

Применение предложенного УОУ изгибом ДК для эндоскопов “КОБРА” и “ГРАДАН” позволило повысить их оперативное использование, поскольку отклонение ДК во время контроля осуществляется без привлечения второй руки оператора. Кроме этого устройство компактно и удобно располагается в руке. Общий вид корпусной конструкции pistolетного типа эндоскопов “КОБРА” и “ГРАДАН” с установленным УОУ показан на рис. 3.

Отдельно общий вид УОУ изгибом ДК показан на рис. 4.

#### СПИСОК ЛИТЕРАТУРЫ

1. Сирота Г.А. Технические эндоскопы – приборы для визуального контроля труднодоступных объектов // В мире НК. – 2000. – № 2(8). – С. 4–7.
2. Волоконно-оптическая интроскопия / Под общ. ред. Д.К. Саттарова. – Л.: Машиностроение, 1987. – 285 с.
3. А.с. 1187131 СССР, МКИ<sup>3</sup> G02B 23/00. Эндоскоп / В.Н. Бурцев, В.Н. Бурцев, В.И. Крылов, В.Н. Рубцов. Заявлено 14.07.82; Опубл. 23.10.85, Бюл. № 39.
4. А.с. 1012882 СССР, МКИ<sup>3</sup> А61В 1/00. Устройство для регулирования изгиба дистальной части эндоскопа / М.Е. Немировский. Заявлено 10.04.81; Опубл. 23.04.83, Бюл. № 15.
5. Пат. 2185083 РФ, МПК<sup>7</sup> А61В 1/00. Устройство управления изгибом конца эндоскопа / В.Н. Тарасов. Заявлено 22.09.99; Опубл. 20.07.02.
6. Перельгин А.В., Чигорко А.А. Проблемы расширения функциональных возможностей и повышения эффективности технических эндоскопов // Качество – стратегия XXI века: Матер. VII Междунар. научно-практ. конф. – Томск, 2003. – С. 176.
7. Чигорко А.А., Перельгин А.В., Понеделко Е.В. и др. Средства НК и ТД. Каталог. Научно-технический бюллетень «Сибирский аршин». Спецвыпуск 18 / Под ред. А.Б. Чигорко. – Томск: Изд-во «М-Принт», 2005. – 88 с.

УДК 519.72

## О СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПРОБЛЕМЫ РЮКЗАКА

В.О. Осипян

Кубанский госуниверситет, г. Краснодар  
E-mail: rrw@mail.ru

*Показана возможность обобщения базовых рюкзачных систем защиты информации. Приводится алгоритм построения инъективного нестандартного рюкзака размерности  $n+1$  с заданными каскадными значениями, исходя из аналогичного рюкзака размерности  $n$ . В работе рассмотрена лёгкая задача укладки нестандартного рюкзака.*

Как известно [1–3], криптостойкость рюкзачных систем защиты информации (РСЗИ) на основе заданного рюкзака зависит от первоначального способа кодирования элементарных сообщений и процедуры последующего шифрования открытого текста.

Рассмотрим класс систем защиты информации с открытым ключом и с рюкзаком, обладающим заранее заданными свойствами. Рюкзачный вектор  $A$  назовём с повторениями или без повторений, если его элементы повторяются или нет – соответственно. Для простоты изложения будем считать, что значения компонент рюкзачного вектора расположены в неубывающем порядке своих значений. При этом коэффициенты повторов для компонент рюкзака и входа  $(A, v)$  можно взять совершенно различными между собой способами из заданных двух целочисленных положительных массивов.

#### Выводы

Разработанная конструкция устройства оперативного управления позволяет за счет использования промежуточного рычажного элемента при помощи одной руки управлять изгибом дистального конца волоконно-оптических эндоскопов “КОБРА” и “ГРАДАН”, тем самым, повысив их оперативное применение.

