НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2018 Том 18 № 6 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2018 Vol. 18 No 6 ISSN 2226-1494 http://ntv.ifmo.ru/en
УНИВЕРСИТЕТ ИТМО

УДК 004.052.42

СОЗДАНИЕ НАДЕЖНЫХ КОДОВ НА ОСНОВЕ БЕНТ-ФУНКЦИЙ И ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ

А.Б. Левина[a], Г.А. Ряскин[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: levina@cit.ifmo.ru

Информация о статье
Поступила в редакцию 05.05.18, принята к печати 18.09.18
doi: 10.17586/2226-1494-2018-18-6-1008-1015
Язык статьи – русский

Ссылка для цитирования: Левина А.Б., Ряскин Г.А. Создание надежных кодов на основе бент-функций и вейвлет-преобразований // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 6. С. 1008–1015. doi: 10.17586/2226-1494-2018-18-6-1008-1015

Аннотация

Предмет исследования. Показана возможность применения вейвлет-преобразований и бент-функций при построении нелинейных надежных кодов. Использование вейвлетных разложений позволяет создать множество различающихся между собой конструкций надежных кодов. **Метод.** Для повышения нелинейных свойств надежных кодов применены бент-функции, которые обеспечивают максимальную нелинейность булевых функций. Тем самым повышается вероятность обнаружения ошибки в канале передачи данных. Предложены разные конструкции помехоустойчивых кодов на основе вейвлет-разложений и бент-функций. Различие конструкций состоит в использовании разных сеток для вейвлет-преобразования: сетка со статичными значениями или сетка на основе входящего информационного слова. Линейные и нелинейные коды сравниваются с разработанными кодами. **Основные результаты.** Разработаны конструкции надежных кодов, обладающие лучшими, по сравнению с существующими конструкциями, характеристиками. Максимальная вероятность маскировки ошибки для разработанных конструкций равняется 0,46875, что является лучшим результатом по сравнению с надежным кодом Кердока. Такой результат позволяет обеспечить качественную защиту от атак по сторонним каналам. **Практическая значимость.** Предложенные конструкции кодов можно применять в задачах обеспечения безопасности информации.

Ключевые слова
помехоустойчивое кодирование, бент-функции, вейвлет преобразование, сплайн-вейвлетное преобразование, надежные коды, нелинейные функции

ROBUST CODES CREATION BASED ON BENT-FUNCTIONS AND WAVELET TRANSFORMATION

A.B. Levina[a], G.A. Ryaskin[a]

[a]ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: levina@cit.ifmo.ru

Article info
Received 05.05.18, accepted 18.09.18
doi: 10.17586/2226-1494-2018-18-6-1008-1015
Article in Russian

For citation: Levina A.B., Ryaskin G.A. Robust codes creation based on bent-functions and wavelet transformation. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 6, pp. 1008–1015 (in Russian). doi: 10.17586/2226-1494-2018-18-6-1008-1015

Abstract

Subject of Research. This paper presents an application of wavelet transformation and bent-functions in the creation of non-linear robust codes. The usage of wavelet decompositions gives the possibility to create a large number of different designs of robust codes. **Method.** To improve the non-linear properties of robust codes, bent-functions were used in the construction. Thereby the maximum non-linearity of functions is ensured increasing the probability of detecting an error in the data channel. Different designs of codes based on wavelet transform and bent-functions are developed. The difference of constructions consists in the usage of different grids for wavelet transformation: a grid with static values, or a grid based on an incoming information word. The existing linear and non-linear codes were analyzed, their comparison with the developed codes was performed. **Main Results.** The developed designs are robust codes and have higher characteristics compared to existing designs of robust codes. The maximum probability of the error masking for the developed designs is 0.46875. This

result is a better one compared to the existing reliable Kerdock code and enables better protection against side-channel attacks. **Practical Relevance.** These code designs can be used in the tasks to ensure the security of information transmitted.

Keywords
error correcting codes, bent-functions, wavelet transformation, spline-wavelet transformation, robust codes, nonlinear functions

Введение

Одним из эффективных способов обеспечения высокой достоверности информации при передаче, хранении и обработке является использование теории кодирования и помехоустойчивых кодов. Целью кодов, исправляющих ошибки, является обеспечение цифровой связи по каналу таким образом, чтобы ошибки в передаче могли быть обнаружены и исправлены приемником [1, 2]. Злоумышленник, воздействуя на аппаратную составляющую криптографического устройства, может изменять и искажать передаваемую по каналу информацию. Этот тип атаки называется атакой по ошибкам вычислений [3]. Для защиты от данного типа атак используют надежные коды, строящиеся на нелинейных функциях. Наибольший интерес вызывают функции, для которых свойство нелинейности максимально – бент-функции [4, 5].

