Дискретная математика

УДК 519.72:004.056.55

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ШИФРОВАНИЯ НА ОСНОВЕ СУММИРОВАНИЯ ПРОИЗВЕДЕНИЙ

А. И. Никонов

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

Рассмотрены свойства шифров, составляемых на основе сумм со слагаемыми — произведениями весовых и свободных компонентов. Свободные компоненты выступают здесь, во-первых, как одинаковые степени членов арифметической прогрессии, во-вторых, как члены геометрической прогрессии и, в-третьих, как члены последовательности комбинированного типа. В состав указанных свойств входит характер изменения относительных суммарных остатков в зависимости от характера изменения параметров рассматриваемых видов последовательностей. За счет введения принадлежности параметров рассмотренных последовательностей множеству действительных чисел составляемый шифр и характеризуется повышенной эффективностью.

Ключевые слова: *относительный суммарный остаток, функциональная последовательность, параметр последовательности, разность, производная.*

Сначала напомним, что какой-либо фактор скрытности повышает собственную эффективность при создании того или иного шифра, если в пределах своего изменения его влияние на результат преобразования, производимого с составленным шифровальщиком математическим выражением ME, соответственно увеличивается [1].

Целью настоящей статьи является описание нескольких разновидностей шифра на основе сумм со слагаемыми — произведениями, свободные компоненты которых имеют сомножители показателей и оснований степеней, принадлежащие числовому множеству $\mathbb{R}$.

В качестве основного математического выражения примем [2, 3]

$$\Phi = \sum_{l=1}^{p} b_l c_l, \tag{1}$$

ISSN: 2310-7081 (online), 1991-8615 (print); doi: http://dx.doi.org/10.14498/vsgtu1316

Образец цитирования: А. И. Никонов, “Повышение эффективности шифрования на основе суммирования произведений” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2014. № 2 (35). С. 199–207. doi: 10.14498/vsgtu1316.

Сведения об авторе: *Александр Иванович Никонов* (д.т.н., проф.), профессор, каф. электронных систем и информационной безопасности.

E-mail address: nikonovai@mail.ru

где b_l — весовые коэффициенты — компоненты произведений ME, выражающие шифруемые буквы первичного алфавита, $b_l \in \mathbb{N}$; $c_l \in \mathbb{R}_+$ — свободные от шифруемых букв множители — компоненты произведений ME, образующие основную (c_l, $l \in I_p = 1, \ldots, p$) и остаточную (c_l, $l \in 1, \ldots, p-g$, $g \in 1, \ldots, p-1$) конечные последовательности; p — объём передаваемой посылки шифротекста, то есть общее количество весовых коэффициентов в посылке, причем $p \geqslant 2$. Математическое выражение, дополняющее основное выражение (1) и служащее инструментом определения условия выделимости весовых коэффициентов рассматриваемого шифра [1, 4], имеет вид относительного суммарного остатка (ОСО)

$$\varphi(\upsilon) = \sum_{l=1}^{\upsilon} \frac{b_l c_l}{c_{\upsilon+1}}, \quad \upsilon = p-g, \quad g = 1, \ldots, p-1.$$

В настоящей статье будут рассмотрены следующие типовые случаи задания функциональных последовательностей [5, 6] со свободными компонентами, где эти компоненты выступают: как одинаковые степени членов арифметической прогрессии, в качестве оснований которых берутся произведения натуральных и действительных чисел (верхний индекс члена этой последовательности — a); как члены геометрической прогрессии, в качестве степенных показателей которых также берутся произведения указанного вида (верхний индекс члена этой последовательности — e); как члены последовательности комбинированного типа, в качестве сомножителей степенных показателей и оснований которых берутся одинаковые натуральные числа, а другие их сомножители представляют собой действительные числа (верхний индекс члена этой последовательности — κ). Общее представление рассматриваемых типовых случаев имеет следующий вид:

$$\varphi_m(\upsilon) = b_m \sum_{l=1}^{\upsilon} \frac{(l_1\psi)^{l_2\nu}}{((\upsilon_1+1)\psi)^{(\upsilon_2+1)\nu}}; \quad l_1, l_2 \in \{l\}, \quad \upsilon_1, \upsilon_2 \in \{0, \upsilon\};$$
$$\nu \in \mathbb{R}_+ \setminus [0,1), \quad \psi \in \mathbb{R}_+ \setminus [0,1]; \quad b_m = \max b_l > 1.$$

