Дискретная математика

УДК 519.72:004.056.55

ШИФРОВАНИЕ НА ОСНОВЕ СУММ СО СЛАГАЕМЫМИ — ПРОИЗВЕДЕНИЯМИ ВЕСОВЫХ И СВОБОДНЫХ КОМПОНЕНТОВ

А. И. Никонов

Самарский государственный технический университет,
443100, Россия, Самара, ул. Молодогвардейская, 244.

E-mail: nikonovai@mail.ru

Рассмотрены математические средства шифрования исходного текста, позволяющие обеспечить простоту соответствующей расшифровки, которая восстанавливает последовательность целочисленных весовых коэффициентов. Составитель шифра проверяет, как выполняется условие выделимости этих коэффициентов. Правило выделения предусматривает использование операций нижнего или верхнего округления. Сформированный шифр представляется значениями конечных сумм.

Ключевые слова: *шифр, конечная сумма, весовой коэффициент, свободный множитель, условие выделимости.*

Настоящая статья посвящена рассмотрению математических средств шифрования исходного (первичного текста), позволяющих успешно обеспечить простоту его расшифровки, которая производится адресатом. Общий подход к созданию указанных математических средств заключается в следующем.

Составитель шифра, имея исходный текст, задает основное математическое выражение ME, составленное из определенных компонентов. Согласно правилу составления ME в него включается множество независимых друг от друга параметров — факторов скрытности, обладающих статусом ключевых. Их значения уже имеются у адресата — штатного получателя данного шифра.

Адресат вместе со всеми знает упомянутое правило составления ME и переданное значение ME, но скрываемые от посторонних ключевые значения известны ему, согласно правилу Керкхоффса [1], лишь совместно с шифровальщиком. Выполняя задачу расшифровывания очередного V-того полученного значения ME, адресат применяет к нему определенное преобразование P, последовательно изменяя натуральное g. При этом из видоизменяемого объекта P (VME_{g-1}) выделяются значения соответствующих компонентов, превосходящих заданный количественный порог либо сниженных сравнительно с этим порогом. Таким образом, образуется конечная последовательность, строка чисел, а затем и знаков первичного алфавита, и эта строка придает расшифрованному сообщению законченный вид.

Александр Иванович Никонов (д.т.н., проф.), профессор, каф. электронных систем и информационной безопасности.

Если оказывается, что какой-либо фактор скрытности в пределах диапазона его изменения никак не влияет или слабо влияет на результат произведенного преобразования P, то такой фактор признается неэффективным. В свою очередь, шифротекст с увеличенным числом эффективных факторов скрытности и с увеличенными числами элементов, находящихся в диапазонах их изменения, если и поддается раскрытию, то с большими трудностями, нежели обычный шифр.

Применим изложенный подход в отношении математического выражения конечной суммы

$$\Phi = \Phi(p) = \sum_{l=1}^{p} b_l c_l, \quad \exists b_l \neq 0; \tag{1}$$

$b_l \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ — весовой коэффициент; $c_l \in \mathbb{R} \setminus \{0\}$ — свободный, то есть не зависимый от весовых коэффициентов, множитель. Таким образом, исследуемая сумма состоит из слагаемых — произведений весовых и свободных компонентов. Суммирование слагаемых из (1) предусматривает наличие хотя бы одной операции сложения, и поэтому $p \in \mathbb{N} \setminus \{1\}$. Строка весовых коэффициентов несет информацию о смысле шифра.

За частичную конечную сумму, соответствующую нашему ME, будем принимать величину

$$\Phi(l^*) = \sum_{l=1}^{l^*} b_l c_l, \quad l^* \leqslant p.$$

Более того, для удобства представления рассматриваемой суммы, не допускающего превышения нижнего предела суммирования над верхним, будем по необходимости продлевать конечные последовательности (b_l), (c_l), начиная их со значений $b_0 = c_0 = 0$. Тогда, конечно,

$$\Phi(l^*) = \sum_{l=0}^{l^*} b_l c_l.$$

Выработаем следующую концепцию алгебраического преобразования величины Φ. Пусть за счет подбора уровней b_l, c_l обеспечено выполнение такого условия выделимости очередного целочисленного весового коэффициента, что связано с определением отклонения $Dev_{p-g} = \Phi(p-g)/c_{p-g+1}$ от целого значения суммы (1):

