\oplus$ следующим образом:

$$\forall w_1, w_2 \in \mu(p, A)\ w = w_1 \oplus w_2 =$$

$$= \sum_{i=1}^{n} \alpha_i a_i \oplus \sum_{i=1}^{n} \beta_i a_i = \sum_{i=1}^{n} \gamma_i a_i, \qquad (9)$$

где $\gamma_i = (\alpha_i + \beta_i) \bmod p$; $\alpha_i, \beta_i \in Z_p$, $i = 1 \ldots n$.

Множество $\mu(p, A)$ с операцией сложения $\oplus$ образует аддитивную конечную абелевую группу $(\mu(p, A), \oplus)$.

Определение. Два рюкзачных вектора $A = (a_1, a_2, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_k)$ – векторы вариаций ΔA и ΔB которых отличаются только значением первого компонента, являются изоморфными, будем обозначать $A \approx B$, если существует изоморфизм f: $\mu(p, A) \to \mu(p, B)$.

Два рюкзачных вектора могут быть изоморфными только тогда, когда они имеют одинаковую размерность и $|\mu(p, A)| = |\mu(p, B)|$.

Рассмотрим два изоморфных рюкзачных вектора $A = (a_1, a_2, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_k)$. Из (4) имеем

$$a_1 = \delta_1,\ a_i = \delta_i + (p-1) \sum_{j=1}^{i-1} p^{i-j-1} \delta_j,$$

$$b_1 = \delta'_1,\ b_i = \delta_i + (p-1) \left(p^{i-2} \delta'_1 + \sum_{j=2}^{i-1} p^{i-j-1} \delta_j \right),\ i = 2 \ldots n.$$

Назовем коэффициентом изоморфизма двух векторов A и B значение $\varepsilon(A, B) = \delta'_1 - \delta_1$.

Тогда

$$b_1 = \delta_1 + \varepsilon,\ b_i = \delta_i + (p-1) \left(p^{i-2} \varepsilon + \sum_{j=1}^{i-1} p^{i-j-1} \delta_j \right),$$

$$b_1 = a_1 + \varepsilon,\ b_i = a_i + (p-1) p^{i-2} \varepsilon,\ i = 2 \ldots n,\ \varepsilon = \varepsilon(A, B) \qquad (10)$$

и справедливо соотношение

$$\sum_{i=1}^{j-1} (p-1) b_i = (p-1)(a_1 + \varepsilon) + \sum_{i=2}^{j-1} (p-1)(a_i + (p-1) p^{i-2} \varepsilon) =$$

$$\sum_{i=1}^{j-1} (p-1) a_i + (p-1) \varepsilon (1 + \sum_{i=2}^{j-1} p^{i-2}) =$$

$$= \sum_{i=1}^{j-1} (p-1) a_i + (p-1) \varepsilon p^{j-2}. \qquad (11)$$

На основании свойств последовательностей $W_{\mu(p,\, A)}$ и $W_{\mu(p,\, B)}$ можно сделать вывод, что $W_{\mu(p,\, B)}$ получается из $W_{\mu(p,\, A)}$ «рекурсивным масштабированием» на ε относительно «узловых» значений $(a_2, \ldots, a_n)$, а каждое значение a_i

смещается согласно (10). А последовательность $\Delta W_{\mu(p,B)}$ получается из $\Delta W_{\mu(p,A)}$ заменой всех вхождений δ_1 на $\delta_1+\varepsilon$.

Если для рюкзачных векторов $A=(a_1, a_2, \ldots, a_n)$, $B=(b_1, b_2, \ldots, b_n)$ и $C=(c_1, c_2, \ldots, c_n)$ выполняется $A \approx B$ и $B \approx C$, то $A \approx C$. Действительно, в силу биекции f: $\mu(p, A)\to\mu(p, B)$ и g:$\mu(p, B)\to\mu(p, C)$ следует, что $h = g°f$: $\mu(p, A)\to \mu(p, C)$ – биективна и $\varepsilon(A, C) = \varepsilon(A, B) + \varepsilon(B, C)$.

