References

1. Mathematical simulation of reaches of the Krasnoyarsk impoundment / V. A. Sapozhnikov [et al.] // Association of subjects of the Russian Federation and a wildlife management problem in Prienisejsky Siberia : theses and materials of reports of inter-regional scientifically-practical conference / KSU. Krasnoyarsk, 2005. P. 296–298.

2. Borodin, A. L., Raspopov V. E. Numerical identification of coefficients of mathematical model of an ecosystem of a reservoir // Joint issue. Computing technologies. T. 13. Herald of the KazSU of AL-FARABI. A series of the mathematics, the mechanics, the informatics. Vol. 3 (58). Almaty–Novosibirsk, 2008. P. 302–306.

3. Gubanov V. G. Biotic circulation and interaction of trophic links in artificial and natural biosystems : diss. dr. phys.-math. sciences. Krasnoyarsk, 2004.

4. Petrov J. S. Special-purpose software for carrying out of computing experiments at mathematical modeling of water ecosystems // YOUTH AND THE SCIENCE: the XXI-st century BEGINNING : Materials of the All-Russia scientific and technical conf. of students, post-graduate students and young scientists. In 4 p. P. 1 / SFU. Krasnoyarsk, 2009. P. 78–80.

5. Kozhevnikova N. A., Phytoplankton of a deep-water part of a Krasnoyarsk impoundment // Alkologia. № 2. 2002. P. 39–40.

6. ShChur L. A. Structure and functional characteristics of bacterial plankton and phytoplankton in ecosystems of reservoirs of different type : diss. dr. biol. sciences. Krasnoyarsk, 2006.

7. Belolipetsky V. M., Genova S. N., Gurevich K. J. Platform for research of dynamics of hydrophysical and radio ecological characteristics of river system // Computing technologies / the Siberian Branch of the Russian Academy of Science. Vol. 6, № 2. 2001. P. 14–24.

V. V. Podkolzin, V. O. Osipyan
Kuban State University, Russia, Krasnodar

ON PROPERTIES OF KNAPSACK SYSTEMS OF INFORMATION PROTECTION WITH THE OPEN 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 information protection are analyzed. Methods of increasing cryptographic security of knapsack systems of information protection with an open key are presented.

Keywords: a knapsack vector, isomorphism, cryptoanalysis, density, injectivity.

Let's express a set of natural numbers {0, 1, …, p–1} through Z_p and a set of all numerical sets of length n with components from Z_p. through Z_p^n .

A knapsack problem for set $w \in N$ and vector $A = (a_1, a_2, ..., a_n)$, where $a_i \in N$, $I = 1…n$, has the solution in Z_p if there is an equation solution

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

we will call vector A of equations (1) a knapsack vector.

A knapsack vector $A = (a_1, a_2, ..., a_n)$ is an injective one if for any natural w the equation (1) has not more than one solution. A knapsack vector which has two elements $a_i = a_j$, $I \neq j$, is not injective. Injectivity of a knapsack vector allows to speak about uniqueness of restoration of the original text according to the cryptogram. Supergrowing knapsack vectors are the simplest injective knapsack vectors from the point of view of understanding and algorithmization. For their components in Z_p the following relationships are carried out:

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

A knapsack vector $A = (a_1, a_2, ..., a_n)$ is a nondecreasing one if its components are ordered according to the rule $a_{i-1} \le a_i$, $I = 2…n$. Accordingly, the vector is increasing if its components are ordered according to the rule $a_{i-1} < a_i$, $I = 2…n$.

Definition. Let's call vector $\Delta A = (\delta_1, \delta_2, ..., \delta_n)$ a variation of vector $A = (a_1, a_2, ..., a_n)$ ($a_i \in N$, $I = 1…n$) in Z_p, For its components the following correlations are carried out:

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

On the basis of vector ΔA it is possible to define a knapsack vector A in Z_p corresponding to it:

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

Let's express a set of various values w for which equation (1) has the solution through $\mu(p, A)$. Capacity $\mu(p, A)$ does not exceed p^n since the quantity of various

vectors in Z_p^n is equal to p^n. Value $|\mu(p, A)|$ reaches the upper boundary, if

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

Thus, capacity $\mu(p, A)$ reaches the upper boundary only when vector A is injective. Really, if vector A is injective, then correlations (5) are carried out and the number of various values $Ax^T (x \in Z_p^n)$ is equal to the number of various elements in Z_p^n, i. e. p^n. On the other hand, if $|\mu(p, A)| = p^n$, then there is a one-to-one depentanizer between elements $\mu(p, A)$ and Z_p^n, and hence equation (1) for any $w \in \mu(p, A)$ has only one solution. From the latter follows an injectivity of knapsack vector A.