Выявление интервала выделимости весовых коэффициентов, в пределах которого значения его точечных элементов имеют одинаковый знак либо нулевое значение, а протяженность этого интервала снижена сравнительно с единицей [1, 4], предполагает получение соответствующих граничных значений параметров формулы ОСО. То есть имеются в виду значения ОСО такие, что

$$0 \leqslant \varphi_m(\upsilon) < 1. \tag{2}$$

При этом первоначально граничное значение числа свободных множителей из последовательности ОСО, отвечающее длине участка (2), может задаваться исходя из каких-либо предметных соображений. Например, это может быть длина используемого алфавита (b_l, $\max l = p$).

Более подробное выражение каждого из перечисленных выше типовых случаев задания ОСО может быть представлено таким образом:

– случай последовательности ($\varphi_m^a(\upsilon)$): $l_1 = l$, $l_2 = 1$, $\upsilon_1 = \upsilon$, $\upsilon_2 = 0$;
– случай последовательности ($\varphi_m^e(\upsilon)$): $l_1 = l$, $l_2 = l$, $\upsilon_1 = 0$, $\upsilon_2 = \upsilon$;

– случай последовательности $(\varphi_m^{\varkappa}(\upsilon))$: $l_1 = l_2 = l$, $\upsilon_1 = \upsilon_2 = \upsilon$.

В пределах каждого из перечисленных случаев имеем три подслучая со следующим сочетанием параметров ν, ψ: 1) $\nu = \mathrm{const}_\nu$, $\psi = \mathrm{const}_\psi$; 2) $\nu = \mathrm{var}_\nu$, $\psi = \mathrm{const}_\psi$; 3) $\nu = \mathrm{const}_\nu$, $\psi = \mathrm{var}_\psi$.

Далее мы будем рассматривать свойства исследуемых относительных суммарных остатков, заключающиеся в определении направленности изменений их величин при изменении аргументов υ, ν, ψ. Указанные изменения величины ОСО в случае исследования аргумента υ будут иметь дискретный, а в случаях исследования аргументов ν, ψ — непрерывный характер. Рассмотрим сначала искомые свойства суммарных остатков нашего шифра, выражаемые — в относительной форме — как одинаковые степени членов арифметической прогрессии. Тогда, использовав обозначение $\upsilon_g = \upsilon + 1 > l$, при изменении соответствующей величины ОСО можем записать:

$$\varphi_m^a(\upsilon) = b_m \sum_{l=1}^{\upsilon} \frac{(l\psi)^\nu}{(\upsilon_g\psi)^\nu} = \sum_{l=1}^{\upsilon} \delta\varphi_{ml}^a(\upsilon),$$

$$\varphi_m^a(\upsilon_g) = b_m \sum_{l=1}^{\upsilon+1} \frac{(l\psi)^\nu}{((\upsilon_g+1)\psi)^\nu} = b_m \left(\frac{1}{(\upsilon_g+1)^\nu} + \sum_{l=1}^{\upsilon} \frac{(l+1)^\nu}{(\upsilon_g+1)^\nu} \right) = \sum_{l=0}^{\upsilon} \delta\varphi_{ml}^a(\upsilon_g).$$