$$\forall g \in I_p = \{1, \ldots, p\} :$$

$$Dev_{p-g} \in (0, \delta_+) = Dev^+_{p-g}, \tag{2}$$

$$Dev_{p-g} = 0 = Dev^0_{p-g}, \tag{3}$$

$$Dev_{p-g} \in (-\delta_-, 0) = Dev^-{}_{p-g}, \tag{4}$$

$$0 < \delta_+, \delta_- < 1. \tag{5}$$

Соотношение (2) или (4) применительно к произвольному индексу g выбирается в зависимости от полученного знака Dev_{p-g}, чтобы участвовать в

определении (с помощью операции соответственно нижнего, верхнего округления [2]) искомой целочисленной величины b_{p-g+1}; соотношение (3) выбирается в случае, когда $Dev_{p-g} = 0$, то есть

$$b_{p-g+1} = \begin{cases} \lfloor \varphi_{p-g+1} \rfloor : & Dev_{p-g} = {Dev^+}_{p-g}, \\ \varphi_{p-g+1} : & Dev_{p-g} = Dev^0_{p-g}, \\ \lceil \varphi_{p-g+1} \rceil : & Dev_{p-g} = {Dev^-}_{p-g}, \end{cases}$$

$$\varphi_{p-g+1} = \Phi(p-g+1)/C_{\Delta g}; \quad C_{\Delta g} = c_{p-g+1}. \tag{6}$$

Конечно же,

$$\varphi_{p-g+1} = \lfloor \varphi_{p-g+1} \rfloor = \lceil \varphi_{p-g+1} \rceil : \quad Dev_{p-g} = 0.$$

Величина отклонения Dev_{p-q} от целочисленного значения b_{p-q+1} может стать индикатором выбора конкретного типа операции округления для любого $g \in I_p$, во-первых, если оказывается известным только сам факт обеспеченности комплексного условия

$$(Dev_{p-g} = Dev^+_{p-g}) \bigvee (Dev_{p-g} = Dev^0_{p-g}) \bigvee (Dev_{p-g} = Dev^-_{p-g}),$$

и, во-вторых, если соблюдается дополнительное неравенство

$$\delta_+ + \delta_- < 1. \tag{7}$$

Тогда будем иметь

$$b_{p-g+1} = \begin{cases} \lfloor \varphi_{p-g+1} \rfloor & : & Dev_{p-g} = {Dev^+}_{p-g} = {Fr^+}_{p-g}, \\ \varphi_{p-g+1} & : & Dev_{p-g} = Dev^0_{p-g} = Fr^0_{p-g}, \\ \lceil \varphi_{p-g+1} \rceil & : & Dev_{p-g} = {Dev^-}_{p-g} = {Fr^-}_{p-g}, \end{cases} \tag{8}$$

где ${Fr^+}_{p-g}$, Fr^0_{p-g}, ${Fr^-}_{p-g}$ — положительное, нулевое, отрицательное отклонения частных вида (6) от целочисленных весовых коэффициентов вида b_{p-q+1}, причем абсолютные величины отклонений, указываемых в соотношениях (8), удовлетворяют неравенству (7); в общем случае подобные отклонения станем обозначать через Fr_{p-g}.

Теперь, преобразовывая с использованием (7) двойное неравенство, связанное с соотношениями (4), (8), находим:

$$1 - \delta_- < 1 + {Fr^-}_{p-g} < 1.$$

Это преобразование позволяет определить саму дробную часть из φ_{p-g+1}, пристыкованную к числу $(b_{p-g+1} - 1)$. Производить проверку с участием величины отклонения Dev_{p-g} на принадлежность φ_{p-g+1} первому или второму интервалу единичной длины соответственно

$$(b_{p-g+1} - 1, b_{p-g+1}], \quad [b_{p-g+1}, b_{p-g+1} + 1)$$

здесь не требуется; форматы первого и второго интервалов установлены согласно соотношениям (2)–(5).