Definition. Let's call the value

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

density of a knapsack vector A in Z_p.

The density defines the relation of capacity $\mu(p, A)$ to the length of a cut $[0, \sum_{i=1}^{n}(p-1)a_i]$. It is obvious that $\forall x \in Z_p^n$ is a value $Ax^T \in [0, \sum_{i=1}^{n}(p-1)a_i]$. Thus, $0 < d_p(A) \le 1$. Moreover for injective knapsack vectors the density is equal to 1 only when all components of a variation of vector A are equal to unit [1], and cryptoanalysis of such knapsack systems consists in finding p.

$W_x = Ax^T$, $w_x \in \mu(p, A)$ corresponds to each set $x = (\alpha_1, \alpha_2, ..., \alpha_n) \in Z_p^n$. We will write out the sequence $W_{\mu(p, A)} = (w_0, w_1, w_2, ..., w_k)$, where $w_i = Ax_i^T$, $x_i = (\alpha_1, \alpha_2, ..., \alpha_n)$, $i = \sum_{i=1}^{n}\alpha_i p^{n-i}$, $I = 1 \ldots k$, $k = p^n - 1$. If vector A is not injective in $W_{\mu(p, A)}$ there are two values $w_i = w_j$, $I \neq j$. We will designate sequence $\Delta W_{\mu(p, A)} = (m_1, m_2, ..., m_k)$, where $m_i = w_i - w_{i-1}$ $(I = 1 \ldots p^n - 1)$.

The sequence $\Delta W_{\mu(p, A)}$ is symmetric with respect to the middle and can be defined recursively relative to the dimension of a knapsack vector A.

Let $A_n = (a_1, a_2, ..., a_n)$ $(a_i \in N, I = 1 \ldots n)$ be a knapsack vector. Vector $A_{n+1} = (a_1, a_2, ..., a_n, a_{n+1})$ is received from A_n by adding the component $a_{n+1} \in N$. Then

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

where $\delta_{n+1}, \Delta W_{\mu(p, An)}$ is repeated $p-1$ times.

The sequence $\Delta W_{\mu(p, A)}$ describes distances between the elements of sequence $W_{\mu(p, A)}$, i. e. its "sparseness", and, hence, is the characteristic of $\mu(p, A)$.

From symmetry $\Delta W_{\mu(p, A)}$ it follows that any $w \in W_{\mu(p, A)}$ can be presented in two ways:

$$w = \sum_{j=1}^{n}\alpha_j a_j = \sum_{k=1}^{n}(p-1)a_k - \sum_{i=1}^{n}\beta_i a_i, \quad (7)$$

where $\alpha_i, \beta_i \in Z_p$, $I = 1 \ldots n$.

Lemma 1. $A_n = (a_1, a_2, ..., a_n)$ is an injective knapsack vector, where $a_i \in N$, $I = 1 \ldots n$. A vector $A_{n+1} = (a_1, a_2, ..., a_n, a_{n+1})$ is received from A_n by adding the component $a_{n+1} \in N$, $\Delta A_{n+1} = (\delta_1, \delta_2, ..., \delta_n, \delta_{n+1})$ is a variation of vector A_{n+1} and $\delta_{n+1} > 0$. Then $A_{n+1} = (a_1, a_2, ..., a_n, a_{n+1})$ is an injective knapsack vector.

The proof.

Let's show that $\forall w_x \in \mu(p, A_{n+1})$ equation (1) has only one solution.

As w_x belongs to set $\mu(p, A_{n+1})$ it follows that $\exists x = (\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}) \in Z_p^{n+1}$ for which $w_x = A_{n+1}x^T$ is carried out.