В настоящей работе представлены надежные коды, построенные на основе вейвлетных разложений и бент-функций; рассмотрены разработанные конструкции помехоустойчивых кодов; доказана надежность разработанных кодов при защите от атак по сторонним каналам; сравниваются характеристики разработанных конструкций с характеристиками существующих линейных и нелинейных кодов. Разработанные кодовые конструкции обладают более низкими значениями максимальной вероятности маскировки ошибки и более низким временем кодирования информации среди рассмотренных.

Теория кодирования

Ошибки в информационном канале могут возникать как из-за помех, так и из-за действий злоумышленника. Основным средством защиты от искажений является использование помехоустойчивого кодирования [1, 2].

Кодом называется совокупность знаков, а также система правил, позволяющая представлять информацию в виде набора таких знаков [2]; кодовым словом является любой ряд допустимых знаков. Идея помехоустойчивого кодирования состоит в том, что допустимы лишь некоторые из возможных кодовых слов. Множество комбинаций разбивается на подмножества разрешенных (входящих в код) и запрещенных комбинаций. Если принятое кодовое слово принадлежит подмножеству запрещенных комбинаций, значит либо при передаче сообщения по каналу, либо при обработке его в устройстве была допущена ошибка.

Основной задачей теории кодирования является обеспечение высокой достоверности и надежности передаваемых данных за счет применения устройств кодирования/декодирования в составе системы передачи информации. Для решения этой задачи применяются различные типы помехоустойчивых линейных и нелинейных кодов [2].

Помехоустойчивые коды изначально создавались для борьбы с искажениями на физическом уровне сетей, в настоящее время они находят применение и в задачах обеспечения безопасности, защиты от атак по сторонним каналам, а именно атак по ошибкам вычислений. В такой модели подразумевается, что злоумышленник способен изменять значение некоторого абстрактного устройства хранения данных, не имея доступа к чтению этих данных. Применительно к защищенной памяти алгебраическая манипуляция представляет собой некоторую аддитивную ошибку, воздействующую на содержимое памяти. Конфигурация ошибок в данном случае абсолютно непредсказуема и зависит от возможностей злоумышленника и метода возбуждения помех. Для защиты от атак по сторонним каналам разработаны надежные коды, которые обнаруживают любую конфигурацию ошибок с заданной вероятностью [6].

Построение надежных кодов на бент-функциях

Код $C \subseteq GF\left(2^n\right)$ называется R-надежным, если область пересечения кода C и любого его дополнения $\tilde{C} = \left\{ \tilde{x} \,|\, \tilde{x} = x + e, x \in C, e \in GF\left(2^n\right), e \neq 0 \right\}$ ограничена сверху значением R: $R = \max\limits_{e \in GF\left(2^n\right)} \left| \left\{ x \,|\, x \in C, x + e \in C \right\} \right|$, где «+» – покомпонентное сложение по модулю два, x – кодовое слово, e – ошибка [7, 8].

Пусть $M = |C|$ – число кодовых слов в C. По определению R-надежного кода, существует не более R кодовых слов, которые могут быть не обнаружены для любой фиксированной ошибки e. Таким образом, вероятность маскировки ошибки $Q(e)$ может быть определена как:

$$Q(e) = \frac{\left| \left\{ x \,|\, x \in C, x + e \in C \right\} \right|}{M}. \quad (1)$$

Надежный код не имеет необнаруживаемых ошибок. Для любого *R*-надежного кода наихудшая вероятность маскировки любой ошибки (1) не больше *R/M*, если считать все появления кодовых слов надежного кода равновероятными. Злоумышленник может внедрять ошибку с максимально надежной маскировкой, вероятность обнаружения которой ниже, чем вероятность обнаружения всех остальных ошибок. *R* является важным параметром для защиты от атак по сторонним каналам, и чем он меньше, тем более надежен код.

Рассмотрим несколько известных конструкций надежных кодов.

Квадратичный систематический код (Код Кердока)

Пусть $x=\left(x_1,x_2,\ldots,x_{2s},x_{2s+1}\right), s\geq 1$. Вектор $\mathbf{x}\in GF\left(2^{(2s+1)}\right)$ принадлежит коду тогда и только тогда, когда $x_{2s+1}=x_1*x_2+x_3*x_4+\ldots+x_{2s-1}*x_{2s}$, где «*» – произведение в поле $GF\left(2\right)$.