Изоморфизм рюкзачных векторов является отношением эквивалентности, а следовательно, множество изоморфных векторов образует класс эквивалентности. В каждом классе существует вектор, для которого коэффициент изоморфизма с любым другим вектором этого класса неотрицательный; назовем такой вектор базовым вектором класса эквивалентности.

Пусть $\Theta=(\theta_1, \theta_2, \ldots, \theta_n)$ – базовый вектор некоторого класса эквивалентности и $A=(a_1, a_2, \ldots, a_n)$ – произвольный элемент этого же класса, т. е. $\Theta \approx A$, $\varepsilon(\Theta, A) > 0$. Так как $|\mu(p, A)| = |\mu(p, \Theta)|$, то из определения плотности рюкзачного вектора в Z_p имеем следующее:

$$|\mu(p, A)| = d_p(A)\sum_{i=1}^{n}(p-1)a_i = d_p(\Theta)\sum_{i=1}^{n}(p-1)\theta_i = |\mu(p, \Theta)|.$$

В силу (11) выполняется следующее:

$$d_p(A)\sum_{i=1}^{n}(p-1)a_i = d_p(A)\left(\sum_{i=1}^{n}(p-1)\theta_i + \varepsilon(p-1)p^{n-2}\right) =$$

$$= d_p(\Theta)\sum_{i=1}^{n}(p-1)\theta_i.$$

Из последнего выразим $d_p(\Theta)$:

$$d_p(\Theta) = d(A)\left(1+\frac{\varepsilon p^{n-2}}{\sum_{i=1}^{n}\theta_i}\right), \text{ здесь } \varepsilon = \varepsilon(\Theta, A);$$

$$d_p(\Theta) = d_p(A))1 + k\,\varepsilon(\Theta, A)), \text{ где } k = \frac{p^{n-2}}{\sum_{i=1}^{n}\theta_i} = \text{cont.} \quad (12)$$

Таким образом, базовый вектор имеет наибольшую плотность среди всех векторов его класса эквивалентности.

В случае если базовый вектор Θ является сверхрастущим, то вектор A также является сверхрастущим. Действительно, из (2) и (10) имеем

$$\sum_{i=1}^{j-1}(p-1)a_i = (p-1)(\theta_1+\varepsilon) +$$

$$+\sum_{i=2}^{j-1}(p-1)(\theta_i + (p-1)p^{i-2}\varepsilon) =$$

$$= \sum_{i=1}^{j-1}(p-1)\theta_i + (p-1)\varepsilon(1+\sum_{i=2}^{j-1}p^{i-2}) <$$

$$< \theta_j + (p-1)\varepsilon p^{j-2} = a_j,\ \varepsilon = \varepsilon(\Theta, A).$$

Из последнего неравенства следует, что для любого класса эквивалентности с базовым сверхрастущим вектором существует рюкзачный вектор из данного класса для любого положительного коэффициента изоморфизма. В общем случае данное утверждение неверно. Например, для инъективного вектора (15, 42, 51, 83) не существует изоморфного вектора в Z_2 с коэффициентом изоморфизма равным 10, так как вектор (25, 52, 71, 123) не является инъективным.

Таким образом, РСЗИ с рюкзачным вектором A, можно преобразовать к эквивалентной РСЗИ с рюкзачным вектором Θ, где Θ – базовый вектор класса эквивалентности вектора A. Целесообразность данного преобразования обусловливается меньшим объемом вычислений (p, Θ) и затрат памяти. Например, для хранения каждого элемента $\mu(2, A)$ сверхрастущего рюкзачного вектора $A=(45, 69, 218, 415, 796, 1752, 3588, 7375, 17897, 36073)$ необходимо 17 бит памяти, а для хранения соответствующих значений базового вектора $\Theta=(1, 25, 130, 239, 444, 1048, 2180, 4559, 12265, 24809)$ достаточно выделить по 16 бит. При больших значениях компонентов рюкзачного вектора и соответствующей размерности, объем памяти требуемой для хранения элементов $\mu(p, A)$ может превысить размеры стандартных типов языков программирования, а следовательно, потребует дополнительных процедур по хранению и выполнению операций над такими «большими» числами, что, естественно, влечет увеличение затрат по времени и памяти. В частности, для вышеуказанного примера, для хранения значений $\mu(2, B)$ сверхрастущего вектора $B=(444444444, 444444468, 888889016, 1777778011, 3555555988, 7111112136, 14222224356, 28444448911, 56888900969, 11377780227)$, принадлежащему этому же классу эквивалентности необходимо выделять уже по 38 бит.

