УДК 004.056

Фауре Э. В.[1], Швыдкий В. В.[2], Щерба В. А.[3]

[1]Канд. техн. наук, доцент, докторант, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина
[2]Канд. техн. наук, доцент, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина
[3]Ст. преподаватель кафедры прикладной математики Черкасского государственного технологического университета, Черкассы, Украина

КОМБИНИРОВАННОЕ ФАКТОРИАЛЬНОЕ КОДИРОВАНИЕ И ЕГО СВОЙСТВА

В работе предложен метод комбинированного факториального кодирования данных, направленный на обеспечение контроля целостности информации, предусматривающий комплексную защиту от навязывания ложных данных (имитозащиту) и ошибок в канале связи. Основная идея предложенного метода кодирования состоит в совмещении процедур полного факториального кодирования, использующего перестановку в качестве проверочной части кодового слова, и циклического избыточного кодирования (CRC). При этом проверочная часть кодового слова комбинированного факториального кода формируется путем вычисления остатка от деления проверочной части кодового слова полного факториального кода, представленной в виде многочлена, на кодовый полином CRC-кода. Определены основные свойства комбинированного факториального кода, выполнена оценка достоверности передачи, крипто- и имитостойкости. Выполнен сравнительный анализ обнаруживающей способности (вероятности необнаруженной кодом ошибки) и энергетического выигрыша для полного и комбинированного факториального кодирования при условии независимости возникающих в канале связи ошибок и их биномиального распределения. Определены пути улучшения представленной оценки вероятности необнаруженной факториальным кодом ошибки. Даны рекомендации по применению полного и комбинированного факториального кодирования.

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

НОМЕНКЛАТУРА

FFC – Full Factorial Code;

IIC – Information Integrity Control;

CFC – Combined Factorial Code;

CRC – Cyclic Redundancy Code (циклический избыточный код);

КФК – комбинированный факториальный код;

КЦИ – контроль целостности информации;

ПФК – полный факториальный код;

РОС – решающая обратная связь;

ФСС – факториальная система счисления;

ΔP – энергетический выигрыш;

$\varepsilon_{n_{CFC}}(x)$ – вектор ошибки, воздействующий на кодовое слово КФК;

$\varepsilon_k(x)$ – вектор ошибки, воздействующий на информационную часть кодового слова КФК;

$\varepsilon_{r_{CFC}}(x)$ – вектор ошибки, воздействующий на проверочную часть кодового слова КФК;

$\hat{\varepsilon}_{r_{CFC}}(x)$ – ошибка, возникающая при формировании в приемнике проверочной части кодового слова КФК;

ν_{CFC} – скорость КФК;

$\pi(0)$ – базовая перестановка множества целых чисел $\{0;1;2;\ldots;M-1\}$;

$\pi(t)$ – перестановка в дискретный момент времени t;

$\coprod$ – символ конкатенации (присоединения);

$A(x)$ – информационная часть кодового слова, представленная в виде многочлена;

$C(x)$ – кодовое слово, представленное в виде многочлена;

$D_{CFC}(x)$ – принятый из канала вектор кодового слова КФК;

$B(t)$ – факториальная запись числа, которое определяет порядковый номер перестановки;

$b_i(t)$ – i-й факториальный коэффициент синдрома перестановки в момент времени t;

$f_{CFC}(j)$ – число ошибок веса $j \in [0;n]$, не обнаруживаемых КФК;

$G(x)$ – многочлен, образующий CRC-код;

h^2 – соотношение сигнал/шум;

h_0^2 – соотношение сигнал/шум на входе некогерентного приемника, обеспечивающее вероятность битовой ошибки p_0 на его выходе;

h_{eq}^2 – соотношение сигнал/шум на входе некогерентного приемника, обеспечивающее эквивалентную вероятность битовой ошибки на его выходе $p_{0\,eq}$;

i – номер факториального коэффициента синдрома перестановки;

k – число двоичных символов в информационной части блока данных;

M – порядок (количество элементов) перестановки;

$N_{r_{CFC}}$ – количество возможных многочленов $G(x)$ степени r_{CFC}, образующих CRC-код;

n – полная длина блока данных;

$P_{IIC}(CFC)$ – вероятность взлома системы КЦИ КФК при однократной попытке подбора ключа;

DOI 10.15588/1607-3274-2016-3-10

$P_{IIC}(FFC)$ – вероятность взлома системы КЦИ ПФК при однократной попытке подбора ключа;

$P_{MAC}(CFC)$ – вероятность подбора имитовставки КФК в одном блоке данных;

$P_{MAC}(FFC)$ – вероятность подбора имитовставки ПФК в одном блоке данных;

P_{ud} – вероятность необнаруженной ошибки;

$P_{ud}(CFC, p_0)$ – вероятность необнаруженной ошибки при использовании КФК;

p_0 – переходная вероятность двоичного симметричного канала связи;

$p_{0\,eq}$ – эквивалентная вероятность битовой ошибки на выходе некогерентного приемника;

Q – вероятность безошибочного приема кодового слова;

$R(x)$ – проверочная часть кодового слова, представленная в виде многочлена;

$R_{CFC}(x)$ – проверочная часть кодового слова КФК, представленная в виде многочлена;

$R_{FFC}(x)$ – проверочная часть кодового слова ПФК, представленная в виде многочлена;

$\hat{R}_{CFC}(x)$ – проверочная часть кодового слова КФК, вычисленная в приемнике и представленная в виде многочлена;

$\hat{R}_{FFC}(x)$ – проверочная часть кодового слова ПФК, вычисленная в приемнике и представленная в виде многочлена;

r – число двоичных символов в проверочной части блока данных;

r_{CFC} – число двоичных символов в проверочной части блока данных КФК;

$S_{CFC}(x)$ – синдром ошибки КФК;

$S_F(t)$ – синдром перестановки в момент времени t;

T_{br} – среднее время взлома системы КЦИ (подбора имитовставки).