Надежный повторяющийся код. Пусть $\mathbf{x}=\left(x_1,x_2\right), x_1,x_2\in GF\left(2^r\right)$. Надежный повторяющийся код C содержит все векторы $\mathbf{x}\in GF\left(2^{2r}\right)$, которые удовлетворяют соотношению $x_1^3=x_2$, где все вычисления происходят в поле $GF\left(2^r\right)$. Длина полученного надежного кода $n=2r,\ M=2^r$.

Бент-функции. Существует тесная взаимосвязь между характеристикой кода, нелинейностью и нелинейными функциями, так как все надежные коды – нелинейны. Свойства надежного кода зависят от нелинейности шифрующей функции кода.

Задача построения булевых функций, обладающих нелинейными свойствами, возникает во многих областях, и часто наибольший интерес вызывают те функции, для которых эти свойства экстремальны. Такие булевы функции называются бент-функциями. Впервые они начали исследоваться в 1960-х гг. в связи с криптографическими приложениями. Бент-функция крайне плохо аппроксимируется аффинными функциями [9].

Бент-функция – булева функция с четным числом переменных, для которой расстояние Хэмминга от множества аффинных булевых функций с тем же числом переменных максимально [10].

Нелинейностью функции f называется расстояние от f до класса аффинных функций. Будем обозначать нелинейность функции f через N_f:

$$N_f=d\left(f,A(n)\right)=\min_{g\in A(n)} d\left(f,g\right),$$

где $A(n)$ – класс линейных функций.

Мера нелинейности является важной характеристикой булевой функции. Линейность часто свидетельствуют о простой (в определенном смысле) структуре функции и, как правило, дает много дополнительной информации о свойствах данной функции.

Простейшие свойства бент-функций [9]:

1) бент-функции существуют только для четных n;
2) бент-функции не уравновешены;
3) бент-функции статистически зависят от всех своих аргументов;
4) пусть *f* является бент-функцией, а h принадлежит классу линейных функций. Тогда $f\oplus h$ принадлежит классу бент-функций;
5) пусть $f\in P_2(n), g\in P_2(m)$ – функции от непересекающихся множеств переменных. Тогда $f\oplus g$ – бент-функция, если и только если f и g – бент-функции.

Приведем примеры бент-функций от разного числа переменных:

– для $n=2$

$$f\left(x_0,x_1\right)=x_0x_1;$$

– для $n=4$

$$f\left(x_0,x_1,x_2,x_3\right)=x_0x_1+x_2x_3,$$

$$f\left(x_0,x_1,x_2,x_3\right)=x_0x_1+x_2x_3+x_2+x_3.$$

С точки зрения криптографии к важным критериям, которым должна удовлетворять булева функция f от n переменных, относятся [11–13]:

– уравновешенность – функция *f* принимает значения 0 и 1 одинаково часто;
– критерий распространения $PC(k)$ порядка *k* – для любого ненулевого вектора $\mathbf{y}\in Z_2^n$ веса не более *k*, функция $f\left(x+y\right)+f\left(x\right)$ уравновешена;

– максимальная нелинейность – функция f такова, что значение ее нелинейности N_f максимально.

Бент-функция отвечает критериям распространения и максимальной нелинейности, что позволяет ей обнаруживать все ошибки в канале и обладать равномерной вероятностью обнаружения ошибок.

Построение булевых функций на вейвлетных разложениях

В настоящее время отмечается интерес к аппаратам локальной аппроксимации, и в частности к сплайнам и вейвлетам [14–16], вследствие широкого применения последних при различного вида обработке числовых потоков. Основная задача такой обработки – сокращение объема числового потока за счет выявления и отбрасывания несущественных (с той или иной точки зрения) частей.

Основная идея вейвлетного разложения (декомпозиции) заключается в том, что информационный поток можно разделить на основной и уточняющий (дополнительный). Основная задача такой обработки – сокращение объема потока за счет выявления и отбрасывания несущественных (с той или иной точки зрения) частей. В каждом отдельном случае специалист определяет, какая информация является уточняющей, а какая основной, и выбирает алгоритмы декомпозиции и реконструкции. В настоящей работе потоки получаются на основе локальных сплайнов, а именно на сплайн-вейвлетном разложении [16].