В зависимости от общего числа весовых коэффициентов p будем иметь следующую разность (случай a, подслучай 1), относящуюся к составным частям рассматриваемой последовательности:

$$\Delta\left(\delta\varphi_{ml}^a(\upsilon)\right) = \delta\varphi_{ml}^a(\upsilon_g) - \delta\varphi_{ml}^a(\upsilon), \quad l = 1, \ldots, \upsilon,$$

в которой

$$\delta\varphi_{ml}^a(\upsilon) = \frac{b_m l^\nu}{\upsilon_g^\nu}, \quad \delta\varphi_{ml}^a(\upsilon_g) = \frac{b_m (l+1)^\nu}{(\upsilon_g+1)^\nu}.$$

Следовательно,

$$\Delta\left(\delta\varphi_{ml}^a(\upsilon)\right) = b_m \frac{((l+1)\upsilon_g)^\nu - (l(\upsilon_g+1))^\nu}{(\upsilon_g+1)^\nu \upsilon_g^\nu}.$$

Поскольку $l\upsilon_g + \upsilon_g > l\upsilon_g + l$ и, кроме того,

$$\delta\varphi_{m_0}^a(\upsilon_g) = \frac{b_m}{(\upsilon_g+1)^\nu} > 0,$$

получаем суммарно $\varphi_m^a(\upsilon_g) > \varphi_m^a(\upsilon)$. Таким образом, с увеличением числа υ или p общая величина ОСО тоже возрастает.

При изменении значений сомножителей показателя степени и затем — сомножителя её основания получим следующие выражения, содержащие соответствующие производные (случай a, подслучаи 2 и 3):

$$\left(\delta\varphi_{ml}^a(\upsilon)\right)'_\nu = \frac{d}{d\nu}\left(\delta\varphi_{ml}^a(\upsilon)\right) = b_m \frac{d}{d\nu}\left(\frac{l^\nu}{\upsilon_g^\nu}\right) = \frac{b_m l^\nu}{\upsilon_g^\nu}(\ln l - \ln \upsilon_g) < 0, \quad l = 1, \ldots, \upsilon;$$

$$(\varphi_m^a(\upsilon))'_\nu = \sum_{l=1}^{\upsilon} (\delta\varphi_{ml}^a(\upsilon))'_\nu < 0;$$

$$(\delta\varphi_{ml}^a(\upsilon))'_\psi = \frac{d}{d\psi}(\delta\varphi_{ml}^a(\upsilon)) = b_m \frac{d}{d\psi}\left(\frac{l^\nu}{\upsilon_g^\nu}\right) = 0, \quad l = 1, \ldots, \upsilon;$$

$$(\varphi_m^a(\upsilon))'_\psi = \sum_{l=1}^{\upsilon} (\delta\varphi_{ml}^a)'_\psi = 0.$$

Итак, в случае a при увеличении параметра ν члены функциональной последовательности $(\varphi_m^a(\upsilon))$ уменьшаются, а при увеличении параметра ψ они остаются неизменными. Вычисление ОСО в данном случае может производиться, в частности, по методике комбинированного представления суммы взвешенных одинаковых степеней [1, 2, 7].

Функциональную последовательность для случая, индексируемого символом ε, рассмотрим исходя из того, что известна формула её члена [1]:

$$\varphi_m^\varepsilon(\upsilon) = b_m \sum_{l=1}^{\upsilon} \frac{\psi^{l\nu}}{\psi^{\upsilon_g \nu}} = \frac{b_m}{\psi^\nu - 1} \cdot \frac{\psi^{\upsilon\nu} - 1}{\psi^{\upsilon\nu}}.$$

Разность между соседними членами рассматриваемой последовательности (случай ε, подслучай 1) выглядит следующим образом:

$$\Delta\varphi_m^\varepsilon(\upsilon) = \varphi_m^\varepsilon(\upsilon_g) - \varphi_m^\varepsilon(\upsilon) = \frac{b_m}{\psi^\nu - 1}\left(\frac{\psi^{\upsilon_g\nu} - 1}{\psi^{\upsilon_g\nu}} - \frac{\psi^{\upsilon\nu} - 1}{\psi^{\upsilon\nu}}\right) = \frac{b_m}{\psi^{\upsilon_g\nu}} > 0.$$