*Авторы выражают искреннюю признательность директору ООО Компания “СМТ” к.т.н. А.Б. Чигорко за активное участие и предоставление технической помощи, во многом способствовавшие выполнению настоящей работы.*

Пусть  $A=(a_1, a_2, \dots, a_n)$  – рюкзачный вектор размерности  $n$ ,  $n \geq 3$  из  $n$  натуральных компонентов  $a_i$ ,  $i=1 \dots n$  и  $(A, v)$  – вход задачи о рюкзаке, где  $v$  – также некоторое натуральное число или нуль. Пусть далее,  $ZK_t = \{k_1, k_2, \dots, k_t\}$ ,  $k_1 + k_2 + \dots + k_t = n$ ,  $t \leq n$ ,  $ZC_p = \{m_1, m_2, \dots, m_p\}$  – множества коэффициентов повторений компонентов рюкзачного вектора  $A$  и входа  $(A, v)$  соответственно. Здесь элемент  $k_i$ ,  $k_i \geq 1$ ,  $i=1 \dots t$  – количество повторений компонент ранга натурального числа  $a_i$  в рюкзаке  $A$  ( $t$  – количество его различных компонент), а элемент  $m_i$ ,  $0 \leq m_i \leq p-1$ ,  $i=1 \dots p$ ,  $p \geq 2$ ,  $p \in N$  из множества  $ZC_p$  указывает максимальное значение коэффициента повтора при  $a_i$ ,  $i=1 \dots n$  для определения входа  $(A, v)$ . Множества  $ZK_t$  и  $ZC_p$  назовём спектрами коэффициентов рюкзака  $A$  и его входа  $(A, v)$  соответственно. Значения множества  $ZC_p$  иначе назовём каскадными значениями.

Так, например, если  $t=4, p=3$  и  $A=(1, 2, 5, 5, 13, 13, 13), ZC_3=\{1, 1, 1, 2, 2, 2, 1\}$ ,

то спектр коэффициентов рюкзака имеет вид

$$ZK_4=\{1, 1, 2, 3\}, k_1=1, k_2=1, k_3=2, k_{13}=3,$$

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

$$m_1 \leq 1, m_2 \leq 1, m_3 \leq 1, m_4 \leq 2, m_5 \leq 2, m_6 \leq 2, m_7 \leq 1.$$

Аналогично определим: решением без повторений компонент для входа  $(A, v)$  назовем подмножество элементов  $A$ , сумма которых равна  $v$ , т.е.

$$\sum_{i=1}^n \alpha_i a_i = v,$$

при условии, что  $\alpha_i \in \{0, 1\}$  – как принято считать для стандартных рюкзачных систем. Если же  $\alpha_i \in ZC_p = \{m_1, m_2, \dots, m_n\}$  и хотя бы один из коэффициентов  $\alpha_i \geq 2$ , то решением – соответственно с коэффициентами повторений компонент из  $ZC_p$ .

Все рассматриваемые в данной работе рюкзаки вовсе не обязаны обладать свойствами, присущими стандартным рюкзакам. Наоборот, здесь  $a_i, a_i \in ZK_i$  может повторяться и входить в сумму для определения входа  $(A, v)$  с коэффициентом  $\alpha_i \leq m_i, i=1 \dots n$ , где  $m_i \in ZC_{p_i}$ . Такие нестандартные рюкзаки обозначим через  $\tilde{A}$ , а входы – соответственно  $(\tilde{A}, v)$ .

Очевидно, в частности, если для нестандартного рюкзачного вектора  $\tilde{A}$

$$k_1=k_2=\dots=k_n=1, \\ m_1=m_2=\dots=m_n=1,$$

то мы имеем стандартный рюкзак без повторений [1]. Если же при  $k_1=k_2=\dots=k_n=1$ , соответствующие им коэффициенты входа  $m_1=m_2=\dots=m_n=1$ , то мы имеем обобщенный рюкзак [4] с заданным максимальным числом  $p-1$  повторений всех его компонентов.

