УДК 004.056

Э. В. Фауре, *к.т.н., доцент*
e-mail: faureemil@gmail.com
Черкасский государственный технологический университет
б-р Шевченко, 460, г. Черкассы, 18006, Украина

МЕТОД ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ФАКТОРИАЛЬНОГО КОДИРОВАНИЯ С ВОССТАНОВЛЕНИЕМ ДАННЫХ

В работе предложен и подробно рассмотрен метод повышения эффективности факториального кодирования с восстановлением данных по перестановке, которое направлено на комплексное решение задач криптографической защиты и защиты данных от ошибок канала связи. Предложенный метод предусматривает введение дополнительных проверочных бит в информационный вектор перед его преобразованием в перестановку без уменьшения скорости кода. Такая операция позволяет повысить достоверность передачи информации при использовании факториального кодирования с восстановлением данных за счет существующей избыточности кода. Для предложенного метода изучены зависимости оценок вероятности необнаруженной ошибки и энергетического выигрыша от длины информационного вектора на входе кодера. Произведено сравнение обнаруживающей способности факториального кодирования с использованием и без использования дополнительных проверочных бит.

Ключевые слова: *факториальный код, перестановка, контроль целостности информации, криптозащита, помехоустойчивое кодирование, достоверность передачи, стойкость.*

Постановка проблемы. В системах передачи данных возникает необходимость одновременной защиты передаваемой информации от несанкционированного чтения, модификации и ошибок канала связи. Последовательное выполнение перечисленных операций приводит к увеличению вводимой избыточности, снижению быстродействия обработки данных и повышению требований к производительности устройств преобразования информации. Данное обстоятельство определяет актуальность разработки методов кодирования, которые обеспечивают комплексное решение задач криптозащиты, имитозащиты и защиты данных от ошибок в канале связи.

Анализ источников и публикаций. Приведенные в работах [1–4] результаты исследований показывают эффективность факториальных методов кодирования для обеспечения контроля целостности информации, совмещающего в себе функции имитозащиты и помехоустойчивого кодирования. Предложенные в этих работах факториальные коды относятся к систематическим кодам, которые не обеспечивают криптографическую защиту информации.

В работе [5] предложен метод факториального кодирования с восстановлением данных по перестановке (ФКВД), реализующий в себе функции обнаружения ошибок в канале связи и криптографической защиты информации.

ФКВД (FCDR – Factorial Code with Data Recovery by Permutation) предусматривает замену информационной последовательности из k бит (вектора $A(x)$) на перестановку $R_{FCDR}(x)$ порядка M $\left(M! \geq 2^k\right)$.

Пусть α – показатель избыточности (по мощности), равный для ФКВД отношению мощности множества перестановок порядка M к мощности множества информационных векторов $A(x)$ степени k:

$$\alpha = M! / 2^k . \qquad (1)$$

Для простейшей системы передачи данных с решающей обратной связью (РОС), где прямой канал – двоичный симметричный с переходной вероятностью p_0 $\left(q_0 = 1 - p_0\right)$, обратный канал – идеальный, в [5] получена оценка вероятности не обнаруженной декодером ФКВД ошибки $P_{ud}\left(FCDR, p_0\right)$ (см. формулу (2)), а также изучена зависимость оценки вероятности необнаруженной ошибки от размера блока данных k на входе кодера. При этом значение M выбиралось таким образом, чтобы

$$(M-1)!<2^k\le M!. \qquad (2)$$

Следовательно, $1\le\alpha<M$. Поскольку равенство $\alpha=1$ выполняется только при $k=1$ и $M=2$, для $k>1$ справедливо $1<\alpha<M$. Таким образом, используемая методика выбора M по (2) решает задачу обеспечения возможности восстановления данных по перестановке, однако приводит к избыточности кода. Наличие такой избыточности создает предпосылки ее использования для повышения достоверности передачи данных.

Целью данной работы является разработка метода повышения эффективности факториального кодирования с восстановлением данных путем повышения достоверности передачи за счет избыточности кода.

Решение задачи. Из формулы (1) следует:

1) величина $[\alpha]$ ($[a]$ означает целую часть числа a) определяет, сколько раз отрезок $\left[0;2^k-1\right]$ укладывается в отрезке $\left[0;M!-1\right]$;

2) уменьшение длины информационного вектора на Δk бит при фиксированном M приводит к увеличению показателя избыточности (по мощности) в $\alpha_2/\alpha_1=\left(M!/2^{k_1-\Delta k}\right)/\left(M!/2^{k_1}\right)=2^{\Delta k}$ раз.