Производная, определяемая в целях указания характера возрастания или убывания уровня $\varphi_m^\varepsilon(\upsilon)$ в зависимости от соответствующих изменений параметра ν (случай ε, подслучай 2), имеет вид

$$(\varphi_m^\varepsilon(\upsilon))'_\nu = \frac{d}{d\nu}(\varphi_m^\varepsilon(\upsilon)) = \frac{d}{d\nu}\left(\frac{b_m}{\psi^\nu - 1}\left(1 - \frac{1}{\psi^{\upsilon\nu}}\right)\right) =$$
$$= \frac{b_m \ln\psi}{(\psi^\nu - 1)^2 \psi^{\upsilon\nu}}\left(-\psi^\nu(\psi^{\upsilon\nu} - 1) + \upsilon(\psi^\nu - 1)\right).$$

Последний сомножитель данного выражения, заключенный в скобки, разложим с использованием формулы бинома [8, 9]:

$$-\psi^\nu\left((\psi^\nu - 1 + 1)^\upsilon - 1\right) + \upsilon(\psi^\nu - 1) =$$
$$= -\psi^\nu\left((\psi - 1)^\upsilon + \upsilon(\psi^\nu - 1)^{\upsilon-1} + \ldots + \upsilon(\psi^\nu - 1) + 1 - 1\right) + \upsilon(\psi^\nu - 1).$$

Поскольку в области задания наших значений ν, ψ имеем $-(\psi^\nu - 1) < 0$, получаем: $(\varphi_m^\varepsilon(\upsilon))'_\nu < 0$.

Производная, определяемая с той же целью, что и рассмотренная относительно значения $\varphi_m^\varepsilon(\upsilon)$ в зависимости от соответствующих изменений параметра ψ (случай ε, подслучай 3), может быть найдена как

$$(\varphi_m^{\varepsilon}(\upsilon))'_{\psi} = \frac{d}{d\psi}(\varphi_m^{\varepsilon}(\upsilon)) = \frac{d}{d\psi}\left(\frac{b_m}{\psi^{\nu}-1}\left(1-\frac{1}{\psi^{\upsilon\nu}}\right)\right) =$$
$$= \frac{b_m \nu \psi^{-1}}{(\psi^{\nu}-1)^2\psi^{\upsilon\nu}}\left(-\psi^{\nu}(\psi^{\upsilon\nu}-1)+\upsilon(\psi^{\nu}-1)\right).$$

Но выше было доказано, что член $-\psi^{\nu}(\psi^{\upsilon\nu}-1)+\upsilon(\psi^{\nu}-1)$ в пределах заданных ν, ψ всегда имеет значение, меньшее нуля, и поэтому можно заключить, что $(\varphi_m^{\varepsilon}(\upsilon))'_{\psi} < 0$.

К таким же результатам — по знакам исследуемых разности и производных для случая ε — можно прийти, рассматривая разновидность задания той же функциональной последовательности по её отдельным составным частям, как это было сделано в случае a.

Итак, при увеличении числа υ (или p) в случае ε общая величина ОСО тоже возрастает, а при увеличении любого из параметров ν, ψ она уменьшается.