Множество значений  $v_i$ , для которых входы  $(\tilde{A}, v_i)$  со спектром  $ZC_p$  имеют решения, назовем допустимыми значениями и обозначим через  $V_{\tilde{A}}=\{v_0, v_1, \dots, v_i\}$ . Количество всех допустимых числовых значений  $v_i$  для нестандартного рюкзачного вектора  $\tilde{A}$  обозначим через  $\mu(V_{\tilde{A}})$  и назовем мощностью входа. Так как для одного и того же  $v_i$  могут быть разные решения, то обозначим через  $\mu(\tilde{A})$  мощность различных между собой решений и назовем его мощностью нестандартного рюкзака  $\tilde{A}$ . Вектор  $\tilde{A}$  назовем инъективным, если каждый его вход обладает не более чем одним решением – с повторениями или без него. Очевидно, для инъективного вектора  $\tilde{A}$  имеет место равенство:

$$\mu(V_{\tilde{A}})=\mu(\tilde{A})=(m_1+1)(m_2+1)\dots(m_n+1).$$

Более того, имеет место также соотношение:

$$m_1 a_1 + m_2 a_2 + \dots + m_n a_n = \frac{2}{\mu(\tilde{A})} \sum_{i=0}^{\mu(\tilde{A})-1} v_i,$$

откуда в частности следует, если:

1.  $\tilde{A}$  – стандартный рюкзак, то  $m_1=m_2=\dots=m_n=1$ ,

$$\mu(\tilde{A})=2n, \text{ следовательно, } a_1+a_2+\dots+a_n = \frac{1}{2^{n-1}} \sum_{i=0}^{2^n-1} v_i;$$

2.  $\tilde{A}$  – обобщенный рюкзак, то  $m_1=m_2=\dots=m_n=p-1, \mu(\tilde{A})=p^n$  и

$$a_1+a_2+\dots+a_n = \frac{2}{p^n(p-1)} \sum_{i=0}^{p^n-1} v_i.$$

Последние соотношения можно применить для установления инъективности нестандартного вектора  $\tilde{A}$ , а с помощью следующего рекуррентного алгоритма легко найти множество всех допустимых значений  $v_i$  со спектром входа  $ZC_p$  и определить  $a_{n+1}$ , если известны  $a_1, a_2, \dots, a_n$ . Для удобства приведём схему построения такого алгоритма, представленной в виде таблицы (см. табл) значений для коэффициентов компонент нестандартного рюкзака. Из таблицы видно как найти всевозможные наборы длины  $n+1$  и соответствующие им значения  $v_i$ , если известны наборы длины  $n$ .

Таблица. Схема построения алгоритма

$a_{n+1}$	$a_n$	$a_{n-1}$	...	$a_0$	$a_1$	$v_i$
0	0	0	...	0	0	0
0	0	0	...	0	1	$a_1$
0	0	0	...	0	2	$2a_1$
			...			
0	0	0	...	0	$m_1$	$m_1 a_1$
0	0	0	...	1	0	$a_2$
0	0	0	...	$m_2$	$m_1$	$m_1 a_1 + m_2 a_2$
			...			
0	$m_n$	$m_{n-1}$	...	$m_2$	$m_1$	$m_1 a_1 + \dots + m_n a_n$
1	0	0	...	0	0	$a_n + 1$
1	0	0	...	0	1	$a_n + 1 + a_1$
1	0	0	...	0	2	$a_n + 1 + 2a_1$
			...			
1	0	0	...	0	$m_1$	$a_n + 1 + m_1 a_1$
1	0	0	...	1	0	$a_n + 1 + a_2$
			...			
1	0	0	...	$m_2$	$m_1$	$a_n + 1 + \dots + m_2 a_2 + m_1 a_1$
			...			
$m_{n+1}$	$m_n$	$m_{n-1}$	...	$m_2$	$m_1$	$m_1 a_1 + \dots + m_n + 1 a_n + 1$

Итак, пусть

$$\tilde{A}=(a_1, a_2, \dots, a_n)$$

– нестандартный рюкзачный вектор размерности  $n, n \geq 3$  из  $n$  произвольных натуральных компонентов  $a_i, i=1 \dots n, (\tilde{A}, v)$  – его вход со спектром входа  $ZC_p$  и

$$v = \sum_{l=1}^n \alpha_l a_l = \tilde{A} \cdot w_v^T$$

– произвольное допустимое значение для входа  $(\tilde{A}, v)$ . Здесь и ниже будем считать, что  $k_i=1, i=1 \dots n$ , т.е. заданный нестандартный рюкзак  $\tilde{A}$  без повторений.