ВВЕДЕНИЕ

Дистанционное управление финансовыми операциями и электронным документооборотом приводит к необходимости обеспечения конфиденциальности и контроля целостности информации – КЦИ (IIC), который предусматривает защиту от навязывания ложных данных и обнаружение ошибок, вносимых каналом связи в процессе передачи сообщения. Эти обстоятельства стимулируют интенсивное развитие методов кодирования, которые обеспечивают комплексное решение задач криптозащиты, имитозащиты и защиты данных от ошибок, обусловленных действием помех в канале связи. Совмещение перечисленных функций позволяет сократить вводимую избыточность и уменьшить затраты производительности процессора, а его освобожденный ресурс – использовать для выполнения сервисных задач. В работах [1, 2] для разработки указанных методов кодирования предложено использовать систему счисления в остаточных классах, а в работе [3] – факториальную систему счисления (ФСС). Настоящая работа продолжает начатое в [4] исследование методов факториального кодирования информации – кодирования, использующего ФСС для формирования кодового слова.

1 ПОСТАНОВКА ЗАДАЧИ

В работе [4] представлен метод факториального кодирования, основанный на представлении проверочной части кодового слова в виде одной перестановки порядка M, который выбирается исходя из заданного набора свойств кода. При этом под перестановкой понимается упорядоченный набор символов $\{0;1;2;\ldots;M-1\}$, расположенных в порядке, который определяется информационной последовательностью и алгоритмом кодирования. Поскольку сумма чисел перестановки не зависит от порядка их следования, она постоянна и априорно известна. Поэтому в дополнение к ранее перечисленным свойствам данного метода кодирования отнесем также свойство самосинхронизации – возможности определения границ блока данных (синхронизации циклов) без использования специального, уникального (не используемого источником данных) символа, называемого маркером, флагом или разделителем.

Введем следующие определения.

Определение 1. Полным факториальным кодом (ПФК) называется систематический избыточный код, использующий в качестве проверочной части кодового слова перестановку чисел порядка M, которая определяется информационной последовательностью и алгоритмом кодирования.

Свойства ПФК подробно исследованы в [4]. Вместе с тем факториальное кодирование не ограничивается ПФК и может быть существенно расширено. В частности, представляет интерес кодирование, которое совмещает принципы факториального и циклического кодирования.

Определение 2. Комбинированным факториальным кодом (КФК) называется систематический избыточный код, использующий в качестве проверочной части кодового слова контрольную сумму циклического избыточного кода (CRC), вычисленную по проверочной части кодового слова ПФК.

Целью данной работы является исследование метода комбинированного факториального кодирования и оценка его характеристик при комплексном решении задач защиты информации и контроля ее целостности в системах передачи данных с решающей обратной связью (РОС).

2 ОБЗОР ЛИТЕРАТУРЫ

Рассмотрим простейшую систему с РОС, где прямой канал – двоичный симметричный с переходной вероятностью p_0 $(q_0 = 1 - p_0)$, обратный канал – идеальный, а символы, составляющие сообщение, являются элементами поля $F_2 = \{0;1\}$. Пусть k и r – число двоичных символов в информационной и проверочной частях блока данных соответственно, $n = k + r$ – полная длина блока.

Заметим, что перестановка для ПФК вычисляется по информационной последовательности таким образом, чтобы каждый из ее используемых символов существенно влиял на результат вычислений. Согласно [5], формирование проверочной части (перестановки) осуществляется за счет итерационной процедуры модификации

информационными символами синдрома перестановки $S_F(t)$. Синдром перестановки [6] $S_F(t)=\{b_{M-1}(t),b_{M-2}(t),...,b_0(t)\}$ представляет собой последовательность факториальных коэффициентов $b_i(t)$ $\left(0\le b_{M-1-i}(t)\le M-1-i\right)$ в факториальной записи числа $B(t)$, которое определяет порядковый номер перестановки $\pi(t)$ в дискретный момент времени t и отображает ее точкой (контрольной точкой) отрезка $[0;M!-1]$ числовой оси

$$B(t)=\sum_{i=0}^{M-1} b_{M-1-i}(t)\cdot(M-1-i)!.$$

Методы модификации синдрома информационными символами могут быть различными [5, 7].

Базовая перестановка $\pi(0)$, относительно которой производится формирование проверочной части (перестановки $\pi(t)$) может быть открытой или скрытой.