Поступим аналогично с ОСО, содержащим слагаемые комбинированного вида степеней арифметической прогрессии и геометрической прогрессии (этот случай индексируется символом κ), и определим соседние члены последовательности относительных суммарных остатков:

$$\varphi_m^{k}(\upsilon) = b_m \sum_{l=1}^{\upsilon} \frac{(l\psi)^{l\nu}}{(\upsilon_g\psi)^{\upsilon_g\nu}} = \sum_{l=1}^{\upsilon} \delta\varphi_{ml}^{k}(\upsilon),$$
$$\varphi_m^{k}(\upsilon+1) = b_m \sum_{l=1}^{\upsilon+1} \frac{(l\psi)^{l\nu}}{((\upsilon_g+1)\psi)^{(\upsilon_g+1)\nu}} =$$
$$= b_m\left(\frac{\psi^{\nu}}{((\upsilon_g+1)\psi)^{(\upsilon_g+1)\nu}} + \frac{\sum_{l=1}^{\upsilon}((l+1)\psi)^{(l+1)\nu}}{((\upsilon_g+1)\psi)^{(\upsilon_g+1)\nu}}\right) =$$
$$= \delta\varphi_{m0}^{k}(\upsilon_g) + \sum_{l=1}^{\upsilon} \delta\varphi_{ml}^{k}(\upsilon_g),$$

а также разность соответствующих составных частей членов данной последовательности

$$\delta\varphi_{ml}^{\kappa}(\upsilon_g) - \delta\varphi_{ml}^{\kappa}(\upsilon) = b_{\psi}(l)\left(\frac{((l+1)^{\nu})^{l+1}}{(l^{\nu})^{l}} - \frac{((\upsilon_g+1)^{\nu})^{\upsilon_g+1}}{\left(\upsilon_g^{\nu}\right)^{\upsilon_g}}\right);$$
$$b_{\psi}(l) = \frac{b_m\psi^{(l+1)\nu}l^{l\nu}}{((\upsilon_g+1)\psi)^{(\upsilon_g+1)\nu}} = \delta\varphi_{m0}^{\kappa}(\upsilon_g)(\psi l)^{l\nu}; \quad l = 1,\ldots,\upsilon.$$

Пользуясь методом математической индукции, докажем следующее неравенство:

$$\frac{((l+1)^{\nu})^{l+1}}{(l^{\nu})^{l}} < \frac{((\upsilon_g+1)^{\nu})^{\upsilon_g+1}}{(\upsilon_g^{\nu})^{\upsilon_g}}. \tag{3}$$

Преобразуя (3) в пределах задания наших значений ν, ψ, легко получаем

эквивалентное ему неравенство

$$\frac{(l+1)^{l+1}}{l^l} < \frac{(\upsilon_g+1)^{\upsilon_g+1}}{\upsilon_g^{\upsilon_g}}; \tag{4}$$

именно оно и будет доказано ниже.

Первый индукционный шаг выглядит применительно к выражению (4) таким образом:

$$l=1: \quad 2^2 < \frac{(\upsilon_{g\min}+1)^{\upsilon_{g\min}+1}}{\upsilon_{g\min}^{\upsilon_{g\min}}},$$
$$\upsilon_{g\min} = \upsilon_{\min}+1 = p - g_{\max}+1,$$
$$g_{\max} = p-1 \Rightarrow \upsilon_{\min}=1,\ \upsilon_{g\min}=2,\ \upsilon_{g\min}+1=3.$$

Следовательно, $2^2 < 3^3/2^2 \Rightarrow 4^2 < 3^3$. Но если неравенство (4) с такими значениями $l=1$ и $\upsilon_g = \upsilon_{g\min}$ верно, то оно останется справедливым и для любой пары чисел $l=1$, $\upsilon_g \geqslant \upsilon_{g\min}$:

$$l=1: \quad 2^2 < \frac{(\upsilon_g+1)^{\upsilon_g+1}}{\upsilon_g^{\upsilon_g}}. \tag{5}$$

Переходя к выполнению второго индукционного шага, заметим, что с допущением правильности (4) при $l \geqslant 2$ ($\upsilon \geqslant l$, $\upsilon_g > l$) должна выполняться следующая система неравенств:

$$\begin{cases} \dfrac{l^l}{(l-1)^{l-1}} < \dfrac{(\upsilon_g+1)^{\upsilon_g+1}}{\upsilon_g^{\upsilon_g}}, \\ \ldots\ldots\ldots\ldots \\ \dfrac{2^2}{1^1} < \dfrac{(\upsilon_g+1)^{\upsilon_g+1}}{\upsilon_g^{\upsilon_g}}. \end{cases}$$