Пусть, далее,  $V_{\tilde{A}}$  – множество всех допустимых значений  $v_i$  инъективного рюкзачного вектора  $\tilde{A}$  размерности  $n$ , со спектром входа  $ZC_p$ , т.е.

$$V_{\tilde{A}} = \{v_0, v_1, \dots, v_{\mu(V_{\tilde{A}})-1}\},$$

а  $V_{\tilde{A}} + a = \{v_0 + a, v_1 + a, \dots, v_{\mu(V_{\tilde{A}})-1} + a\}$

– множество всех значений  $v_i$  со сдвигом на натуральное число  $a$ . Тогда

$$V_{\tilde{A}+1} = \bigcup_{u=0}^{m_{n+1}} (V_{\tilde{A}} + u a_{n+1})$$

– представляет собой множество всех допустимых значений для рюкзачного вектора  $\tilde{A}+1$  размерности  $n+1$  со спектром входа

$$ZC_p = \{m_1, m_2, \dots, m_n, m_{n+1}\}.$$

Поэтому для определения компонента  $a_{n+1}$  инъективного рюкзачного вектора  $\tilde{A}+1$  размерности  $n+1$  с каскадным значением  $m_{n+1}$ , необходимо и достаточно выполнение следующих двух условий:

$$1. \quad a_n < a_{n+1} < \sum_{u=1}^n a_u;$$

$$2. \quad V_{\tilde{A}} \cap \bigcup_{u=1}^{m_{n+1}} (V_{\tilde{A}} + u a_{n+1}) = \emptyset.$$

Таким образом, на основе указанного рекуррентного алгоритма можно найти все инъективные вектора размерности  $n+1$ , исходя из аналогичных векторов размерности  $n$ .

Рюкзачный вектор

$$\tilde{A} = (a_1, a_2, \dots, a_n)$$

назовём сверхрастущим, если для любого  $j=2 \dots n$  имеет место неравенство

$$a_j > \sum_{k=1}^{j-1} m_k a_k. \quad (1)$$

Очевидно, если рюкзачный вектор  $\tilde{A}$  сверхрастущий, то он инъективный и одновременно возрастающий.

В самом деле, так как мы имеем следующий диапазон значений для  $v$ :

$$0 \leq v \leq m_1 a_1 + m_2 a_2 + \dots + m_n a_n,$$

то очевидно, если  $v$  не принадлежит указанному диапазону, то вход  $(\tilde{A}, v)$  не имеет решений. Не имеют решений и те входы  $(\tilde{A}, v)$ , для которых  $v$  не представляется в виде линейной комбинации:

$$v = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n, \alpha_i \in ZC_p. \quad (2)$$

Если же  $v$  имеет вид (2), и компоненты рюкзака  $\tilde{A}$  удовлетворяют (1), то каждый из  $\mu(V_{\tilde{A}})$  различных входов  $(\tilde{A}, v)$  имеет одно единственное решение в силу того, что заданный рюкзачный вектор сверхрастущий. Далее, будем говорить, что компонент  $a_i, i=1 \dots n$  входит в сумму  $v$  с кратностью  $\alpha_i \in \{m_1, m_2, \dots, m_n\}$ , если  $a_i$  имеет  $\alpha_i$  вхождений в  $v$ . Аналогично можно ввести другие известные определения и обозначения для рассматриваемого вектора так, как, например, в работе [4].

В частности, аналогично можно доказать следующие теоремы относительно нестандартного рюкзака  $\tilde{A}$  без повторов.

**Теорема 1.** Рюкзачный вектор без повторов  $\tilde{A} = (a_1, a_2, \dots, a_n)$  размерности  $n, n \geq 3$  с каскадными значениями  $ZC_p = \{m_1, m_2, \dots, m_n\}$  для входа  $(\tilde{A}, v)$  является плотным и инъективным, если

$a_1 = c, a_j = m^{j-2}((m-1)c+1), j=2 \dots n, m = \max\{m_1, m_2, \dots, m_n\}, m \in 1$ , где  $c$  – некоторая целая положительная константа.