В работе [4] подробно рассмотрены свойства и обнаруживающая способность ПФК. При этом показано, что ошибка декодирования (ошибка, которую код не обнаруживает) возникает тогда, когда помеха, воздействующая на проверочную часть блока, преобразует переданную перестановку $\pi(t)$ в другую перестановку $\pi'(t)$, не совпадающую с перестановкой $\pi''(t)$, вычисленной декодером по принятой с ошибками информационной части блока.

Определим свойства и обнаруживающую способность КФК. При этом оценим следующие количественные показатели:

– скорость кода;

– вероятность не обнаруженной кодом ошибки;

– вероятность взлома кода методом «грубой силы».

Как и в [4], используем широко принятый [8 С. 601; 9, С. 232; 10. С. 361] подход к рассмотрению наборов (векторов) над полем F_2 в виде элементов алгебры многочленов с коэффициентами из F_2.

3 МАТЕРИАЛЫ И МЕТОДЫ

Концепция КФК (CFC) сочетает факториальное кодирование с циклическим избыточным кодированием. При этом по информационной последовательности сначала вычисляется проверочная часть кодового слова ПФК, после чего по полученной перестановке, представленной в виде многочлена $R_{FFC}(x)$ степени $(r_{FFC}-1)$, вычисляется вычет

$$R_{CFC}(x)=\left|R_{FFC}(x)\right|_{G(x)}, \qquad (1)$$

где $G(x)$ – многочлен степени r_{CFC}, образующий CRC-код.

Блок данных, состоящий из информационной части $A(x)$ (размерности k бит) и проверочной части $R(x)=R_{CFC}(x)$ (размерности $r=r_{CFC}$ бит), выводится в канал связи в виде $C(x)=A(x)\amalg R(x)$, где $\amalg$ – символ конкатенации (присоединения) $\left(C(x)=x^r\cdot A(x)\oplus R(x)\right)$. Полная длина блока $n=n_{CFC}=k+r_{CFC}$ бит, скорость КФК

$$\nu_{CFC}=k/(k+r_{CFC}).$$

Оценка достоверности передачи может быть получена следующим образом. При передаче по каналу связи на блок данных воздействует вектор ошибки $\varepsilon_{n_{CFC}}(x)$ с мощностью множества векторов $\mu\left\{\varepsilon_{n_{CFC}}(x)\right\}=2^n$. Этот вектор может быть представлен в виде конкатенации двух векторов – вектора помехи, покрывающего информационную часть блока из k бит, и вектора помехи, покрывающего проверочную часть блока из r_{CFC} бит:

$$\varepsilon_{n_{CFC}}(x)=\varepsilon_k(x)\amalg\varepsilon_{r_{CFC}}(x).$$

Отсюда принятый из канала связи вектор имеет вид

$$D_{CFC}(x)=C_{CFC}(x)\oplus\varepsilon_{n_{CFC}}(x)=$$

$$=\left(A(x)\oplus\varepsilon_k(x)\right)\amalg\left(R_{CFC}(x)\oplus\varepsilon_{r_{CFC}}(x)\right).$$

В приемнике по принятой из канала последовательности $A(x)\oplus\varepsilon_k(x)$ формируется проверочная часть (перестановка) для ПФК. По ее двоичному представлению $\hat{R}_{FFC}(x)$ согласно (1) вычисляется остаток $\hat{R}_{CFC}(x)=\left|\hat{R}_{FFC}(x)\right|_{G(x)}$. Этот остаток может быть представлен в виде $\hat{R}_{CFC}(x)=R_{CFC}(x)\oplus\hat{\varepsilon}_{r_{CFC}}(x)$, где $\hat{\varepsilon}_{r_{CFC}}(x)$ – ошибка, возникающая при формировании в приемнике проверочной части и преобразующая переданную проверочную часть в любую из $2^{r_{CFC}}$ возможных значений.

Ситуация, когда вычисленная в приемнике и принятая из канала проверочные части совпадают $\left(\hat{R}_{CFC}(x)=R_{CFC}(x)\oplus\varepsilon_{r_{CFC}}(x)\right)$, является признаком отсутствия ошибок в принятом блоке и служит основанием для вывода его потребителю. Соответственно, ситуация $\hat{R}_{CFC}(x)\ne R_{CFC}(x)\oplus\varepsilon_{r_{CFC}}(x)$ является признаком приема блока данных с ошибкой и служит основанием для его переспроса.

Отсюда синдром ошибки принимает вид:

$$S_{CFC}(x)=\left(R_{CFC}(x)\oplus\hat{\varepsilon}_{r_{CFC}}(x)\right)\oplus$$

$$\oplus\left(R_{CFC}(x)\oplus\varepsilon_{r_{CFC}}(x)\right)=\hat{\varepsilon}_{r_{CFC}}(x)\oplus\varepsilon_{r_{CFC}}(x).$$

Если $\varepsilon_{n_{CFC}}(x)=0$, то $S_{CFC}(x)=0$. Поэтому равенство $S_{CFC}(x)=0$ является признаком отсутствия модификации блока данных.