Перемножая левые и правые части (4) и этой системы, имеем:

$$\frac{(l+1)^{l+1}}{1^1} < \frac{(\upsilon_g+1)^{(\upsilon_g+1)l}}{\upsilon_g^{\upsilon_g l}}.$$

Применяя к правой части данного неравенства биномиальное выражение и учитывая, что $l+1 \leqslant \upsilon_g$, получаем:

$$(l+1)(l+1)^l\upsilon_g^{\upsilon_g l} < \upsilon_g^{(\upsilon_g+1)l} + (\upsilon_g+1)l\upsilon_g^{(\upsilon_g+1)l-1} + \ldots = \\ = \upsilon_g^{(\upsilon_g+1)l}(l+1) + l\upsilon_g^{(\upsilon_g+1)l-1} + \ldots. \tag{6}$$

Итак, правая часть неравенства (6) оказывается больше левой, а отсюда следует и справедливость неравенства (3).

Тогда имеем:

$$(\varphi_m^{\kappa}(\upsilon_g) - \delta\varphi_{m0}^{\kappa}(\upsilon_g)) - \varphi_m^{\kappa}(\upsilon) = \sum_{l=1}^{\upsilon} (\delta\varphi_{ml}^{\kappa}(\varphi_g) - \delta\varphi_{ml}^{\kappa}(\varphi)) =$$
$$= \sum_{l=1}^{\upsilon} b_{\psi}(l) \left(\frac{(l+1)^{(l+1)\nu}}{l^{l\nu}} - \frac{(\upsilon_g+1)^{(\upsilon_g+1)\nu}}{\upsilon_g^{\upsilon_g\nu}} \right) < 0. \quad (7)$$

Урегулируем вопрос с членом

$$\delta\varphi_{m0}^{\kappa}(\upsilon_g) = \frac{b_m\psi^{\nu}}{((\upsilon_g+1)\psi)^{(\upsilon_g+1)\nu}}, \quad (8)$$

для чего рассмотрим составную часть из (7), в сущности, такую же, что и на первом индукционном шаге (5), только с учётом сомножителя $\delta\varphi_{m0}^{\kappa}(\upsilon_g)$. А именно, используем применительно к составной части из (7) при $l = 1$ запись ряда Ньютона [6, 10]:

$$\delta\varphi_{m1}^{\kappa}(\upsilon_g) - \delta\varphi_{m1}^{\kappa}(\upsilon) = \delta\varphi_{m0}^{\kappa}(\upsilon_g) \left(\psi^{\nu} \cdot 2^2 - \right.$$
$$\left. - \psi^{\nu} \left(\upsilon_g^{(\upsilon_g+1)\nu} + (\upsilon_g+1)\nu\upsilon_g^{(\upsilon_g+1)\nu-1} + \ldots \right) \right). \quad (9)$$

Прибавим сюда член (8), в результате чего нетрудно убедиться, что знак модифицированного таким образом выражения (9) остаётся отрицательным. Учитывая затем остальные слагаемые левой части неравенства (7), получаем:

$$\varphi_m^{\kappa}(\upsilon_g) - \varphi_m^{\kappa}(\upsilon) < 0.$$

Это означает, что с увеличением параметра υ (или p) значение произвольного члена последовательности $(\varphi_m^{\kappa}(\upsilon))$, в данном случае κ (подслучай 1), уменьшается.