Для сплайн-вейвлетного преобразования помимо самого информационного потока необходима сетка с одинаковым шагом, состоящая из элементов того же поля, что и исходный поток. К тому же нужно определить номер элемента изначального информационного потока, который будет из него удаляться.

Пусть X – неравномерная сетка, состоящая из элементов $X = \{x_j\}_{j\in Z}$, где Z – множество целых чисел. Сплайны первого порядка на сетке X определяются следующим образом:

$\omega_j(t) = (t - x_j)(x_{j+1} - x_j)^{-1}$ при $t \in [x_j, x_{j+1})$,

$\omega_j(t) = (t - x_j)(x_{j+1} - x_j)^{-1}$ при $t \in [x_{j+1}, x_{j+2})$,

$\omega_j(t) = 0$ при $t \notin [x_j, x_{j+2})$.

В процессе вейвлетных разложений из сетки X удаляется некий элемент x_k, после такого преобразования получается новая сетка $\tilde{X}$, на основе которой строятся новые сплайны $\tilde{\omega}_j(t)$. Новые и старые сплайны связаны между собой. Эта взаимосвязь элементов $\tilde{\omega}_j(t)$ и $\omega_j(t)$ может быть показана с помощью формул, где ε – удаляемый из сетки X элемент:

$\tilde{x}_j = x_j$, если $j \le k-1$, $\tilde{x}_j = x_{j+1}$, если $j \ge k, \varepsilon = x_k$.

Новые сплайны $\tilde{\omega}_j(t)$ зависят от старых $\omega_j(t)$ следующим образом:

$\tilde{\omega}_j(t) = \omega_j(t)$, если $j \le k-3$,

$\tilde{\omega}_j(t) = \omega_{j+1}(t)$, если $j \ge k$,

$\tilde{\omega}_{k-2}(t) = \omega_{k-2}(t) + \tilde{\omega}_{k-2}(x_k)\omega_{k-1}(t)$,

$\tilde{\omega}_{k-1}(t) = \omega_{k-1}(t) + \tilde{\omega}_{k-1}(x_k)\omega_{k-1}(t)$.

Таким же образом старые сплайны могут быть выражены через новые. Представленная выше взаимосвязь элементов старых и новых сплайнов позволяет нам определить формулы декомпозиции и реконструкции.

Формулы декомпозиции сплайн-вейвлетных разложений первого порядка имеют вид:

$a_i = c_i$ при $i \le k-2$, $a_i = c_{i+1}$ при $i \ge k-1$, $b_j = 0$ при $j \ne k-2$;

$$b_{k-1} = c_{k-1} - (x_{k+1} - x_k)(x_{k+1} - x_{k-1})^{-1} c_{k-2} - (x_k - x_{k-1})(x_{k+1} - x_{k-1})^{-1} c_k. \quad (2)$$

Формулы реконструкции сплайн-вейвлетных разложений первого порядка имеют вид:

$c_j = a_j$ при $j \le k-2$, $c_j = a_{j-1}$ при $i \ge k$,

$$c_{k-1} = b_{k-1} + (x_{k+1} - x_k)(x_{k+1} - x_{k-1})^{-1} a_{k-2} + (x_k - x_{k-1})(x_{k+1} - x_{k-1})^{-1} a_{k-1}. \quad (3)$$

Пусть $\Omega(X)$ – пространство, которое является линейной оболочкой функции ω_j: $\Omega(X) = \{u | u = \sum c_j \omega_j, c_j \in R\}$, ω_j: тогда $\Omega(X)$ – пространство сплайнов первого порядка на сетке

X, а ω_j – образующая пространства $\Omega(X)$.

После удаления элемента из сетки X получается пространство сплайнов первого порядка $\Omega(\tilde{X})$ на сетке $\tilde{X}$:

$$\Omega(\tilde{X}) = \{\tilde{u} | \tilde{u} = \sum \tilde{a}_j \tilde{\omega}_j, \tilde{a}_j \in R\}.$$

Для двух описанных пространств справедливо $\Omega(\tilde{X}) \subset \Omega(X)$. Пространством вейвлетов называется пространство W_k; $\Omega(X) = \Omega(\tilde{X}) + W_k$ называется сплайн-вейвлетным разложением пространства $\Omega(X)$.

Функции декомпозиции и реконструкции можно использовать для построения булевых функций, где все вычисления происходят в поле $GF(2)$. Если задать сетку статичным кодовым словом, то формула декомпозиции будет линейной, если на основе входящего информационного слова – нелинейной.