Вместе с тем, если $\varepsilon_{n_{CFC}}(x)\ne 0$ и $\hat{\varepsilon}_{r_{CFC}}(x)\oplus\varepsilon_{r_{CFC}}(x)=0$, возникают необнаруженные

ошибки на выходе декодера. Заметим, что $\varepsilon^{\wedge}_{r_{CFC}}(x)$ и $\varepsilon_{r_{CFC}}(x)$ статистически независимы, а ошибки декодирования при $\varepsilon_k(x) \neq 0$ и $\varepsilon^{\wedge}_{r_{CFC}}(x) = \varepsilon_{r_{CFC}}(x) = 0$ являются результатом возникновения коллизий.

Примем, что данные на входе и выходе блока формирования перестановки являются статистически независимыми. При этом перестановки, формируемые в нем по принятым с ошибками информационным частям блока данных, распределены равномерно с вероятностью (см. формулы (1), (11) в [4]):

$$p^{\wedge}_r = \begin{cases} \left(1-q_0^k\right)/M! \text{ при } M! < 2^k, \\ \left(1-q_0^k\right)\Big/\left(2^k-1\right) \text{ при } M! \geq 2^k. \end{cases}$$

Примем также, что $r_{CFC} \leq k$ и $2^{r_{CFC}} \leq M!$. Тогда вероятность появления каждого из $2^{r_{CFC}}$ возможных векторов $R_{CFC}(x)$, и, соответственно, каждого из $2^{r_{CFC}}$ возможных векторов $\varepsilon^{\wedge}_{r_{CFC}}(x)$, равна $p^{\wedge}_{r_{CFC}} = \left(1-q_0^k\right)\Big/2^{r_{CFC}}$ и определяет вероятность необнаруженной ошибки КФК кодом:

$$P_{ud}(CFC, p_0) = P\left\{\varepsilon^{\wedge}_{r_{CFC}}(x) = \varepsilon_{r_{CFC}}(x)\right\} = \left(1-q_0^k\right)\Big/2^{r_{CFC}}. \quad (2)$$

Оценка крипто- и имитостойкости ПФК и КФК может быть получена следующим образом. Выполним количественную оценку стойкости факториальных кодов от несанкционированного чтения и/или навязывания ложных данных при атаке только на передаваемые данные и взломе методом «грубой силы» путем перебора множества значений ключевого пространства.

При использовании ПФК информационная часть блока данных передается в открытом (не преобразованном) виде, поэтому этот код не обеспечивает криптографическую защиту данных. Согласно [4, 5], контрольная сумма (перестановка) обеспечивает имитозащиту данных с вероятностью взлома системы КЦИ при однократной попытке подбора ключа $P_{IIC}(FFC) \leq (M!)^{-2}$ и вероятностью подбора имитовставки в одном блоке данных $P_{MAC}(FFC) = (M!)^{-1}$.

При использовании КФК информационная часть блока данных передается, как и при ПФК, в открытом виде, поэтому КФК также не обеспечивает криптографическую защиту данных. Вероятность подбора ключа КЦИ при однократной попытке

$$P_{IIC}(CFC) = P_{IIC}(FFC) \cdot \left(N_{r_{CFC}}\right)^{-1} \leq (M!)^{-2} \cdot \left(N_{r_{CFC}}\right)^{-1},$$

где $N_{r_{CFC}}$ – количество возможных многочленов $G(x)$ степени r_{CFC}, образующий CRC-код. Вероятность подбора имитовставки для одного блока данных при однократной попытке $P_{MAC}(CFC) = 2^{-r_{CFC}}$.

Среднее время взлома системы КЦИ (подбора имитовставки) определяется выражением $T_{br} = 0,5/(P_{br} \cdot N)$ сек, где P_{br} – вероятность взлома системы КЦИ (подбора имитовставки) для анализируемого кода, N – производительность компьютерной группировки, выполняющей процедуру взлома (ключей/сек).

4 ЭКСПЕРИМЕНТЫ

Энергетический выигрыш ΔP при применении факториального кодирования будем определять для оптимального некогерентного приемника двоичных сигналов с ЧМн. Такой приемник характеризуется вероятностью битовой ошибки $p = 0,5 \cdot e^{-0,5h^2}$ [11, С. 45], где h^2 – соотношение сигнал/шум (отношение энергии сигнала, приходящейся на 1 бит принимаемого сообщения, к спектральной плотности мощности шума). Тогда энергетический выигрыш

$$\Delta P = 10 \lg \frac{\left(h_{eq}\right)^2}{h_0^2} = 10 \lg \frac{\ln\left(2p_{0eq}\right)}{\ln\left(2p_0\right)},$$

где $h_0^2 = 2\ln(2p_0)$ – соотношение сигнал/шум на входе некогерентного приемника, обеспечивающее вероятность битовой ошибки p_0 на его выходе; h_{eq}^2 – соотношение сигнал/шум на входе некогерентного приемника, обеспечивающее эквивалентную вероятность битовой ошибки на его выходе p_{0eq}, определенную в [12, С. 676] как вероятность ошибки в гипотетическом симметричном постоянном двоичном канале, при которой вероятность безошибочного приема достаточно длинного сообщения такая же, как и в рассматриваемой системе:

$$\left(1-p_{0eq}\right)^k = \left(1-P_{ud}\right)^{1/(Q+P_{ud})},$$

где $Q = (1-p_0)^n$.