Теперь определим производную составной части произвольного члена функциональной последовательности $(\varphi_m^{\kappa}(\upsilon))$, а также самого данного члена по переменной ν (случай κ, подслучай 2):

$$(\delta\varphi_{ml}^{\kappa}(\upsilon))'_{\nu} = \frac{d}{d\nu}(\delta\varphi_{ml}^{\kappa}(\upsilon)) = b_m \frac{d}{d\nu} \left(\frac{(l\psi)^{l\nu}}{(\upsilon_g\psi)^{\upsilon_g\nu}} \right) =$$
$$= \frac{b_m l^{l\nu}}{\upsilon_g^{\upsilon_g\nu}\psi^{(\upsilon_g-l)\nu}} \left(\ln(l\psi)^l - \ln(\upsilon_g\psi)^{\upsilon_g} \right) < 0;$$
$$(\varphi_m^{\kappa}(\upsilon))'_{\nu} = \sum_{l=1}^{\upsilon} (\delta\varphi_{ml}^{\kappa}(\upsilon))'_{\nu} < 0.$$

Поступая аналогичным образом в отношении составной части и члена в целом той же функциональной последовательности, получаем следующий вид соответствующих производных по переменной ψ (случай κ, подслучай 3):

$$(\delta\varphi_{ml}^{\kappa}(\upsilon))'_{\psi} = \frac{d}{d\psi}(\delta\varphi_{ml}^{\kappa}(\upsilon)) = b_m \frac{d}{d\psi} \left(\frac{(l\psi)^{l\nu}}{(\upsilon_g\psi)^{\upsilon_g\nu}} \right) =$$

$$= \frac{b_m \nu l^{l\nu}(l-\upsilon_g)}{\upsilon_g^{\upsilon_g\nu}\psi^{(\upsilon_g-l)\nu+1}} < 0;$$

$$(\varphi_m^{\kappa}(\upsilon))'_{\psi} = \frac{d}{d\psi}(\varphi_m^{\kappa}(\upsilon)) = \sum_{l=1}^{\upsilon}(\delta\varphi_{ml}^{\kappa}(\upsilon))'_{\psi} < 0.$$

Как видим, при увеличении любого из параметров ν, ψ в рассаматриваемом случае (подслучаи 2, 3) уровень произвольного члена функциональной последовательности $\varphi_m^{\kappa}(\upsilon)$ уменьшается.

Приведенные выводы по характеру изменения свободных компонентов рассматриваемого шифра могут быть полезны при выборе основы используемого математического выражения ME, когда оказывается необходимым привести его параметры в соответствие с требуемым числом элементов шифра, участвующих в формировании данной шифрованной посылки.

В заключение обратим внимание на параметр шифра, также связанный с его эффективностью и определяемый границей используемой памяти. То есть несколько исследованных выше разновидностей ME потребует для своей реализации, при равном количестве элементов шифра и отсутствии введения соответствующих дополнительных множителей, различных границ используемой памяти и, соответственно, различной плотности размещения данных элементов. Здесь надо учитывать, что указанное размещение, представляющее рассматриваемый шифр, может вступить в противоречие с техническими возможностями практических средств его реализации.