Теорема. Пусть $A=(a_1, a_2, \ldots, a_n)$ – инъективный рюкзачный вектор размерности n и $t \neq 0$ – целое число. Тогда не существует инъективного рюкзачного вектора размерности n, посредством компонентов которого в Z_p выражаются все элементы множества $\{w + t|w \in \mu(p, A)\}$.

Доказательство. Предположим, что существует инъективный рюкзачный вектор $B = (b_1, b_2, \ldots, b_n)$, т. е. $\{w + t|w \in \mu(p, A)\} \subseteq \mu(p, B)$:

1. $t > 0$. Тогда $|\mu(p, B)|i|\mu(p, A)| + 1$, так как ноль входит в $\mu(p, B)$, но не входит в $\{w + t \mid w \in \mu(p, A)\}$. Но в силу инъективности векторов A и B выполняется $|\mu(p, B)| = |\mu(p, A)|$. Противоречие.

2. $t < 0$. Так как $0 \in \mu(p, A)$, то $t \in \mu(p, B)$, что противоречит $b_i \in N$, $i = 1, \ldots, n$.

Таким образом, модификация РСЗИ путем изменения числового значение криптотекста на некоторую величину приводит к увеличению сложности ее криптоанализа.

Определение. Два рюкзачных вектора $A = (a_1, a_2, \ldots, a_n)$ и $B =(b_1, b_2, \ldots, b_n)$ подобны, будем обозначать $A \cong B$, тогда и только тогда, когда существует взаимно однозначное отображение f: $A\to B$ такое, что:

1) $\forall a \in A\, f(Ca) = Cf(a)$, где $C \in Z$;

2) $\forall a', a'' \in A$ выполняется $f(a' + a') = f(a') + f(a'')$.

Примером двух подобных рюкзачных векторов могут служить два вектора, один из которых получен из другого сильным модульным умножением.

Исследуем свойства двух подобных инъективных рюкзачных векторов $A = (a_1, a_2, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_n)$, отображение которых определяется функцией $f(x) = cx$ в некотором поле, где c – некоторая константа:

$$F(a_i) = ca_i = b_i,\ i = 1\ldots n,$$

$$\forall w_a \in \mu(p, A)\, f(w_a) = f(\sum_{i=1}^{n}\alpha_i a_i) =$$

$$= \sum_{i=1}^{n}\alpha_i f(a_i) = \sum_{i=1}^{n}\alpha_i(ca_i) = \sum_{i=1}^{n}\alpha_i b_i.$$

Плотности таких векторов связаны соотношением

$$d_p(B)=\frac{\left|\mu_p(B)\right|}{\sum_{i=1}^{n}(p-1)b_i}=\frac{\left|\mu_p(A)\right|}{\sum_{i=1}^{n}(p-1)ca_i}=\frac{\left|\mu_p(A)\right|}{c\left(\sum_{i=1}^{n}(p-1)a_i\right)},$$

$$d_p(A)=cd_p(B). \quad (13)$$

Последовательности $W_{\mu(p,A)}$ и $W_{\mu(p,B)}$ обладают свойствами, определенными соотношением (10). Элементы последовательностей $\Delta W_{\mu(p,A)}$ и $\Delta W_{\mu(p,B)}$ связаны следующим образом:

$m_i = ch_i$, $i = 1...n$, где $m_i \in \Delta W_{\mu(p,B)}$, $h_i \in \Delta W_{\mu(p,A)}$.

Наиболее известные системы защиты информации с открытым ключом и с рюкзаком на основе секретного ключа [2], в которой в качестве открытого ключа используется вектор, полученный из рюкзачного вектора сильным модульным умножением на значения секретного ключа. Криптоанализ таких систем возможен аналитическими или статистическими методами либо посредством анализа открытого ключа.

Аналитические методы основаны на методах решений уравнения (1) на основе известных значений из $\mu(p, A)$. Применимость данных методов основана на объемах проводимых вычислений. Верхняя граница числа решений (1) приведена в [3] и в общем случае является NP-полной задачей.