Создание надежного кода на основе сплайн-вейвлетных разложений и бент-функций

С помощью сплайн-вейвлетных разложений можно создать множество различных кодовых конструкций.

Сплайн-вейвлетный код. Пусть $c = \{c_1, c_2, \ldots, c_{n-1}, c_n\}$ – кодовое слово некоторого разделяемого кода (n,k). Тогда $\{c_1, c_2, \ldots, c_{k-1}, c_k\}$ является информационной частью этого кода, а $\{c_{k+1}, \ldots, c_n\}$ – проверочной. В данной конструкции для всего кода выбирается сетка $x = \{x_1, x_2, \ldots, x_{k-1}, x_k\}$, на усмотрение программиста удаляются любые элементы, число удаляемых элементов $(n-k)/2$. Количество символов строго четное и кратное 4, $\frac{k}{n} = \frac{2}{3}$. Удаляемые элементы будем обозначать множеством $z = \{z_1, \ldots, z_{(n-k)/2}\}$, вейвлетные элементы $b = \{b_1, \ldots, b_{(n-k)/2}\}$.

Конструкция 1. Сплайн-вейвлетный код со статичной сеткой.

Пусть $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ – вектор поля $GF(2^n)$, $1 \le i \le n$, принадлежащий коду, если

$$c_{k+j} = c_{z_i} + c_{z_i+1} + \left(x_{z_i+2} + x_{z_i-1}\right)\left(x_{z_i+2} + x_{z_i}\right)^{-1}(c_{z_i-1} + c_{z_i+1}),$$

$$b_{z_i} = c_{z_i} + c_{z_i+1} + \left(x_{z_i+2} + x_{z_i-1}\right)\left(x_{z_i+2} + x_{z_i}\right)^{-1}(c_{z_i-1} + c_{z_i+1}).$$

При четном z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \ldots + b_{z_i} * c_{z_i-1} + \ldots + c_{n-1} * c_n.$$

При нечетном z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \ldots + b_{z_i} * c_{z_i+1} + \ldots + c_{n-1} * c_n,$$

где $1 \le j \le (n-k)/2$, k – количество проверочных символов в коде, $z_i \in z$, «+» – сложение по модулю 2, соответствует операции XOR, «*» – произведение в поле $GF(2)$.

Сплайн-вейвлетный код с сеткой, основанной на кодовом слове. Пусть $c = \{c_1, c_2, \ldots, c_{n-1}, c_n\}$ обозначает кодовое слово некоторого разделяемого кода (n,k). Тогда $\{c_1, c_2, \ldots, c_{k-1}, c_k\}$ является информационной частью этого кода, а $\{c_{k+1}, \ldots, c_n\}$ – проверочной. В данной конструкции для всего кода выбирается сетка $x = \{x_1, x_2, \ldots, x_{k-1}, x_k\}$, основанная на информационной части кодового слова и зависящая от номера удаляемого элемента. Шаг сетки равняется сдвигу относительно номера удаляемого элемента, т.е. $x_i = c_{(i-z_i)(mod\ n-r)}$.

Конструкция 2. Сплайн-вейвлетный код с сеткой, основанной на информационной части кодирования.

Пусть $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ – вектор поля $GF(2^n)$, $1 \le i \le n$, принадлежащий коду, если

$$c_{k+j} = c_{z_i} + c_{z_i+1} + \left(c_2 + c_{-1(\mathrm{mod}\ n)}\right)\left(c_2 + c_0\right)^{-1}(c_{z_i-1} + c_{z_i+1}),$$

$$b_{z_i} = c_{z_i} + c_{z_i+1} + \left(c_2 + c_{-1(\mathrm{mod}\, n)}\right)\left(c_2 + c_0\right)^{-1}(c_{z_i-1} + c_{z_i+1}).$$

При четном z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \ldots + b_{z_i} * c_{z_i-1} + \ldots + c_{n-1} * c_n .$$

При нечетном z_i:

$$c_{k+j+(n-k)/2} = c_1 * c_2 + \ldots + b_{z_i} * c_{z_i+1} + \ldots + c_{n-1} * c_n ,$$

где $1 \le j \le (n-k)/2$, k – количество проверочных символов в коде, $z_i \in z$, «+» – сложение по модулю 2, соответствует операции XOR, «*» – произведение в поле $GF(2)$.

Сравнение разработанных конструкций с существующими решениями

Сравним построенные коды с линейным и надежным кодами той же длины. Одними из наиболее важных критериев для определения надежности кода являются средняя вероятность обнаружения ошибки заданной кратности и максимальная вероятность маскировки ошибки.