СПИСОК ЛИТЕРАТУРЫ/ REFERENCES

1. А. И. Никонов, “Шифрование на основе сумм со слагаемыми — произведениями весовых и свободных компонентов” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2012. № 4(29). С. 199–206 doi: 10.14498/vsgtu1120. [A. I. Nikonov, “Enciphering on the basis of the sums with products of weight and free components as summands”, *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2012, no. 4(29), pp. 199–206 (In Russian)].
2. А. И. Никонов, “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 doi: 10.14498/vsgtu751. [A. I. Nikonov, “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 (In Russian)].
3. А. И. Никонов, “Об одном свойстве взвешенных сумм одинаковых степеней как матричных произведений” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2010. № 5(21). С. 313–317 doi: 10.14498/vsgtu816. [A. I. Nikonov, “On One Property of the Weighed Sums of Equal Powers as Matrix Products”, *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2010, no. 5(21), pp. 313–317 (In Russian)].
4. А. И. Никонов, “Условия выделимости весовых коэффициентов из сумм с членами последовательностей двух видов” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2013. № 2(31). С. 91–100 doi: 10.14498/vsgtu1231. [A. I. Nikonov, “Conditions of separability of weight factors from the sums with members of sequences of two aspects”, *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2013, no. 2(31), pp. 91–100 (In Russian)].
5. В. А. Ильин, В. А. Садовничий, Бл. Х. Сендов, *Математический анализ*. Т. 2: Продолжение курса. М.: МГУ, 1987. 358 с. [V. A. Il’in, V. A. Sadovnichii, B. Kh. Sendov, *Matematicheskiy analiz* [Mathematical analysis], V. 2, Moscow, Moscow State Univ. Press, 1987, 358 pp. (In Russian)]
6. Н. Н. Воробьев, *Теория рядов*. М.: Наука, 1979. 408 с. [N. N. Vorob’yev, *Teoriya ryadov* [Theory of Series], Moscow, Nauka, 1979, 408 pp. (In Russian)]

7. А. И. Никонов, “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 doi: 10.14498/vsgtu1099. [A. I. Nikonov, “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 (In Russian)].
8. J. A. Anderson, *Discrete Mathematics with Combinatorics*, Upper Saddle River, NJ, Prentice Hall, 2001, xiv+807 pp.; Дж. Андерсон, *Дискретная математика и комбинаторика*. М.: Вильямс, 2004. 960 с.
9. С. В. Судоплатов, Е. В. Овчинникова, *Элементы дискретной математики*. М.: ИНФРА-М, 2002. 280 с. [S. V. Sudoplatov, E. V. Ovchinnikova, *Elementy diskretnoy matematiki* [Elements of. discrete mathematics], Moscow, INFRA-M, 2002, 280 pp. (In Russian)]
10. Н. Я. Виленкин, *Комбинаторика*. М.: Наука, 1969. 328 с. [N. Ya. Vilenkin, *Kombinatorika* [Combinatorics], Moscow, Nauka, 1969, 328 pp. (In Russian)]

Поступила в редакцию 23/IV/2014;
в окончательном варианте — 18/V/2014;
принята в печать — 23/V/2014.

MSC: 68P25; 05A10

RISING OF EFFICIENCY OF ENCIPHERING ON THE BASIS OF SUMMATION OF PRODUCTS

A. I. Nikonov

Samara State Technical University,
244, Molodogvardeyskaya st., Samara, 443100, Russian Federation.

The properties of the code numbers made on the basis of the sums with products of weight and free components are considered. Free components appear here, at first, as equal powers of members of an arithmetical progression, secondly, as members of a geometrical progression, and, in the third, as members of sequence of the combined type. Besides, the structure of the specified properties includes character of a modification of relative summarized residuals depending on a modification of parameters of considered aspects of sequences. With respect to the introduction of a membership of parameters of considered sequences to set of real numbers the made code number also is characterized by the raised efficiency.

Keywords: *relative summarized residual, functional sequence, sequence parameter, difference, derivative.*

Received 23/IV/2014;
received in revised form 18/V/2014;
accepted 23/V/2014.

ISSN: 2310-7081 (online), 1991-8615 (print); doi: http://dx.doi.org/10.14498/vsgtu1316

Citation: A. I. Nikonov, “Rising of Efficiency of Enciphering on the Basis of Summation of Products”, *Vestn. Samar. Gos. Tekhn. Univ., Ser. Fiz.-Mat. Nauki* [J. Samara State Tech. Univ., Ser. Phys. & Math. Sci.], 2014, no. 2 (35), pp. 199–207. doi: 10.14498/vsgtu1316. (In Russian)
Author Details: *Alexander I. Nikonov* (Dr. Sci. (Techn.)), Professor, Dept. of Electronic Systems and Information Security.

E-mail address: nikonovai@mail.ru