1. If $\alpha_{n+1} = 0$, then $w_x \in \mu(p, A_n)$ and (1) has the only solution because of injectivity of A_n;

2. Let $0 < \alpha_{n+1} < p$. As $\delta_{n+1} > 0$ then any element $\mu(p, A_n)$ is less than a_{n+1}. Thus, if there is unique α_{n+1} and $w'_x \in \mu(p, A_n)$ then $w_x = \alpha_{n+1}a_{n+1} + w'_x$ and consequently equation (1) has the only solution.

From randomness $w_x \in \mu(p, A_{n+1})$ it follows that A_{n+1} is an injective knapsack vector.

Lemma 2. $A_n = (a_1, a_2, ..., a_n)$ is an injective increasing knapsack vector, where $a_i \in N$, $I = 1 \ldots n$. Vector $A_{n+1} = (a_1, a_2, ..., a_n, a_{n+1})$ is received from A_n by adding the component $a_{n+1} \in N$, $\Delta A_{n+1} = (\delta_1, \delta_2, ..., \delta_n, \delta_{n+1})$ is a variation of vector A_{n+1} and $\delta_{n+1} < 0$.

Vector $A_{n+1} = (a_1, a_2, ..., a_n, a_{n+1})$ is an injective increasing knapsack vector if the following equation is carried out:

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

The proof.

First of all we will define a condition at which A_{n+1} will be increasing. Since A_n is an increasing vector, it is necessary to follow the condition

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

Hence

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

Let $A_{n+1} = (a_1, a_2, ..., a_n, a_{n+1})$ be increasing, but not injective, i. e. let there exist $\omega_x \in \mu(p, A_{n+1})$, then the equation (1) does not have only one solution. From the injectivity of A_n and properties of sequences $W_{\mu(p, An)}$ and $W_{\mu(p, An+1)}$ it follows that all such ω_x belong to cuts $[a_{n+1} + k\,a_{n+1}, \sum_{j=1}^{n}(p-1)a_j + k\,a_{n+1}]$, where $k = 0 \ldots p-2$.

Also, if

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

and equation (1) has more than one solution for ω_x, then the equation (1) also has more than one solution for $\omega_x + k\,a_{n+1}$, where $k = 0\ldots p-2$, and on the contrary.

On the basis of the above-stated information we will consider ω_x satisfying (8), then $\omega_x \in \mu(p, A_n)$ and $\omega_x \in \mu(p, A_{n+1})$.

As ω_x belongs to set $\mu(p, A_{n+1})$ we have:

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

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

As ω_x belongs to set $\mu(p, A_n)$ and validity (7) we have:

$$\omega_x = \sum_{j=1}^{n}\gamma_j a_j = \sum_{k=1}^{n}(p-1)a_k - \sum_{j=1}^{n}\varphi_j a_j,$$

where $\gamma_i, \varphi_i \in Z_p$, $I = 1\ldots n$.

Thus, there is an equality:

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

From the latter equality it follows that $-\delta_{n+1} \in W_{\mu(2p-1,\,An)}$. Hence, for injectivity of vector A_{n+1}, $|\delta_{n+1}| \notin W_{\mu(2p-1,\,An)}$ is necessary.

Then we we will define an addition operation $\oplus$ on set $\mu(p, A)$ of knapsack vector $A = (a_1, a_2, \ldots, a_n)$ as follows:

$$\forall w_1, w_2 \in \mu(p,)\ w = w_1 \oplus w_2 = \sum_{i=1}^{n}\alpha_i a_i \oplus \sum_{i=1}^{n}\beta_i a_i = \sum_{i=1}^{n}\gamma_i a_i, \qquad (9)$$

where $\gamma_i = (\alpha_i + \beta_i)\ mod\ p$; $\alpha_i, \beta_i \in Z_p$, $I = 1\ldots n$.

The set $\mu(p, A)$ with an addition operation $\oplus$ forms an additive finite Abelian group $(\mu(p, A), \oplus)$.