Согласно [12, С. 677], при $p_{0eq}, P_{ud} \ll 1$ эквивалентная вероятность битовой ошибки

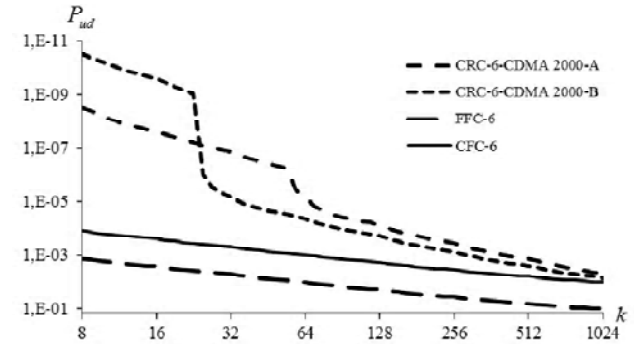
$$p_{0eq} \approx \frac{P_{ud}}{k\left(Q+P_{ud}\right)}.$$

Пример. Оценим энергетический выигрыш КФК для некогерентного приема при $p_0 = 10^{-3}$, $n = 1400$ и $r_{CFC} = 16$, $G(x) = x^{16} + x^{12} + x^5 + 1$. Тогда $k = 1384$, $\nu_{CFC} = 1384/1400 = 0,988$, а $P_{ud}(CFC, p_0) = 1,14 \cdot 10^{-5}$. Энергетический выигрыш $\Delta P = 4,25$ дБ.

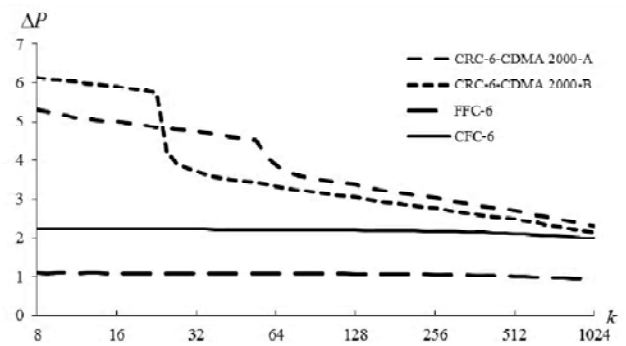
5 РЕЗУЛЬТАТЫ

На рис. 1 представлены графики зависимостей оценок вероятностей необнаруженной ошибки P_{ud} от длины информационной части блока k в результате применения КФК, ПФК и CRC-кода при $p_0 = 10^{-3}$. Оценки для CRC-кода заимствованы из работы [4], использующей результаты из [13].

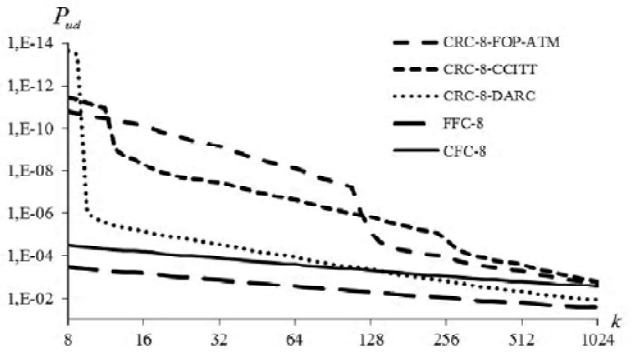
Графики зависимостей оценок энергетического выигрыша ΔP от длины информационной части блока k в результате применения КФК, ПФК и CRC-кода при $p_0 = 10^{-3}$ представлены на рис. 2.