Статистические методы основаны на статистических характеристиках элементов естественного языка или другого языка исходного текста и статистике элементов криптотекста. Основной целью таких методов является не нахождение рюкзачного вектора, а нахождение взаимно однозначного соответствия между элементами исходного и шифрованного текста. Они применимы только при наличии статистических объемов криптотекстов.

Методы криптоанализа открытого ключа заключаются в восстановлении рюкзачного вектора РСЗИ по вектору открытого ключа. В частности, для двух сверхрастущих рюкзачных векторов, полученных один из другого посредством сильного модульного умножения, А. Шамиром предложен алгоритм нахождения рюкзачного вектора A РСЗИ, если известен вектор B [2].

На основе вышеописанных свойств рюкзачных векторов можно сформулировать следующие выводы:

– криптоанализ РСЗИ можно проводить не только на основе статистики значений элементов криптотекстов, но и на распределении значений. В силу того, что вероятность появлений последовательностей элементов $\Delta W_{\mu(p,A)}$ рюкзачного вектора $A = (a_1, a_2, \ldots, a_n)$ в Z_p есть величина постоянная для заданной размерности n, то таблица вероятностей рассчитывается на этапе предварительной подготовки криптоанализа. Анализ криптотекстов проводится на основе разностей между парами значений его элементов. В этом случае существенным является не объем известных криптотекстов, а количество различных значений его элементов. Построение инъективного рюкзачного вектора базируется на основе свойств $W_{\mu(p,A)}$ и Лемме 1;

– применимость статистических методов анализа криптотекстов базируется на его объеме. Поэтому при малых объемах такой информации данные методы практически не применимы. Модификация РСЗИ с одним рюкзачным вектором в систему с динамически генерируемыми рюкзачными векторами [4; 5] приводит к практической неприменимости статистических методов анализа криптотекстов;

– для повышения криптостойкости классических систем защиты информации с открытым ключом и с рюкзаком необходимо использовать неизоморфные и неподобные рюкзачные векторы, а также изменять значения выходов блока шифрования РСЗИ на значение некоторой константы. Например, видоизменив классическую систему защиты информации с открытым ключом и с рюкзаком на основе секретного ключа (m, t) [2], можно существенно повысить криптостойкость системы.

Рассмотрим простой пример. Пусть $A = (2, 5, 6)$ – инъективный возрастающий рюкзачный вектор, перед определением открытого ключа – вектора B, применим функцию $f(x) = x^2 - x$ к элементам вектора A и, учитывая, что $f(2) = 2, f(5) = 20, f(6) = 30$, получим $A' = (2, 20, 30)$. Используя пару $m = 220$ и $t = 17$ как секретный ключ [1],сильным модульным умножением [1] получим открытый ключ $B = (34, 120, 70)$. Криптоанализ вектора B согласно алгоритма А. Шамира может привести только к получению сверхрастущего вектора A' [2], в котором шифротекст $w = 7$ недопустим. Таким образом, использование в качестве секретного ключа $(m, t, f(x))$ приводит к тому, что известные методы анализа системы защиты информации с открытым ключом, в частности, использующие сильное модульное умножение, не применимы или требуют дополнительных затрат по поиску преобразования $f(x)$.

Библиографические ссылки

1. Осипян В. О. Разработка методов построения систем передачи и защиты информации. Краснодар, 2004.

2. Саломаа А. Криптография с открытым ключом. М. : Мир, 1995.

3. Подколзин В. В., Осипян В. О. Верхняя граница числа решений обобщенной задачи о рюкзаке на заданном входе // Актуальные проблемы безопасности информационных технологий : материалы III Междунар. науч.-практ. конф. / под общей ред. О. Н. Жданова, В. В. Золотарева ; Сиб. гос. аэрокосмич. ун-т. Красноярск, 2009. С. 30–33.

4. Подколзин В. В. Модель системы защиты информации с открытым ключом на основе динамической генерации рюкзачного вектора. М. : ОПиПМ, 2009. Т. 16. Вып. 5. С. 913–914.