Definition. Two knapsack vectors $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_k)$, whose variation vectors ΔA and ΔB differ only in the value of the first component are isomorphic ones. We will denote them as $A \approx B$ if there is an isomorphism f: $\mu(p, A) \to \mu(p, B)$.

Two knapsack vectors can be isomorphic only when they have identical dimension and $|\mu(p, A)| = |\mu(p, B)|$.

Let's consider two isomorphic knapsack vectors $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_k)$. From (4) we have:

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

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

Let's call value $\varepsilon(A, B) = \delta'_1 - \delta_1$ a coefficient of isomorphism of two vectors A and B.

Then

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

$$b_1 = a_1 + \varepsilon,\ \ b_i = a_i + (p-1)\,p^{i-2}\varepsilon,$$

$$I = 2\ldots n,\ \varepsilon = \varepsilon(A, B). \qquad (10)$$

And the following correlation is valid :

$$\sum_{i=1}^{j-1}(p-1)b_i = (p-1)(a_1+\varepsilon) + \sum_{i=2}^{j-1}(p-1)(a_i + (p-1)p^{i-2}\varepsilon) = \sum_{i=1}^{j-1}(p-1)a_i + (p-1)\varepsilon(1 + \sum_{i=2}^{j-1}p^{i-2}) = \sum_{i=1}^{j-1}(p-1)a_i + (p-1)\varepsilon p^{j-2}. \qquad (11)$$

On the basis of properties of sequences $W_{\mu(p,\ A)}$ and $W_{\mu(p,\ B)}$ it is possible to draw a conclusion that $W_{\mu(p,\ B)}$ is received from $W_{\mu(p,\ A)}$ by "recursive scaling" on ε relative to nodal values $(a_2, \ldots, a_n)$, and each value a_i is displaced according to (10). Sequence $\Delta W_{\mu(p,\ B)}$ is received from $\Delta W_{\mu(p,\ A)}$ by replacement of all occurrences δ_1 on $\delta_1 + \varepsilon$.

If for knapsack vectors $A = (a_1, a_2, \ldots, a_n)$, $B = (b_1, b_2, \ldots, b_n)$ and $C = (c_1, c_2, \ldots, c_n)$ $A \approx B$ and $B \approx C$ are carried out then $A \approx C$. Really, due to bijectivity f:$\mu(p, A) \to \mu(p, B)$ and g:$\mu(p, B) \to \mu(p, C)$ it follows that $h = g\mathcal{f}$: $\mu(p, A) \to \mu(p, C)$ is bijective and $\varepsilon(A, C) = \varepsilon(A, B) + \varepsilon(B, C)$.

Isomorphism of knapsack vectors is an equivalence relation, and, hence, a set of isomorphic vectors forms an equivalence class. In each class there is a vector for which the coefficient of isomorphism with any other vector of this class is non-negative. Let's call such a vector a base vector of an equivalence class.

Let $\Theta = (\theta_1, \theta_2, \ldots, \theta_n)$ be a base vector of some equivalence class and $A = (a_1, a_2, \ldots, a_n)$ be an arbitrary element of the same class, i. e. $\Theta \approx A$, $\varepsilon(\Theta, A) > 0$. As $|\mu(p, A)| = |\mu(p, \Theta)|$ from density definition of a knapsack vector in Z_p we have:

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

Owing to (11) it follows that:

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

From the latter we will express $d_p(\Theta)$:

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

$$d_p(\Theta) = d_p(A)(1+k\,\varepsilon(\Theta, A)),$$

where

$$k = \frac{p^{n-2}}{\sum_{i=1}^{n}\theta_i} = \text{cont}. \qquad (12)$$

Thus, the basic vector has the greatest density among all vectors of its equivalence class.

In case if the basic vector Θ is supergrowing then vector A is also supergrowing. Really from (2) and (10) we have:

$$\sum_{i=1}^{j-1}(p-1)a_i = (p-1)(\theta_1+\varepsilon)+\sum_{i=2}^{j-1}(p-1)(\theta_i+(p-1)p^{i-2}\varepsilon) =$$

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

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

From the latter inequality it follows that for any equivalence class with a basic supergrowing vector there is a knapsack vector from the given class for any positive coefficient of isomorphism. Generally the given statement is not true. For example, for an injective vector (15, 42, 51, 83) there is no isomorphic vector in Z_2 with an isomorphism coefficient equal to 10 since vector (25, 52, 71, 123) is not injective.