Необходимо, чтобы коды обеспечивали равновероятную защиту от всех ошибок, не имели необнаруживаемых ошибок и имели наименьшую максимальную вероятность маскировки ошибки:

$$Q(e) = \max_{e \in Z_2^n} \frac{\left|\{x \mid x \in C, x + e \in C\}\right|}{M} . \qquad (4)$$

Для вычисления элемента $c_{k+j+(n-k)/2}$ используются бент-функции от элементов информационного слова и вейвлетного элемента. Элементы функции c_{k+j} вычисляются по формуле декомпозиции (2). Составим примеры для разных конструкций кодов. Число информационных символов $k = 8$, избыточных символов – $r = 4$. В качестве метода сравнения надежности кодов используется метод расчета средней вероятности обнаружения ошибки, максимальная вероятность маскировки ошибки (4), а также время, потраченное на операцию кодирования.

Номер удаляемого элемента возьмем равным трем (это ни на что не влияет). Удаления элементов производиться не будет, дополнительный поток будет использоваться в избыточных символах.

Формулы декомпозиции (2) и реконструкции (3) при удалении элемента под номером $k-1$ имеют вид:

$$b_{k-1} = c_{k-1} - \left(x_{k+1} - x_k\right)\left(x_{k+1} - x_{k-1}\right)^{-1} c_{k-2} - \left(x_k - x_{k-1}\right)\left(x_{k+1} - x_{k-1}\right)^{-1} c_k ,$$

$$c_{k-1} = b_{k-1} + \left(x_{k+1} - x_k\right)\left(x_{k+1} - x_{k-1}\right)^{-1} a_{k-2} + \left(x_k - x_{k-1}\right)\left(x_{k+1} - x_{k-1}\right)^{-1} a_{k-1} .$$

Преобразуем формулы, в результате при удаления элемента k, при условии, что $x_{k+2} \ne x_k$:

$$b_k = c_k - c_{k+1} - \left(x_{k+2} - x_{k-1}\right)\left(x_{k+2} - x_k\right)^{-1}(c_{k-1} - c_{k+1}),$$

$$c_k = b_k + c_{k+1} - \left(x_{k+2} - x_{k-1}\right)\left(x_{k+2} - x_k\right)^{-1}(c_{k-1} - c_{k+1}).$$

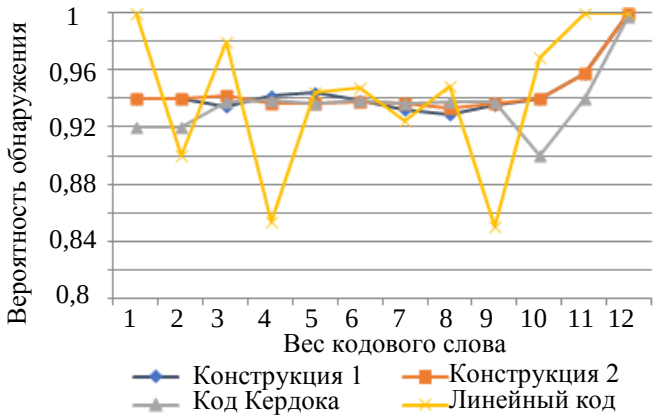
Остальные элементы множества c сдвигаются, но не меняются, а значит, можно использовать элементы исходной последовательности.

В качестве бент-функции для помехоустойчивого кода возьмем $f = c_1c_2 + c_3c_4 + c_5c_6 + c_7c_8$. При удалении третьего элемента заменим c_3 на элемент дополнительного потока b, функция принимает вид $f = c_1c_2 + bc_4 + c_5c_6 + c_7c_8$. В зависимости от значений сетки функция принимает вид $f = c_1c_2 + c_3c_4 + c_4 + c_5c_6 + c_7c_8$ или $f = c_1c_2 + c_3c_4 + c_4c_2 + c_5c_6 + c_7c_8$, или $f = c_1c_2 + c_3c_4 + c_5c_6 + c_7c_8$. Сложение идет по модулю 2, т.е. соответствует операции XOR. Будем использовать полученное значение функции f в качестве избыточной составляющей r_0, а избыточную составляющую $r_1 = b$ – в качестве элемента дополнительного потока. Сравним этот код с кодом, построенным на неравномерной сетке, с линейным кодом и надежным кодом той же длины.