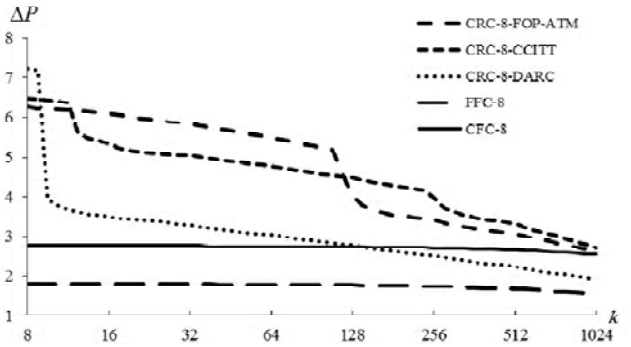
а



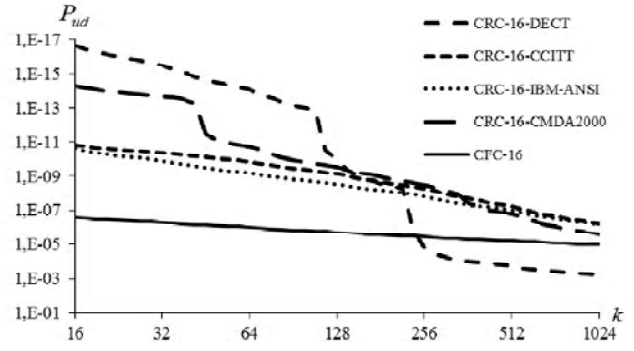
а



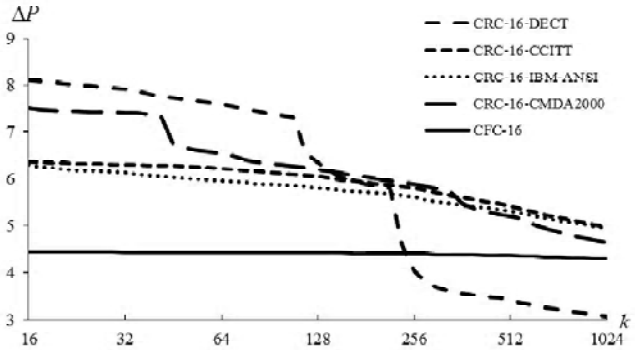
б



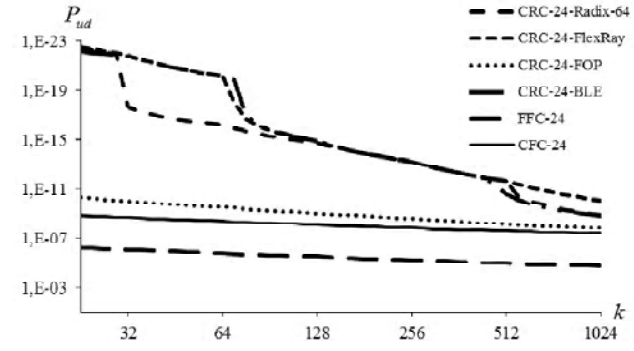
б



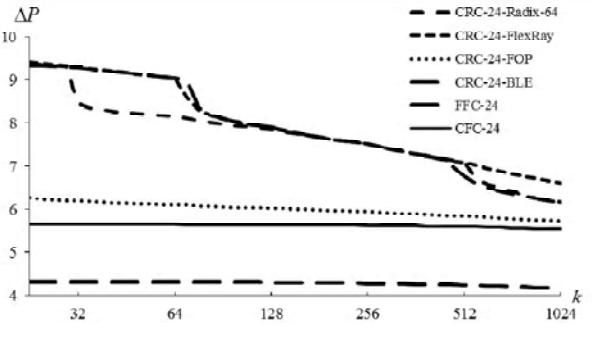
в



в



г



г

Рисунок 1 – Графики зависимостей оценок вероятностей необнаруженной ошибки от длины информационной части при $p_0 = 10^{-3}$ и а – $r = 6$; б – $r = 8$; в – $r = 16$; г – $r = 24$

Рисунок 2 – Графики зависимостей оценок энергетического выигрыша от длины информационной части при $p_0 = 10^{-3}$ и а – $r = 6$; б – $r = 8$; в – $r = 16$; г – $r = 24$

6 ОБСУЖДЕНИЕ

Рис. 1 и 2 свидетельствуют о том, что обнаруживающая способность КФК выше, чем ПФК при одинаковых скоростях кодов и кодировании символов перестановки ПФК равномерным двоичным кодом. Кроме того, длина проверочной части КФК определяется только кодовым полиномом и может принимать любое целое положительное значение (в то время как для ПФК $r_{FFC} = M \cdot (\text{entier}(\log_2 M)+1): r \in \{2;6;8;15;18;21;24;36\ldots\}$). Вместе с тем обнаруживающая способность КФК в целом уступает обнаруживающей способности циклического избыточного кода, однако для некоторых образующих полиномов CRC-кода и длины информационной части справедливо $\Delta P_{CFC} > \Delta P_{CRC}$. Так, например, $\Delta P_{CFC-8} > \Delta P_{CRC-8-DARC}$ при $k \geq 146$ ($\Delta P_{CRC-8-DARC} - \Delta P_{CFC-8} \approx -0,638$ дБ при $k = 1024$), а $\Delta P_{CFC-16} > \Delta P_{CRC-16-DECT}$ при $k \geq 243$ ($\Delta P_{CRC-16-DECT} - \Delta P_{CFC-16} \approx -1,219$ дБ при $k = 1024$). Следует отметить, что оценка вероятности необнаруженной ошибки CRC-кода определена практически точно, в то время как оценка КФК (4) может быть улучшеа. Для этого, как и для формирования используемой здесь оценки энергетического выигрыша CRC-кода, необходимо определить число ошибок веса , не обнаруживаемых КФК.

Выполним сравнительную оценку свойств помехоустойчивых кодов. Результаты анализа приведем в табл. 1.

Анализ свойств представленных кодов позволяет сформулировать следующие рекомендации по их применению: при необходимости обеспечения КЦИ при ее передаче или хранении можно использовать ПФК или КФК; причем, если не требуется самосинхронизации кода, более эффективно использовать КФК.

ВЫВОДЫ

Разработанные принципы комбинированного факториального кодирования позволяют расширить научно-техническую базу методов и средств контроля целостности информации при ее хранении и передаче.

Свойства комбинированного факториального кодирования:

– информационная часть кодового слова передается в канал связи в исходном виде, поэтому данный код не обеспечивает защиту информации от несанкционированного чтения;

– процедура формирования проверочной части кодового слова обеспечивает сцепление всех информационных символов, разрушая при этом их статистические связи, закон формирования проверочной части может быть скрыт, что в совокупности обеспечивает возможность ее использования в качестве имитовставки сообщения и совмещение функций имитозащиты и защиты от ошибок в канале связи;

– при одинаковых длине кодовой комбинации и скорости кода обнаруживающая способность КФК выше, чем ПФК, однако ниже CRC-кода;

– КФК не обладает свойством самосинхронизации.