Таким образом, если для заданного k вычисленное по (2) значение M такое, что $\alpha>2$, перед формированием проверочной части существует возможность ввести в информационную часть дополнительные проверочные биты, являющиеся, например, битами паритета. При этом порядок перестановки M и скорость кода v_{FCDR} (см. формулу (1) в [5]) не изменятся. Количество дополнительно вводимых бит ограничено выражением

$$r_{add}\le\left[\log_2\alpha\right]. \qquad (3)$$

Поскольку $\alpha<M$, справедлива оценка $r_{add}\le\left[\log_2 M\right]$. С другой стороны, удовлетворяющие условию (2) допустимые пределы изменения длины блока k на входе кодера в зависимости от M имеют вид $\left[\log_2(M-1)!\right]+1\le k\le\left[\log_2 M!\right]$, откуда также следует, что количество дополнительно вводимых бит $r_{add}\le\left[\log_2 M!\right]-\left[\log_2(M-1)!\right]-1\le\left[\log_2 M\right]$.

Следовательно, чем больше длина блока k и, соответственно, порядок перестановки M (по существу, чем выше качество канала связи), тем большим может быть количество дополнительно вводимых бит и, соответственно, выше значение вносимой избыточности и ресурса повышения достоверности.

На представленном на рис. 1 графике показаны максимальные значения количества дополнительно вводимых бит r_{add} в зависимости от M при выполнении условия (2).

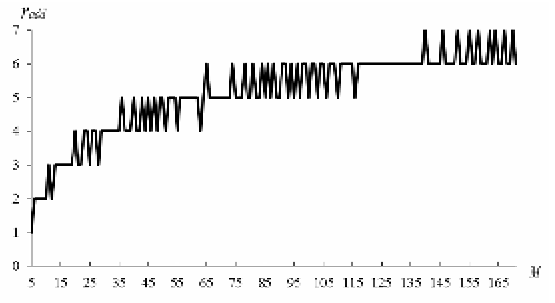


Рис. 1. График зависимости максимального количества дополнительно вводимых бит r_{add} от порядка перестановки M

Отметим, что в системах передачи данных с фиксированным M достоверность передачи может быть повышена за счет уменьшения размера блока данных на входе кодера на r_{add} бит и введения вместо них дополнительных проверочных бит.

Рассмотрим обнаруживающую способность ФКВД с использованием дополнительных проверочных бит (с дополнением). Такой метод кодирования будем обозначать ФКВДд (FCDRadd – FCDR with addition).

Очевидно, что ошибка не обнаруживается ФКВДд тогда и только тогда, когда переданная перестановка трансформирована в другую перестановку, а дополнительные проверочные биты принимают верные значения.

Пусть событие A={ошибка в блоке данных не обнаружена ФКВДд: принятая с ошибкой комбинация является перестановкой, а дополнительные проверочные биты совпадают с вычисленными в декодере}, $P(A)=P_{ud}\left(FCDRadd,p_0\right)$; событие B={перестановка (блок данных) при передаче по каналу связи преобразована в другую перестановку}, $P(B)=P_{ud}\left(FCDR,p_0\right)$.

При условии, что данные на входе и выходе блока формирования перестановки являются статистически независимыми, при декодировании принятого с ошибкой кодового слова ФКВДд каждый из дополнительно вводимых в информационную часть r_{add} проверочных бит с равными вероятностями может принимать значения 0 и 1. Тогда вероятность того, что после появления события B дополнительные проверочные биты примут верные значения (и, соответственно, ошибки в блоке обнаружены не будут), равна $P\left(A\middle|B\right)=2^{-r_{add}}$. Из формулы полной вероятности

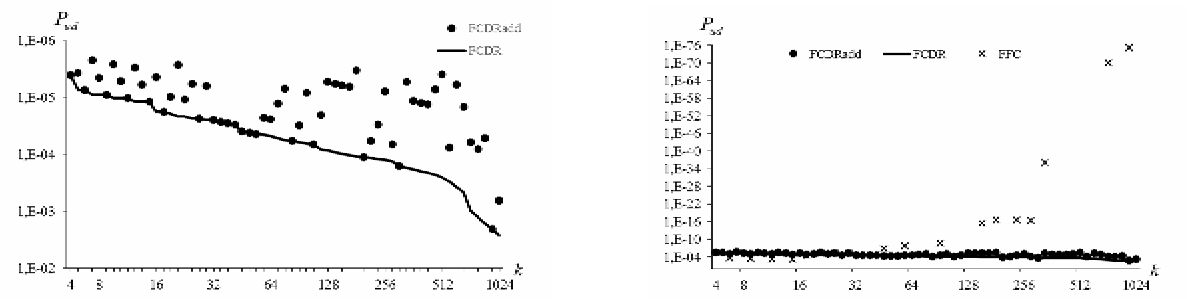
$$P_{ud}\left(FCDRadd,p_0\right)=\frac{P_{ud}\left(FCDR,p_0\right)}{2^{r_{add}}}, \qquad (4)$$

где $P_{ud}\left(FCDR,p_0\right)$ оценивается в соответствии с формулой (2) из [5];

r_{add} – количество дополнительно вводимых проверочных бит, ограниченное формулой (3).