**Доказательство.** Так как из указанного рекуррентного соотношения при  $n \geq 3$  непосредственно следует, что

$$a_j = m a_{j-1} = (m-1)a_{j-1} + a_{j-1},$$

то имеем:

$$a_j = m^{j-2}((m-1)c+1) = (m-1)a_{j-1} + a_{j-1} = \\ = (m-1)a_{j-1} + ((m-1)a_{j-2} + a_{j-2}) =$$

...

$$= (m-1)a_{j-1} + (m-1)a_{j-2} + \dots + (m-1)a_2 + (m-1)a_1 + 1.$$

Или

$$a_j = (m-1) \sum_{k=1}^{j-1} a_k + 1.$$

Таким образом, рюкзачный вектор  $\tilde{A}$  – сверхрастущий, следовательно, и инъективен, причём разность между левой и правой частями полученного равенства, как видно, минимальна и равна единице.

**Следствие.** В частности, при  $c=1$  из теоремы следует, что инъективный рюкзачный вектор

$$\tilde{A} = (1, m, m^2, \dots, m^{n-1})$$

является одновременно и плотным.

Заметим, что доказанная теорема справедлива также для более сильного условия, когда вместо  $m$  выступают соответствующие значения  $m_i, i=1 \dots n$ , а на практике можно предложить следующий рекуррентный алгоритм построения инъективного (плотного) вектора  $\tilde{A}+1$  размерности  $n+1$  со спектром  $ZC_p = \{m_1, m_2, \dots, m_n, m_{n+1}\}$ , если известен аналогичный вектор  $\tilde{A} = (a_1, a_2, \dots, a_n)$  размерности  $n (n \geq 2)$ . Для этого необходимо определить очередной компонент  $a_{n+1}$  в виде:

$$a_{n+1} = m_1 a_1 + m_2 a_2 + \dots + m_n a_n + a$$

так, чтобы выполнялось следующее очевидное равенство относительно мощностей:

$$\mu(V_{\tilde{A}+1}) = m_{n+1} \mu(V_{\tilde{A}}),$$

где

$$V_{\tilde{A}+1} = \bigcup_{k=0}^{m_{n+1}} (V_{\tilde{A}} + k a_{n+1}), V_{\tilde{A}} + a = \{v_0 + a, v_1 + a, \dots, v_i + a\},$$

$$a \in Z, m_i \in ZC_p, i=1 \dots n, a_2 > a_1.$$

**Теорема 2.** Пусть

$$\tilde{A} = (a_1, a_2, \dots, a_n)$$

– инъективный рюкзачный вектор размерности  $n, n \geq 3$ , а вектор

$$\tilde{B} = (b_1, b_2, \dots, b_n), b_i = e \cdot a_i \pmod{m}, (m, e) = 1$$

получен из  $n \geq 3$  сильным модульным умножением относительно  $m$  и  $e$ . Тогда решение задачи о рюкзаке для входа  $(\tilde{B}, v \cdot e)$  совпадает с единственным решением для входа  $(\tilde{A}, v)$ .

**Доказательство.** Схема доказательства данной теоремы полностью совпадает со схемой построения алгоритма для стандартной рюкзачной системы. Разница лишь в том, что в качестве функции шифрования применяется функция

$$F(x) = \tilde{B} W_x^T,$$

где  $WX$  – шифр сообщения  $X$ . Более того, алгоритм построения системы защиты информации с открытым ключом на основе рюкзака  $\tilde{A}$  полностью совпадает с алгоритмом построения систем защиты информации с обобщённым рюкзаком  $\tilde{A}_p$  [4].

Отметим, что данная теорема допускает все параметры обобщённой рюкзачной системы защиты информации с открытым ключом. При этом необходимо сделать ещё следующее замечание: процедура восстановления открытого текста, в целом, не зависит от самих компонент рюкзачного вектора  $\tilde{A}$ , она зависит только от размера самого рюкзака и способа первоначального кодирования элементарных сообщений открытого текста. Данное замечание относится ко всем существующим открытым рюкзачным системам.