СПИСОК ЛИТЕРАТУРЫ

1. Пат. 75935 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі коду умовних лишків / Василенко В. С., Чунарьова А. В., Василенко М. Ю, Чунарьов А. В. ; заявник та патентовласник Національний авіаційний університет. – №u2012103515; заявл. 26.03.2012; опубл. 25.12.2012, Бюл. № 24. – 4 с.
2. Пат. 75938 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі лишково-хеммінгового коду / Василенко В. С, Чунарьова А. В., Василенко М. Ю, Чунарьов А. В. ; заявник та патентовласник Національний авіаційний університет. – №u2012103518; заявл. 26.03.2012; опубл. 25.12.2012, Бюл. №24. – 4 с.
3. Горячев А. В. Обнаружение ошибок в перестановках / А. В. Горячев // Вісник СумДУ. Серія Технічні науки. – 2009. – № 4. – С. 126–134.
4. 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. – № 2, Т. 4. – (В печати).
5. Фауре Э. В. Метод формирования имитовставки на основе перестановок / Э. В. Фауре, В. В. Швыдкий, В. А. Щерба // Захист інформації. – 2014. – № 4, Т. 16. – С. 334–340. – Режим доступу: http://jrnl.nau.edu.ua/index.php/ZI/article/view/334/8755.
6. Фауре Э. В. Метод формирования воспроизводимой непредсказуемой последовательности перестановок / Э. В. Фауре, В. В. Швыдкий, А. И. Щерба // Безпека інформації. – 2014. – № 3, Т. 20. – С. 253–258. – Режим доступу: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/7552/8608.
7. Швидкий В. В. Дослідження статистичних властивостей колізій під час формування імітовставки на основі перестановок / В. В. Швидкий, В. С. Клопко // Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції, Черкаси, 14–20 березня 2016 р. – Черкаси, 2016 р. – С. 17.
8. Лидл Р. Конечные поля: В 2 т. Т. 2 / Р. Лидл, Г. Нидеррайтер ; [пер. с англ. под ред. Нечаева В. И.] – М. : Мир, 1988. – 822 с. – (Редакция литературы по математическим наукам).
9. Питерсон У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон ; [пер. с англ. под ред. Р. Л. Добрушина, С. И. Самойленко] – М. : Мир, 1976. – 590 с. – (Редакция литературы по новой технике).
10. Прокис Д. Цифровая связь / Джон Прокис ; [пер. с англ. под ред. Д.Д. Кловского]. – М. : Радио и связь, 2000. – 800 с.
11. Теплов Н. Л. Помехоустойчивость систем передачи дискретной информации / Н. Л. Теплов. – М. : Связь, 1964. – 360 с.
12. Финк Л. М. Теория передачи дискретных сообщений / Л. М. Финк. – [Изд. 2-е, перераб. и дополн.]. – М. : Советское радио, 1970. – 728 с.
13. Koopman P. Best CRC Polynomials [Електронний ресурс]. – Режим доступу: http://users.ece.cmu.edu/~koopman/crc/index.html.

Статья поступила в редакции 09.08.2016.
После доработки 18.08.2016.

Таблица 1 – Свойства помехоустойчивых кодов

Код	Систематический	Помехоустойчивый	Криптостойкий	Имитостойкий	Самосинхронизирующийся
ПФК	+	+	–	+	+
КФК	+	+	–	+	–
CRC	+	+	–	–	–

Фауре Е. В.[1], Швидкий В. В.[2], Щерба В. О.[3]

[1]Канд. техн. наук, доцент, докторант, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна

[2]Канд. техн. наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна

[3]Ст. викладач кафедри прикладної математики Черкаського державного технологічного університету, Черкаси, Україна

КОМБІНОВАНЕ ФАКТОРІАЛЬНЕ КОДУВАННЯ ТА ЙОГО ВЛАСТИВОСТІ

У роботі запропоновано метод комбінованого факторіального кодування даних, спрямований на забезпечення контролю цілісності інформації, який передбачає комплексний захист від нав'язування хибних даних (імітозахист) і помилок у каналі зв'язку. Основна ідея запропонованого методу кодування полягає в поєднанні процедур повного факторіального кодування, що використовує перестановку в якості перевірної частини кодового слова, і циклічного надлишкового кодування (CRC). При цьому перевірна частина кодового слова комбінованого факторіального коду формується шляхом обчислення залишку від ділення перевірної частини кодового слова повного факторіального коду, представленої у вигляді многочлена, на кодовий поліном CRC-коду. Визначено основні властивості комбінованого факторіального коду, виконано оцінку достовірності передавання, крипто- й імітостійкості. Виконано порівняльний аналіз виявляючої здатності (ймовірності невиявленої кодом помилки) й енергетичного виграшу для повного та комбінованого факторіального кодування за умови незалежності помилок, що виникають у каналі зв'язку, та їх біноміального розподілу. Визначено шляхи поліпшення представленої оцінки ймовірності невиявленої факторіальним кодом помилки. Надано рекомендації щодо застосування повного і комбінованого факторіального кодування.