Избыточные символы для линейного кода $r_0 = c_1 + c_2$, $r_1 = c_3 + c_4$, $r_2 = c_5 + c_6$, $r_3 = c_7 + c_8$; для нелинейного (код Кердока) $r_0 = c_1c_2 + c_3c_4 + c_5c_6 + c_7c_8$, $r_1 = c_1c_3 + c_2c_4 + c_6c_8 + c_5c_7$, $r_2 = c_1c_5 + c_2c_6 + c_3c_7 + c_4c_8$, $r_3 = c_1c_3 + c_2c_4 + c_6c_8 + c_5c_7$.

Построим график вероятностей обнаружения ошибки для надежного сплайн-вейвлетного кода со статичной сеткой – конструкция 1, для сплайн-вейвлетного кода с сеткой, основанной на кодовом слове –

конструкция 2, для надежного кода Кердока и линейного кода график одинаков для всех значений сетки (см. рисунок).



Вероятность обнаружения ошибок для разных конструкций кодов

Средняя вероятность обнаружения ошибки несущественно различается для конструкций 1, 2 и надежного кода Кердока. В случае линейного кода вероятность неравномерна, что делает этот код уязвимым для атак по сторонним каналам, злоумышленник может внедрять ошибку определенного веса, для которой вероятность обнаружения будет минимальной.

Максимальная вероятность маскировки ошибки этих кодов по формуле (4) сравнивается в табл. 1, время, затраченное на кодирование, – в табл. 2.

Время, затраченное на кодирование, считалось программой, написанной на языке C++, опыты проводились в операционной системе Windows 8.1, процессор Intel Core i7-4700HQ, программная среда Microsoft Visual Studia 2013. Поскольку на точность измерения системного времени влияют различные факторы, вносящие искажения, вычислялось среднее время трех последовательных измерений.

Код	Максимальная вероятность маскировки ошибки, $Q(e)$
Конструкция 1	0,5
Надежный код Кердока	0,5
Линейный код	1
Конструкция 2	0,468750

Таблица 1. Максимальная вероятность маскировки ошибки для разных конструкций кодов

Код	Время, с			Среднее значение времени, с
	1-й блок	2-й блок	3-й блок	
Конструкция 1	0,043	0,045	0,047	0,045
Надежный код Кердока	0,066	0,068	0,067	0,067
Линейный код	0,035	0,037	0,039	0,037
Конструкция 2	0,065	0,068	0,068	0,067

Таблица 2. Сравнение времени кодирования блока данных разных конструкций кодов

У конструкции 2 наиболее низкое значение максимальной вероятности маскировки, и потому это – наиболее надежный код с точки зрения защиты от атак по сторонним каналам. У конструкции 1 самые низкие показатели времени, затраченного на кодирование.

Заключение

Представленные коды являются надежными, они обладают рядом преимуществ по сравнению с существующими. Разработанные кодовые конструкции обладают наиболее высокими максимальной вероятностью маскировки ошибки и скоростью кодирования информации среди рассмотренных кодовых конструкций. Разработанные конструкции кодов можно применять в задачах обеспечения безопасности информации, передающейся по каналам связи, а именно для защиты от атак по сторонним каналам.

Литература

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М.: Техносфера, 2005. 320 с.
2. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов,

References

1. Morelos-Zaragoza R.H. *The Art of Error Correcting Coding*. 2nd ed. Wiley, 2006, 269 p.
2. MacWilliams F.J., Sloane N.J.A. *The Theory of Error-Correcting Codes*. Amsterdam-Oxford, North-Holland