Совершенно ясно, если для нестандартного рюкзака  $\tilde{A}$  полагать что  $m_1=m_2=\dots=m_n=p-1$ , то все рассмотренные выше рассуждения относительно РСЗИ останутся в силе, что, в свою очередь, означает: их можно перенести на случай обобщённых рюкзаков  $\tilde{A}_p$  с заданным максимальным числом

$p-1$  повторений всех его компонентов. Если же полагать  $m_1=m_2=\dots=m_n=1$ , то мы соответственно получим РСЗИ со стандартным рюкзаком.

В обоих случаях рюкзаки без повторений, т.е.  $k_1=k_2=\dots=k_n=1$ . Очевидно, когда компоненты рюкзачного вектора  $\tilde{A}$  с повторениями [5], т.е. хотя бы один элемент из множества  $ZK_i=\{k_1, k_2, \dots, k_i\}$  больше единицы или то же самое, что  $t < n$ , то  $\tilde{A}$  в данном случае сверхрастущим быть не может, и потому невозможно рассмотреть лёгкую задачу укладки рюкзака и, тем более, задачу построения СЗИ, использующей такой рюкзак.

В заключение подчеркнём, что для больших значений параметров нестандартных рюкзачных векторов, криптостойкость соответствующих систем защиты информации сравнительно выше, чем криптостойкость аналогичных стандартных СЗИ. В самом деле, если обозначить через  $N(K)$  – количество всех вариантов выбора ключей, то для стандартного рюкзака оно равно  $N(K)=2^n$ , для обобщённого рюкзака –  $N(K)=P^n$ , а для нестандартного рюкзака  $\tilde{A}$  –  $N(K)=(m_1+1)(m_2+1)\dots(m_n+1)$ , где  $n$  – длина рюкзака.

#### СПИСОК ЛИТЕРАТУРЫ

1. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 320 с.
2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
3. Коблиц Н. Курс теории чисел и криптографии. – М.: ТВП, 2001. – 260 с.
4. Осипян В.О. Об одном обобщении рюкзачных криптосистем // Известия вузов. Сев.-Кавк. регион. Техн. науки. – 2003. – Прилож. № 5. – С. 18–25.
5. Осипян В.О. О криптосистемах с заданным рюкзаком // Информационное противодействие угрозам терроризма. – 2004. – № 3. – С. 53–56.

УДК 681.326

## ИСПРАВЛЕНИЕ ОДИНОЧНЫХ ОШИБОК В МНОГОФАЗНЫХ КОДАХ

Л.А. Белицкая

ФГУП «Научно-производственный центр «Полюс», г. Томск  
E-mail: polus@online.tomsk.net

*Предлагается использовать систематический код для исправления одиночных ошибок в многофазных кодах. С использованием теории цифро-векторных множеств строятся многомерные таблицы истинности и на их основе – геометрические образы исправленных сигналов.*

Многофазный код является естественным кодом целого ряда устройств, где используются многофазные напряжения [1]. Он применяется в инверторах напряжения электроприводов переменного тока и других устройствах преобразовательной техники, в преобразователях угла в код и пересчетных схемах, в том числе и для выполнения всех арифметических операций [2]. Многофазный код наиболее исследован, и для него решена задача обнаружения и исправления ошибок исходя из его особой физической структуры. Эта особенность основана на контроле и сохранении непрерывности множеств логических нулей и единиц [2]. При этом можно ис-

правлять не только одиночные ошибки, но и двойные, тройные и т.д., а также различные их пачки. Данные возможности возрастают с увеличением числа фаз кода, но наиболее ценно исправление именно одиночных ошибок. Недостаток многофазного кода в том, что ошибки, возникающие на границе единиц и нулей, не исправляются.

Рассмотрим многофазный код в многомерном цифровом пространстве с добавлением контрольных разрядов.

Особенность его заключается в том, что при последовательном прохождении кодовых комбина-