Пример. Оценим энергетический выигрыш ФКВДд для некогерентного приема при $p_0=10^{-3}$ и $M=128$. Пусть $k=712$, а $r_{add}=4$. Тогда скорость кода $\nu_{FCDR}=712/896=0.795$, а $P_{ud}\left(FCDRadd,p_0\right)\le 3.009\cdot 10^{-5}$. Энергетический выигрыш $\Delta P\ge 3.94$ дБ.

На рис. 2, *а* представлены графики зависимостей оценок вероятностей необнаруженной ошибки от размера блока данных k на входе кодера в результате применения ФКВДд и ФКВД при $p_0=10^{-3}$, $M:\left(M-1\right)!<2^k\le M!$ и $r_{add}=\left[\log_2\alpha\right]$. На рис. 2, *б* дополнительно отображены оценки вероятности необнаруженной ошибки, достигаемые в результате применения полного факториального кода (ПФК) [2] при идентичных ФКВД длине информационной части блока k и скорости кода. Заметим, что зависимости скоростей ФКВД и ФКВДд от размера блока данных k на входе кодера совпадают и при $M:\left(M-1\right)!<2^k\le M!$ отображаются графиком на рис. 1 в [5].

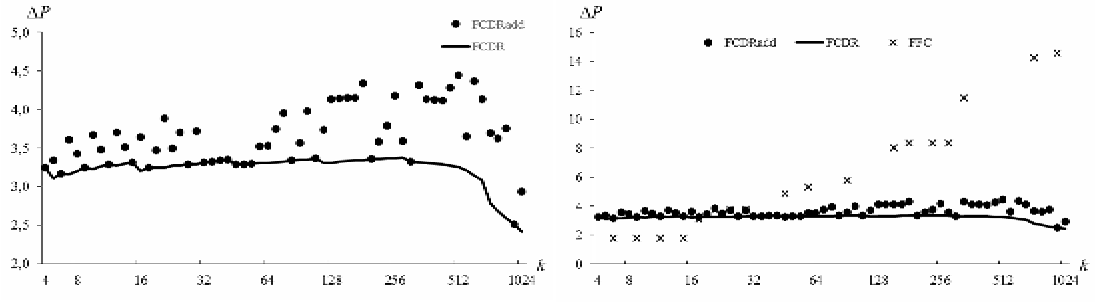


а) *б)*

Рис. 2. Графики зависимостей оценок вероятностей необнаруженной ошибки от размера блока данных k на входе кодера для ФКВДд и ФКВД (*а*); ФКВДд, ФКВД и ПФК (*б*)

На рис. 3, *а* представлены графики зависимостей оценок энергетического выигрыша от размера блока данных k на входе кодера в результате применения ФКВДд и ФКВД при $p_0=10^{-3}$, $M:\left(M-1\right)!<2^k\le M!$ и $r_{add}=\left[\log_2\alpha\right]$. На рис. 3, *б* дополнительно отображены оценки энергетического выигрыша, достигаемые в результате применения ПФК при идентичных ФКВД длине информационной части блока k и скорости кода.

Рис. 2 и 3 свидетельствуют о том, что введение дополнительных проверочных бит при формировании ФКВД позволяет повысить обнаруживающую способность кода (например, $\Delta P_{FCDRadd}-\Delta P_{FCDR}\approx 1.194\,дБ$ при $k=512$, $\Delta P_{FCDRadd}-\Delta P_{FCDR}\approx 1.601\,дБ$ при $k=1012$) и расширить диапазон значений размера блока данных k на входе кодера (с $k\le 18$ до $k\le 22$ для $p_0=10^{-3}$), при которых энергетический выигрыш ФКВД превышает соответствующий энергетический выигрыш ПФК при одинаковых скоростях кодов и кодировании символов перестановок равномерным двоичным кодом.



а) *б)*

Рис. 3. Графики зависимостей оценок энергетического выигрыша от размера блока данных *k* на входе кодера для ФКВДд и ФКВД (*а*); ФКВДд, ФКВД и ПФК (*б*)

Выводы. Представленный метод введения дополнительных проверочных бит перед преобразованием информационного вектора в перестановку позволяет повысить обнаруживающую способность факториального кодирования с восстановлением данных. Полученные результаты при $k \le 1024$ и $p_0 = 10^{-3}$ свидетельствуют об увеличении энергетического выигрыша в результате применения предложенного метода на величину до 1,6 дБ.