Ключові слова: факторіальний код, перестановка, контроль цілісності інформації, завадостійке кодування, достовірність передавання, стійкість.

Faure E. V.[1], Shvydkyi V. V.[2], Shcherba V. O.[3]

[1]PhD, Associate Professor, Post-Doctoral Associate, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine

[2]PhD, Associate Professor, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine

[3]Senior Lecturer of Department of Applied mathematics, Cherkasy State Technological University, Cherkasy, Ukraine

COMBINED FACTORIAL CODING AND ITS PROPERTIES

In this paper the authors propose a method of combined factorial data coding directed to the information integrity control that provides a comprehensive protection against intentional alteration of data and communication channel errors. The basic idea of the proposed method consists in combining of procedures of full factorial coding that uses a permutation as a codeword check value, and a cyclic redundancy coding (CRC). In this case a codeword check value of combined factorial code is generated from a codeword check value of full factorial code represented by a polynomial, by the CRC polynomial modulo. The basic properties of the combined factorial code are defined. The assessments of transmission reliability, cryptographic strength and strength against intentional alteration of data are evaluated. A comparative analysis of detecting ability (probability of an error undetected by the code) and energy gain for the full and combined factorial coding is done on the condition of independence of errors that appear in communication channel and their binomial distribution. The ways of improvement of the presented assessment of the probability of an undetected by factorial code error are defined. Recommendations for the use of full and combined factorial coding are given.

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

REFERENCES

1. Vasylenko V. S, Chunar'ova A. V., Vasylenko M. Ju, Chunar'ov A. V. Pat. 75935 Ukrai'na, MPK N03M13/31 (2006.01). Sposib zabezpechennja cilisnosti informacii' na bazi kodu umovnyh lyshkiv ; zajavnyk ta patentovlasnyk Nacional'nyj aviacijnyj universytet. №u2012103515; zajavl. 26.03.2012; opubl. 25.12.2012, Bjul. №24, 4 p.
2. Vasylenko V. S, Chunar'ova A. V., Vasylenko M. Ju, Chunar'ov A. V. Pat. 75938 Ukrai'na, MPK N03M13/31 (2006.01). Sposib zabezpechennja cilisnosti informacii' na bazi lyshkovo-hemmingovogo kodu ; zajavnyk ta patentovlasnyk Nacional'nyj aviacijnyj universytet. – №u2012103518; zajavl. 26.03.2012; opubl. 25.12.2012, Bjul. №24, 4 p.
3. Goryachev A.V. Obnaruzhenie oshibok v perestanovkax, *Visnyk SumDU. Serija Tehnichni nauky*, 2009, No. 4, pp. 126–134.
4. Faure E'. V., Shvydkij V. V., Shherba A. I. Kontrol' celostnosti informacii na osnove faktorial'noj sistemy schisleniya, *Journal of Qafqaz University. Mathematics and computer science*, 2016, No. 2, Vol. 4. (V pechati).
5. Faure E'. V., Shvydkij V. V., Shherba V. A. Metod formirovaniya imitovstavki na osnove perestanovok, Zaxist informacií, 2014, No. 4, Vol. 16, pp. 334–340. Access mode: http://jrnl.nau.edu.ua/index.php/ZI/article/view/334/8755.
6. Faure E'. V., Shvydkij V. V., Shherba A. I. Metod formirovaniya vosproizvodimoj nepredskazuemoj posledovatel'nosti perestanovok, *Bezpeka informacií*, 2014, No. 3, Vol. 20, pp. 253–258. Access mode: http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/7552/8608.
7. Shvydkyj V. V., Klopko V. S. Doslidzhennja statystychnyh vlastyvostej kolizij pid chas formuvannja imitovstavky na osnovi perestanovok, *Avtomatyzacija ta komp'juterno-integrovani tehnologii' u vyrobnyctvi ta osviti: stan, dosjagnennja, perspektyvy rozvytku: materialy Vseukrai'ns'koi' naukovo-praktychnoi' Internet-konferencii', Cherkasy, 14–20 bereznja 2016 r.* Cherkasy, 2016 r, P. 17.
8. Lidl R., Niderrajter G. ; [per. s angl. pod red. Nechaeva V. I.] Konechnye polya: V 2 t. T. 2. Moscow, Mir, 1988, 822 p. (Redakciya literatury po matematicheskim naukam).
9. Piterson U., Ue'ldon E'.; [per. s angl. pod red. R. L. Dobrushina, S. I. Samojlenko] Kody, ispravlyayushhie oshibki. Moscow, Mir, 1976, 590 p. (Redakciya literatury po novoj texnike).
10. Prokis D. [per. s angl. pod red. D. D. Klovskogo]. Cifrovaya svyaz'. Moscow, Radio i svyaz', 2000, 800 p.
11. Teplov N. L. Pomexoustojchivost' sistem peredachi diskretnoj informacii. Moscow, Svyaz', 1964, 360 p.
12. Fink L. M. Teoriya peredachi diskretnyx soobshhenij. [Izd. 2-e, pererab. i dopoln.]. Moscow, Sovetskoe radio, 1970, 728 p.
13. Koopman P. Best CRC Polynomials [Electronic resource]. Access mode: http://users.ece.cmu.edu/~koopman/crc/index.html.