В случае соблюдения неравенства (7) интервалы $(1-\delta_-,1)$, $(0,\delta_+)$ не перекрывают друг друга, обеспечивая тем самым однозначность взаимного соответствия уровня Fr_{p-g} и участка числовой оси, находящегося возле искомого значения b_{p-g+1}. То есть само расположение каждого из интервалов положительного, нулевого или отрицательного отклонений указывает на его принадлежность к одному из двух интервалов единичной длины. Любое допустимое значение Fr_{p-g} указывает на первый или второй интервалы единичной длины или на место их стыка, а вместе с тем определяет, операцию какого округления (в случае $Fr_{p-g}=0$ — никакого или безразлично какого) надо производить.

Если же условие (7) не выполняется, то сам по себе уровень Dev_{p-g} не способен указывать на определённый участок единичной длины, содержащий значение φ_{p-g+1}, что вызывает необходимость при задании очередного индекса g и нахождении очередного значения φ_{p-g+1} уточнять расположение данного значения и обосновывать этим тип применяемого далее округления.

Поскольку

$$\Phi(p-g+1)=\Phi-\sum_{\gamma=1}^{g}b_{p-\gamma+2}c_{p-\gamma+2}, \tag{9}$$

учитывая соотношения (6), (8) и округляя правую часть (9), будем иметь:

$$b_{p-g+1}=\begin{cases}\left\lfloor\left(\Phi-\sum\limits_{\gamma=1}^{g}b_{p-g+2}c_{p-\gamma+2}\right)/C_{\Delta_g}\right\rfloor: & 0<Fr_{p-g}<\delta_+,\\ \left(\Phi-\sum\limits_{\gamma=1}^{g}b_{p-\gamma+2}c_{p-\gamma+2}\right)/C_{\Delta_g}: & Fr_{p-g}=0,\\ \left\lceil\left(\Phi-\sum\limits_{\gamma=1}^{g}b_{p-\gamma+2}c_{p-\gamma+2}\right)/C_{\Delta_g}\right\rceil: & -\delta_-<Fr_{p-g}<0.\end{cases}$$

Представленная выше концепция алгебраического преобразования суммы Φ со слагаемыми вида (b_lc_l) может быть осуществлена алгоритмически. Произвольный, g-тый шаг соответствующего алгоритма может быть выстроен на базе вышеприведенных соотношений, уточняющих и округляющих правую часть (9); $g=1,\ldots,p$, $b_{p+1}=0$.

Рассмотрим план решения задачи (алгоритм) расшифровки. На g-том шаге производится вычисление очередного значения

$$\Phi-\sum_{\gamma=1}^{g}b_{p-g+2}c_{p-g+2},$$

что равно

$$b_{p-g+1}C_{\Delta_g}+\sum_{l=0}^{p-g}b_lc_l.$$

Значения свободных компонентов вида $c_{p-\gamma+2}$, как и сам вид c_l, известны нам изначально с формированием математического облика Φ, а значения

весовых коэффициентов вида $b_{p-\gamma+2}$ ($\gamma \leqslant g$) найдены в рамках предыдущих шагов данного алгоритма. Нам также известно, что для данного шага

$$(0 < Dev_{p-g} < \delta_+) \bigvee (Dev_{p-g} = 0) \bigvee (1 - \delta_- < Dev_{p-g} < 1).$$

Тогда, руководствуясь полученным g-тым промежутком допустимых значений Dev_{p-g}, применяем соответствующее выражение для уточнения правой части (9).

В некоторых частных случаях комплекс применяемых таким образом выражений может быть уменьшен. Если для каждого $p \in I_p$ обеспечено соблюдение двойного неравенства

$$0 \leqslant Fr_{p-g} < 1, \tag{10}$$

то коэффициент b_{p-g+1} может быть представлен как

$$\left\lfloor \Phi - \sum_{\gamma=1}^{g} b_{p-g+2} c_{p-g+2} \right\rfloor : \quad 0 < Fr_{p-g} < 1,$$

$$\Phi - \sum_{\gamma=1}^{g} b_{p-g+2} c_{p-g+2} : \quad Fr_{p-g} = 0$$

или в виде

$$\left\lfloor \Phi - \sum_{\gamma=1}^{g} b_{p-g+2} c_{p-g+2} \right\rfloor .$$

Покажем теперь, каким образом следует обеспечить выполнение условия выделимости весовых коэффициентов, для определённости имеющее вид (10). При этом в качестве выражения ME будем рассматривать конечные степенные суммы, слагаемые которых содержат свободные множители, представляемые степенями с основаниями и показателями — линейными многочленами:

$$ME = \Phi = \sum_{l=1}^{p} b_l c_l, \quad b_l \in \mathbb{N}_0, \quad \exists b_l \neq 0;$$

$$c_l = a_l^{m_l}, \quad a_l = a_0 + a_1 l, \quad m_l = m_0 + m_1 l;$$

$$a_0,\, a_1 \in \mathbb{R}_+, \quad m_0,\, m_1 \in \mathbb{N}_0.$$

Максимум задаваемых весовых коэффициентов, зависящий от объёма первичного алфавита, обозначим через b_m. Практически $b_m > 1$.

Сумма значений последовательности $\left(a_l^{m_l},\, l = 1, \ldots, p\right)$ есть значение многочлена от одной переменной [3], когда такая переменная последовательно принимает целочисленные значения.

Заметим сразу, что при $a_1 = m_1 = 0$, когда c_l становится константой, $a_0^{m_0} \neq 0$ и условие (10) всегда нарушается для какого-либо слагаемого — отношения из суммы $\Phi(p-g)/c_{p-g+1}$, используемой в проверке (10). В самом деле, хотя среди весовых коэффициентов вида b_l могут встречаться и нулевые, но $\exists b_l \neq 0$, а следовательно, их множество содержит хотя бы один коэффициент, имеющий значение, не меньшее единицы. Тогда и для всей суммы

Fr_{p-g} в целом как объекта правого неравенства (10) указанное условие также выполняться не будет.

Далее рассмотрим два типовых случая, возникающих при задании свободных компонентов, и укажем возможности соблюдения в их рамках условия (10). Первым таким случаем является задание c_l как члена геометрической прогрессии

$$c_l^{\mathrm{r}} = \begin{cases} 0 & : \quad l = 0, \\ a_0^{m_1 l} & : \quad l \in I_p. \end{cases}$$

Здесь факторы скрытности — это параметры $a_0 \neq 0$, m_1, а также p — верхняя граница интервала I_p.

В данном случае условие (10) рассматривается применительно к максимуму дробночастного отклонения

$$\max Fr_{p-g} = \left(b_m / a_0^{m_1(p-g+1)}\right) \sum_{l=0}^{p-g} c_l^{\mathrm{r}};$$

само же двойное неравенство (10) приобретает вид

$$0 \leqslant \max Fr_{p-g} = \frac{b_m}{x-1} \cdot \frac{x^{p-g}-1}{x^{p-g}} < 1, \quad x = a_0^{m_1}.$$

Оно выполняется при $x - 1 > 0$, когда разность $x^{p-g} - 1$ также положительна либо имеет нулевой уровень; далее здесь потребуется выполнение соотношения $x > b_m + 1$.

Второй специально рассматриваемый нами случай — это задание свободных компонентов, слагаемых из суммы Ф как одинаковых степеней членов арифметической прогрессии вида

$$c_l^a = \begin{cases} 0 & : \quad l = 0, \\ (a_0 + a_1 l)^\nu & : \quad l \in I_p, \quad \nu \in \mathbb{N}. \end{cases}$$

Факторами скрытности в данном выражении выступают параметры a_0, $a_1 \neq 0$, ν. Условие (10) представляется здесь как

$$0 \leqslant \max Fr_{p-g} = b_m \sum_{l=0}^{p-g} c_l^a / c_{p-g+1}^a = b_m \sum_{l=0}^{p-g} D_l^\nu < 1, \tag{11}$$

$$D_l = \begin{cases} 0: & l = 0, \quad g \in I_p, \\ (a_0 + a_1 l)/(a_0 + a_1(p-g+1)) = 1 - (\Delta_g - l)/(r_a + \Delta_g): & \\ & l = 1, \ldots, p-g, \quad g \in I_p \setminus \{p\}, \end{cases}$$

где $r_a = a_0/a_1$, $\Delta_g = p - g + 1$.