5. Подколзин В. В., Осипян В. О. Об одной модификации задачи защиты информации с открытым ключом на основе обобщенного рюкзака входе. М. : ОПиПМ, 2009. Т. 16. Вып. 5. С. 905.

V. V. Podkolzin, V. O. Osipyan

ABOUT PROPERTIES OF KNAPSACK SYSTEMS OF INFORMATION PROTECTION WITH THE PUBLIC KEY IN Z_P

Properties of sequences of numbers expressed through components of a knapsack vector are investigated. Properties of isomorphic and similar knapsack systems of protection of the information are analyzed. Methods of increase of cryptographic complexity of knapsack systems of information protection with public key are given.

Keywords: knapsack vector, isomorphism, crypto analysis, density, injectivity

УДК 587/588:630.52

И. М. Данилин, А. И. Данилин, Д. А. Свищев

ЛАЗЕРНАЯ ЛОКАЦИЯ И ЦИФРОВАЯ АЭРОСЪЕМКА – ПОДСПУТНИКОВЫЙ КОМПОНЕНТ В СИСТЕМЕ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНВЕНТАРИЗАЦИИ, МОНИТОРИНГА И КАДАСТРА ЛЕСНЫХ ЗЕМЕЛЬ

Обсуждаются подходы и решения в области дистанционного зондирования лесов для целей информационного обеспечения инвентаризации, мониторинга и кадастра лесных земель, с использованием инновационных методов и технологий высокого уровня – лазерной локации, цифровой аэросъемки и спутникового позиционирования.

Ключевые слова: лазерная локация, цифровая аэросъемка, спутниковое позиционирование, инвентаризация, мониторинг, кадастр лесных земель.

В современной практике лесопользования, мониторинга и кадастра получение достоверной и оперативной информации о состоянии и динамике лесных земель является актуальной задачей как с природоресурсной, так и с экологической, природоохранной точек зрения. В решении этой задачи в последние годы во многих странах мира и в России все активнее используется лазерная локация и цифровая аэросъемка, которые представляют собой важнейшую составляющую геоматики – нового интегрального направления развития методов дистанционного зондирования Земли (аэро- и космической съемки), геоинформационных технологий, цифровой фотограмметрии и картографирования, спутникового геопозиционирования и телекоммуникаций. Эти передовые и высокоэффективные методы находят сегодня широкое применение во многих отраслях, являясь, по сути, информационной основой кадастров природных ресурсов, земле- и лесоустройства, экологического мониторинга, систем сбора, обработки, анализа данных и баз знаний, по показателям точности и экономической эффективности превосходят другие методы изучения и измерения параметров земной поверхности и природных систем [1–7].

Современные авиационные лазерно-локационные системы стремительно развиваются и на сегодняшний день имеют частоту сканирования более 200 тыс. импульсов (измерений) в секунду (рис. 1).

Наибольшая плотность точек сканирования при этом составляет 1 точка на 5–7 см поверхности, а точность измерения геометрических параметров наземных объектов и морфоструктурных элементов растительности в плановой и профильной проекциях составляют порядка ±5…10 см. Точность спутникового позиционирования контуров линий и границ лесных выделов, пробных площадей, отдельных деревьев и морфоструктурных элементов их стволов и крон, в том числе и в подкроновом пространстве, практически не ограничена и определяется техническими характеристиками приборов геопозиционирования [1; 4].

Средствами пространственного и детального отображения контуров и рельефа земной поверхности с представленной на них растительностью и основой для предварительного трассирования маршрутов авиационной лазерной и цифровой аэрофотосъемки могут также являться спутниковые снимки, получаемые в современных оптико-электронных системах Landsat, Ресурс-ДК, Ikonos, OrbView-3, WorldView-2, GeoEye-1 и/или других системах высокого и сверхвысокого разрешения и дешифрированные по основным параметрам и характеристикам растительного покрова [5].

Вместе с тем, структура, объемные показатели деревьев и древостоев, их фитомасса наиболее достоверно и точно определяются по лазерно-локационным данным («лазерным портретам»), интегрированным с цифровыми геотрансформированными аэрофотоснимками на основе цифровой модели местности (ЦММ) и поля распределения лесного полога, которые генерируются из исходных данных лазерной локации способом фильтрации импульсов локатора, отраженных от земной поверх-