Список литературы

1. Фауре Э. В. Контроль целостности информации на основе факториальной системы счисления/ Э. В. Фауре, В. В. Швыдкий, А. И. Щерба // Journal of Qafqaz University. Mathematics and computer science. – 2016. – (В печати).
2. Фауре Э. В. Комбинированное факториальное кодирование и его свойства [Электронный ресурс] / Э. В. Фауре, В. В. Швыдкий, В. А. Щерба // Радіоелектроніка, інформатика, управління. – 2016. – № 3. – С. 80–86. – Режим доступу : http://www.csit.narod.ru/ric/riu_2016_3.pdf
3. Пат. 107655 Україна, МПК G06F 21/64 (2013.01), H04L 1/16 (2006.01). Спосіб контролю цілісності інформації / Рудницький В. М., Фауре Е. В., Швидкий В. В., Щерба А. І. ; заявник та патентовласник ЧДТУ. – № a201505937 ; заявл. 16.06.2015 ; опубл. 24.06.2016, Бюл. № 12.
4. Пат. 107657 Україна, МПК H03M 13/09 (2006.01), H04K 1/06 (2006.01), G09C 1/06 (2006.01). Спосіб комбінованого кодування інформації / Рудницький В. М., Фауре Е. В., Швидкий В. В., Щерба А. І. ; заявник та патентовласник ЧДТУ. – № a201508148 ; заявл. 17.08.2015 ; опубл. 24.06.2016, Бюл. № 12.
5. Фауре Э. В. Факториальное кодирование с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – № 2. – С. 33–39.

References

1. Faure, E. V., Shvydkyi, V. V. and Shcherba, A. I. (2016) Information integrity control based on the factorial number system. *Journal of Qafqaz University. Mathematics and computer science* [in Russian], (In print).
2. Faure, E. V., Shvydkyi, V. V. and Shcherba, V. A. (2016) Combined factorial coding and its properties. *Radioelektronika, informatyka, upravlinnya,* (3), pp. 80–86, available at: http://www.csit.narod.ru/ric/riu_2016_3.pdf
3. Rudnytskyi, V. M., Faure, E. V., Shvydkyi, V. V. and Shcherba, A. I. The method of information integrity control. Cherkasy State Technological University, assignee. UA Patent 107655, printed 24 June 2016 [in Ukrainian].
4. Rudnytskyi, V. M., Faure, E. V., Shvydkyi, V. V. and Shcherba, A. I. The method of combined information coding. Cherkasy State Technological University, assignee. UA Patent 107657, printed 24 June 2016 [in Ukrainian].
5. Faure, E. V. (2016) Factorial coding with data recovery. *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universitetu,* (2), pp. 33–39 [in Russian].

E. V. Faure, *Ph.D., associate professor*
e-mail: faureemil@gmail.com
Cherkasy State Technological University
Shevchenko blvd, 460, Cherkasy, 18006, Ukraine

THE METHOD FOR INCREASING FACTORIAL CODING EFFICIENCY WITH DATA RECOVERY

Introduction. *Methods of coding that provide a comprehensive solution of cryptographic protection, protection against intentional alteration of data, and data protection against communication channel errors can improve the efficiency of information processing tools by reducing included redundancy and used computing resources. The development of such methods is a topical area of current research.*

The purpose of this study *is to develop and analyze the method for increasing factorial coding efficiency with data recovery by increasing transmission reliability due to the code existing redundancy.*

The main material. *The proposed method provides the injection of additional check bits into information vector before its conversion into permutation without reducing the code rate. This operation allows to increase the reliability of information transmission using factorial coding with data recovery at the expense of existing code redundancy. The dependences of undetected error probability assessments and energy gain from information vector length at the encoder input are studied for the proposed method. The comparison of detection ability of factorial coding with or without additional check bits is done.*

Conclusions. *The presented method of injection of additional check bits into information vector before its conversion into permutation allows to increase the detection ability of factorial coding with data recovery. The results obtained with information vector length at the encoder input less or equal to 1024 and bit error probability equal to 10E-3 show an increase of energy gain by up to 1.6 dB as a result of the use of the proposed method.*

Keywords: *factorial code, permutation, information integrity control, cryptographic protection, error control coding, transmission accuracy, strength.*

Рецензенти: *В. М. Рудницький, д.т.н., професор,*
С. В. Голуб, д.т.н., професор