исправляющих ошибки. М.: Связь, 1979. 745 с.
3. Атака по сторонним каналам [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/?oldid=84074315, свободный (дата обращения: 20.05.2017).
4. Akdemir K.D., Wang Z., Karpovsky M.G., Sunar B. Design of cryptographic devices resilient to fault injection attacks using nonlinear robust codes / In: Joye M., Tunstall M. (eds) Fault Analysis in Cryptography. Springer, 2011. P. 171–199. doi: 10.1007/978-3-642-29656-7_11
5. Carlet C. Partially-bent functions // Designs, Codes and Cryptography. 1993. V. 3. N 2. P. 135–145. doi: 10.1007/bf01388412
6. Karpovsky M.G., Wang Z. Design of strongly secure communication and computation channels by nonlinear error detecting codes // IEEE Transactions on Computers. 2014. V. 63. N 11. P. 2716–2728. doi: 10.1109/TC.2013.146
7. Karpovsky M.G., Kulikowski K., Wang Z. Robust error detection in communication and computation channels // Proc. Int. Workshop on Spectral Techniques. 2007.
8. Левина А.Б., Таранов С.В. Построение линейных и надежных кодов на основе коэффициентов масштабирующих функций вейвлетных преобразований // Сибирский журнал индустриальной математики. 2015. Т. 18. № 3(63). С. 49–56. doi: 10.17377/SIBJIM.2015.18.305
9. Токарева Н.Н. Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. Т. 2. № 1. С. 15–37.
10. Панкратова И.А. Булевы функции в криптографии. Томск: ТГУ, 2014. 88 с.
11. Токарева Н.Н. Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken: LAP, 2011. 180 с.
12. Смарт Н. Криптография. М: Техносфера, 2005. 525 с.
13. Carlet C. Boolean functions for cryptography and error correcting codes / In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Eds. P. Hammer, Y. Crama. Cambridge, 2007. P. 257–397. doi: 10.1017/cbo9780511780448.011
14. Демьянович Ю.К., Ходаковский В.А. Введение в теорию вэйвлетов. СПб: ПГУПС, 2007. 49 с.
15. Добеши И. Десять лекций по вейвлетам. Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
16. Левина А.Б. Сплайн-вэйвлеты и их некоторые применения. Дис. … канд. физ.-мат. наук. Москва, 2009. 215 с.

Авторы

Левина Алла Борисовна – кандидат физико-математических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56427692900, ORCID ID: 0000-0003-4421-2411, levina@cit.ifmo.ru

Ряскин Глеб Александрович – инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ORCID ID: 0000-0003-3046-047, Ryaskinkgleb20@gmail.ru

Publ., 1977, 785 p.
3. *Attack on third-party channels.* Available at: http://ru.wikipedia.org/?oldid=84074315 (accessed: 20.05.2017).
4. Akdemir K.D., Wang Z., Karpovsky M.G., Sunar B. Design of cryptographic devices resilient to fault injection attacks using nonlinear robust codes. In *Fault Analysis in Cryptography*. Eds. M. Joye, M. Tunstall. Springer, 2011, pp. 171–199. doi: 10.1007/978-3-642-29656-7_11
5. Carlet C. Partially-bent functions. *Designs, Codes and Cryptography*, 1993, vol. 3, no. 2, pp. 135–145. doi: 10.1007/bf01388412
6. Karpovsky M.G., Wang Z. Design of strongly secure communication and computation channels by nonlinear error detecting codes. *IEEE Transactions on Computers*, 2014, vol. 63, no. 11, pp. 2716–2728. doi: 10.1109/TC.2013.146
7. Karpovsky M.G., Kulikowski K., Wang Z. Robust error detection in communication and computation channels. *Proc. Int. Workshop on Spectral Techniques*, 2007.
8. Levina A.B., Taranov S.V. Construction of linear and robust codes that is based on the scaling function coefficients of wavelet transforms. *Journal of Applied and Industrial Mathematics*, 2015, vol. 9, no. 4, pp. 540–546.
9. Tokareva N.N. Bent functions: results and applications. A survey. *Applied Discrete Mathematics*, 2009, no. 1, pp. 15–37. (in Russian)
10. Pankratova I.A. *Boolean Functions in Cryptography*. Tomsk, TSU Publ., 2014, 88 p. (in Russian)
11. Tokareva N.N. *Nonlinear Boolean Functions: Bent Functions and Their Generalizations*. Saarbrucken, LAP, 2011,180 p. (in Russian)
12. Smart N. *Cryptography: An Introduction*. McGraw-Hill, 2004, 433 p.
13. Carlet C. Boolean functions for cryptography and error correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering.* Eds. P. Hammer, Y. Crama. Cambridge, 2007, pp. 257–397. doi: 10.1017/cbo9780511780448.011
14. Dem'yanovich Yu.K., Khodakovskii V.A. *Introduction to Wavelet Theory*. St. Petersburg, PSURT Publ., 2007, 49 p. (in Russian)
15. Daubechies I. *Ten Lectures on Wavelets*. Philadelphia, Society for Industrial and Applied Mathematics, 1992, 378 p.
16. Levina A.B. *Spline Wavelets and Some Applications*. Dis. Phy.-Math. Sci. Moscow, 2009, 215 p. (in Russian)

Authors

Alla B. Levina – PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56427692900, ORCID ID: 0000-0003-4421-2411, levina@cit.ifmo.ru

Gleb A. Ryaskin – engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, ORCID ID: 0000-0003-3046-047, Ryaskinkgleb20@gmail.ru