Данное условие выполняется при соблюдении неравенств

$$r_a + \Delta_g > 0, \quad r_a > \max(-\Delta_g) = -1.$$

Тогда

$$\lim_{\nu\to\infty} D_l^\nu = 0, \quad b_m \lim_{\nu\to\infty} D_l^\nu = 0, \quad l = 0,\dots,p-g, \quad g \in I_p.$$

Сумма конечного числа пределов вида $b_m \lim D_l^\nu$ также имеет нулевое значение:

$$\sum_{l=0}^{p-g} b_m \lim_{\nu\to\infty} D_l^\nu = 0, \quad g \in I_p.$$

Следовательно, не подлежит сомнению тот факт, что существует и может быть найдено такое минимальное значение ν, начиная с которого выполняется условие (11).

При задании величины Ф во втором рассматриваем случае сто́ит, в частности, иметь в виду вариант её представления со значениями параметров $a_0 = 0$, $a_1 = 1$, когда $c_l = l^\nu$ [4,5]. Факторами скрытности здесь выступают p, ν; условие (11) также выполняется.

Итак, в итоге выработана концепция шифрования с использованием математического выражения — конечной суммы со слагаемыми — произведениями весовых и свободных компонентов. Сформировано условие выделимости целочисленных весовых коэффициентов — носителей передаваемой информации, причем выявлена реалистичность выполнения указанных условий.

Предложен также алгоритм расшифрования принятого закодированного сообщения, то есть алгоритм формирования конечной последовательности восстановленных значений весовых коэффициентов, соответствующей первичному тексту данного сообщения. Алгоритм обеспечивает простоту расшифрования, требующего для начала знания нескольких ключевых параметров и числа или блока чисел (в зависимости от объёма передаваемой информации) — значения или значений суммы Ф, вбирающей в себя количественное обобщение искомой конечной последовательности (b_l, $l = 1,\dots,p$). Наличие указанной простоты подтверждается уже самим видом выражений, определяющих выполнение шагов предложенного алгоритма.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Рябко Б. Я., Фионов А. Н.* Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004. 173 с. [*Ryabko B. Ya., Fionov A. N.* The basis of the modern cryptography for IT practitioners. Moscow: Nauchniy Mir, 2004. 173 pp.]
2. *Anderson J. A.* Discrete Mathematics with Combinatorics. New Jersey: Prentice Hall, 2000. 799 pp.; русск. пер.: *Андерсон Дж.* Дискретная математика и комбинаторика. М.: Вильямс, 2004. 960 с.
3. *Кострикин А. И.* Введение в алгебру. Основы алгебры. М.: Наука, 1994. 320 с. [*Kostrikin A. I.* Introduction to algebra. Foundations of algebra. Moscow: Nauka, 1994. 320 pp.]
4. *Никонов А. И.* Преобразование суммы взвешенных степеней натуральных чисел с одинаковыми показателями // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2010. №1(20). С. 258–262. [*Nikonov A. I.* Converting the Sum of Weighted Degrees of Natural Numbers with the Same Parameters // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2010. no. 1(20). Pp. 258–262].
5. *Никонов А. И.* Приведение суммы взвешенных одинаковых степеней к явному комбинаторному представлению // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2012. №3(28). С. 163–169. [*Nikonov A. I.* Reduction of the sum of the weight equal powers

to explicit combinatorial representation // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2012. no. 3(28). Pp. 163–169].

Поступила в редакцию 09/X/2012;
в окончательном варианте — 23/XI/2012.

MSC: 68P25; 05A10

ENCIPHERING ON THE BASIS OF THE SUMS WITH PRODUCTS OF WEIGHT AND FREE COMPONENTS AS SUMMANDS

A. I. Nikonov

Samara State Technical University,
244, Molodogvardeyskaya st., Samara, 443100, Russia.

E-mail: nikonovai@mail.ru

The purpose of the given paper is reviewing of mathematical resources of enciphering of the source text, allowing to ensure the simplicity of appropriate decryption; the source text is a sequence of integer weight coefficients. The composer of the cipher checks how the condition of separability of these coefficients is satisfied. The selection rule provides usage of operations of the lower or upper roundoff. The generated cipher is represented by the values of the finite sums.

Key words: *cipher, finite sums, weight coefficients, free multipliers, separability condition.*

Original article submitted 09/X/2012;
revision submitted 23/XI/2012.

Alexander I. Nikonov (Dr. Sci. (Techn.)), Professor, Dept. of Electronic Systems and Information Security.