Thus, KSPI with knapsack vector A is possible to transform into equivalent KSPI with a knapsack vector Θ, where Θ is a basic vector of an equivalence class of vector A. The expediency of the given transformation is caused by smaller volume of calculations $\mu(p, \Theta)$ and memory expenses. For example, to store each element $\mu(2, A)$ of supergrowing knapsack vector A = (45, 69, 218, 415, 796, 1752, 3588, 7375, 17897, 36073) 17 bits of memory are necessary, and to store corresponding values of a basic vector Θ = (1, 25, 130, 239, 444, 1048, 2180, 4559, 12265, 24809) 16 bits for each are enough. If values of a knapsack vector components are great and if there is corresponding dimension then the memory capacity necessary to store elements $\mu(p, A)$ can exceed the sizes of standard types of programming languages and consequently will demand additional procedures for storage and performance of operations with such "big" numbers which, naturally, causes the increase in time and memory expenses. In particular for the above-stated example to store values $\mu(2, B)$ of supergrowing vector B = (444444444, 444444468, 888889016, 1777778011, 3555555988, 7111112136, 14222224356, 28444448911, 56888900969, 11377780227) belonging to the same class of equivalence already 38 bits are necessary for each.

Theorem. Let $A = (a_1, a_2, \ldots, a_n)$ be an injective knapsack vector with dimension n and $t \neq 0$ be an integer value. Then, an injective knapsack vector with dimension n by means of whose components in Z_p all elements of a set are expressed $\{w + t|w \in \mu(p,)\}$ does not exist.

The proof.

Let's assume that an injective knapsack vector $B = (b_1, b_2, \ldots, b_n)$ exists. Then $\{w+t|w \in \mu(p,A)\} \subseteq \mu(p, B)$.

1. $t > 0$. Then $|\mu(p, B)| \geq |\mu(p, A)| + 1$ since zero is included in $\mu(p, B)$, but is not included in $\{w + t|w \in \mu(p,)\}$. But due to injectivity of vectors A and B $|\mu(p, B)| = |\mu(p, A)|$ is carried out. As we can see there is contradiction.

2. $t < 0$. Since $0 \in \mu(p,A)$, $t \in \mu(p, B)$ that contradicts $b_i \in N$, i=1, ..., n.

Thus, updating of KSPI by way of changing the numerical value of a crypto text leads to increase in the complexity of its crypto analysis.

Definition. Two knapsack vectors $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_n)$ are similar, we will denote them A≅B only when there is a mutually single-valued transformation $f: A \rightarrow B$ such that:

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

– $\forall a', a'' \in A, f(a' + a'') = f(a') + f(a'')$ is carried out.

Two vectors one of which is received from another by strong modular multiplication can serve as an example of two similar injective knapsack vectors.

Let us investigate the properties of two similar injective knapsack vectors $A = (a_1, a_2, \ldots, a_n)$ and $B = (b_1, b_2, \ldots, b_n)$ the transformation of which is defined by function $f(x) = cx$ in some field where c is some constant:

$$f(a_i) = ca_i = b_i,\ I = 1\ldots n,$$

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

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

Densities of such vectors are connected by a correlation:

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

$$d_p(A) = c\, d_p(B). \qquad (13)$$

Sequences $W_{\mu(p,\ A)}$ and $W_{\mu(p,\ B)}$ possess properties defined by a correlation (10). The elements of sequences $\Delta W_{\mu(p, A)}$ and $\Delta W_{\mu(p, B)}$ are connected as follows:

$$m_i = ch_i,\ I = 1\ldots n, \text{ where } m_i \in \Delta W_{\mu(p, B)},\ h_i \in \Delta W_{\mu(p, A)}$$

The most widely known are systems of information protection with an open key and with a knapsack on the basis of a secret key [2] in which a vector received from a knapsack vector by strong modular multiplication by values of a secret key is used as an open key. It is possible to perform the crypto analysis of such systems by analytical or statistical methods, or by means of the analysis of an open key.

Analytical methods are based on methods of decisions of equation (1) on the basis of known values from $\mu(p,)$. Applicability of the given methods is based on volumes of done calculations. The upper boundary of a number of solutions (1) is presented in [3] and generally is a NP-full problem.

Statistical methods are based on statistical characteristics of elements of a natural language or other language of the original text and the statistics of crypto text elements. The main objective of such methods is to find a mutually single-valued correspondence between the elements of an original text and a cipher text rather than to find a knapsack vector. They are applicable only in the presence of statistical volumes of cipher texts.

Methods of crypto analysis of an open key consist in restoration of a KSPI knapsack vector according to an open key vector. In particular, for two supergrowing knapsack vectors, received one from another by means of strong modular multiplication, A. Shamir offers an algorithm of finding a knapsack vector A KSPI if vector B [2] is known.

On the basis of knapsack vectors properties described above it is possible to formulate the following results:

1. Crypto analysis of KSPI can be made not only on the basis of statistics of cipher texts elements values, but also on distribution of values. As the probability of occurrences of elements $\Delta W_{\mu(p, A)}$ sequences of knapsack vector $A = (a_1, a_2, \ldots, a_n)$ in Z_p is a constant value for the set dimension n, the table of probabilities is calculated at the stage of preliminary preparation of crypto analysis. The analysis of cipher texts is made on the basis of differences between pairs of values of its elements. In this case a number of various values of a cipher text elements is more important than the volume of known cipher texts. The construction of an injective knapsack vector is carried out on the basis of properties $W_{\mu(p, A)}$ and Lemma 1.

2. The applicability of statistical methods of cipher texts analysis is based on its volume. Therefore if volumes of such information are small then the given methods are practically inapplicable. Updating KSPI with one knapsack vector into a system with dynamically generated knapsack vectors [4; 5] leads to practical inapplicability of statistical methods of cipher texts analysis.

To increase the cryptographic security of classical systems of information protection with an open key and with a knapsack it is necessary not only to use isomorphic and similar knapsack vectors, but also to change values of exits of the enciphering block of KSPI by value of some constant. For example, having altered a classical system of information protection with an open key and with a knapsack on the basis of a secret key (m, t) [2], it is possible to raise the system cryptographic security essentially.

Let's consider a simple example. Let $A = (2, 5, 6)$ be an injective increasing knapsack vector. Before the definition of an open key – vector B, we will apply function $f(x) = x^2 - x$ to the elements of vector A and considering that $f(2) = 2$, $f(5) = 20$, $f(6) = 30$, we will receive $A' = (2, 20, 30)$. Using pair $m = 220$ and $t = 17$ as a secret key [2] we will receive open key $B = (34, 120, 70)$ by strong modular multiplication [2]. A crypto analysis of vector B according to A. Shamir's algorithm can lead only to reception of a supergrowing vector A' [2] in which cipher texts $w = 7$ is inadmissible. Thus, the use of a secret key (m, t, $f(x)$) leads to the fact, that known methods of the analysis of an information protection system with an open key, in particular, those using strong modular multiplication, are inapplicable or demand additional expenses concerning transformation search $f(x)$.

References

1. Osipyan V. O. Development of methods of information transmission and security systems construction. Krasnodar, 2004.

2. Salomaa A. Cryptography with an open key. M. : World, 1995.

3. Podkolzin V. V., Osipyan V. O. Upper boundary of a number of solutions of a generalized task of a knapsack on a set point // Actual problems of information technologies safety : materials of III International theoretical and practical conf. / edited by O. N. Zhdanov, V. V. Zolotarev ; Siberian state aerospace university. Krasnoyarsk, 2009. P. 30–33.

4. Podkolzin V. V. A model of information security system with an open key on the basis of dynamic generation of a knapsack vector. M. : OPandPM, 2009. Vol. 16. Issue 5. P. 913–914.

5. Podkolzin V. V., Osipyan V. O. Of one modification of information security task with an open key on the basis of a generalized knapsack point. M. : OPandPM, 2009, Vol. 16. Issue 5. P. 905.