УДК 621.391.833
А. В. ДИКАРЕВ, канд. техн. наук, доцент,
Государственный университет телекоммуникаций, Киев

ОСОБЫЕ КОЛЬЦЕВЫЕ КОДЫ — предотвращение несанкционированного доступа

Показано, что в результате внесения предыскажений в кольцевые коды последние приобретают новые полезные свойства, вследствие чего их можно квалифицировать как особые кольцевые коды. Исходные «классические» и особые кольцевые коды связаны некоторой функциональной зависимостью.

Придавая особым кодам определенные свойства криптографии, имеем возможность использовать их не только для обнаружения и исправления ошибок, но и для защиты данных от несанкционированного доступа.

Ключевые слова: кольцевой код; идентификатор; кодовое слово; вектор; фильтр.

ВВЕДЕНИЕ

Кольцевой код (заготовка кольцевого кода) представляет собой квадратную матрицу двоичных символов размером $N \times N$. Каждая строка ее — вектор, все компоненты которого сдвинуты относительно компонентов предыдущей строки (начиная с первой) на один разряд вправо либо влево, но обязательно в одну сторону. Первая строка кольцевого кода называется его ***исходным вектором*** (исходной последовательностью). Главной и полной характеристикой любого кольцевого кода является его ***вектор показателей сдвига*** **(ВПС)** [1; 2]. В общем случае параметр ВПС является эквивалентом кольцевого кода и может заменить любую его строку, выполняющую одновременно роль кодового слова. Следовательно, ***ВПС является идентификатором кодового слова***, при помощи которого можно обнаруживать и исправлять канальные ошибки. Наряду с полезными свойствами ВПС имеет существенные недостатки.

• Из-за большого информационного объема, который составляют $N - 1$ целых чисел элементов ВПС, последний не пригоден для практического использования в качестве идентификатора кодового слова.

• ВПС является общим (коллективным) идентификатором всех строк данного кольцевого кода и не различает каждую строку в отдельности.

• Один и тот же ВПС является общим для кольцевых кодов с прямыми и обратными по значению символами строк, а также перевернутого на 180° по длине исходного вектора имеющегося в нем распределения нулевых и единичных символов (перевернутого дельта-фактора).

Указанные недостатки удается устранить введением предварительных искажений в исходный вектор кольцевого кода.

Для определенности понятий кольцевые коды, построенные по обычному алгоритму, будем называть ***классическими***, а кольцевые коды с предыскажениями — ***особыми кольцевыми кодами***.

ОСНОВНАЯ ЧАСТЬ

Предыскажения в особых кольцевых кодах могут носить следующий характер:

• изменяется исходный вектор кольцевого кода;

• оставаясь без изменения, исходный вектор кольцевого кода смещается на заданное число разрядов влево либо вправо;

• используется ВПС не одного, а по крайней мере трех видов модификаций заготовки кольцевого кода посредством XOR-, OR- или AND-преобразований исходного вектора с остальными строками кольцевого кода. Последние три преобразования можно дополнить их отрицанием Not, и тогда число ВПС, получаемых из одной заготовки кольцевого кода, удваивается и становится равным шести.

Примеры спецификаторов особых кольцевых кодов

Роль спецификаторов как эквивалентов строк кольцевого кода и способы их получения описаны в [3; 4].

Предыскажению при создании спецификаторов строк с одинаковым успехом могут подвергаться как исходный вектор кольцевого кода, так и любая его строка. В частности, данные табл. 1 демонстрируют результаты эксперимента, состоящего в том, что исходный вектор для каждой строки подвергался искажению на один символ на месте, соответствующем ее порядковому номеру. Такие предыскажения дают возможность идентифицировать номер строки кольцевого кода и выявлять в ней канальные ошибки.

Таблица 1

Предыскажения исходного вектора кольцевого кода с $N = 13$ и $m = 3$

Номер символа	1	2	3	4	5	6	7	8	9	10	11	12	13	*D(i)*
Первая строка (исходный вектор)	0	0	1	0	0	**1**	0	0	0	1	0	0	0	
Искаженный исходный вектор 1	1	0	1	0	0	**1**	0	0	0	1	0	0	0	
Вектор показателей сдвига 1	7	5	5	5	5	**5**	5	7	3	5	7	7		2; –2
Вторая строка	0	1	0	0	1	**0**	0	0	1	0	0	0	0	
Искаженный исходный вектор 2	0	0	0	0	1	**0**	0	0	1	0	0	0	0	
Вектор показателей сдвига 2	5	5	5	3	5	**3**	5	5	3	3	5	5		0; 0
Третья строка	1	0	0	1	0	**0**	0	1	0	0	0	0	0	
Искаженный исходный вектор 3	1	0	1	1	0	**0**	0	1	0	0	0	0	0	
Вектор показателей сдвига 3	5	7	5	5	5	**5**	5	7	5	5	5	7		0; –2

Посредством предварительного искажения строки кольцевого кода на приемном конце можно проверить ее правильность и в то же время получить защиту от несанкционированного доступа к информации. При этом верное кодовое слово будет квалифицировано как ошибочное.

Предварительное искажение связано с некоторым увеличением общего числа операций для определения правильности кодового слова (максимально в N раз), что для современных вычислительных средств не представляет особых затруднений.

Особые кольцевые коды со сдвигом исходного вектора

Циклическим сдвигом на один или несколько разрядов исходного вектора классического кольцевого кода можно создать $N - 1$ особых кольцевых кодов с различными ВПС.

Поясним, как сдвиги исходного вектора без его предыскажения влияют на новый ВПС особого кольцевого кода. Отметим, что число разрядов сдвига можно увязать с текущим номером строки кольцевого кода, и тогда каждой строке особого кольцевого кода будет соответствовать свой особый ВПС. На основании ВПС таких особых кольцевых кодов получаются абсолютно новые спецификаторы. Этот факт иллюстрируют табл. 2-4 на примере особого кольцевого кода с параметрами $N = 12$ и $m = 4$. В этих кодах исходный вектор теряет свое начало. Так, в табл. 2 начальный сдвиг исходного вектора составляет один разряд вправо, в табл. 3 сдвиг равен двум разрядам вправо, а в табл. 4 — шести разрядам вправо,

Таблица 2

Эффект от сдвига исходного вектора на один разряд

№ п/п	Вид кольцевого кода	Показатели кольцевого кода	*D*(1)
1	Строка кольцевого кода	001010010010	
2	Вид исходного вектора	000101001001	
3	XOR-код	6466**4**664680	2; 6
4	OR-код	48767767767	–3; 0
5	AND-код	4012**1**121121	–1; 0
6	Без фильтрации	8646**6**466468	2; –2

Таблица 3

Эффект от сдвига исходного вектора на два разряда

№ п/п	Вид кольцевого кода	Показатели кольцевого кода	*D*(1)
1	Строка кольцевого кода	001010010010	
2	Вид исходного вектора	100010100100	
3	XOR-код	46646**6**46808	–2; –2
4	OR-код	84876**7**76776	2; 1
5	AND-код	04012**1**12112	0; –1

Таблица 4

Эффект от сдвига исходного вектора на шесть разрядов

№ п/п	Вид кольцевого кода	Показатели кольцевого кода	*D*(1)
1	Строка кольцевого кода	001010010010	
2	Вид исходного вектора	010001010010	
3	XOR-код	66466**4**68086	2; –2
4	OR-код	78487**6**77677	1; 0
5	AND-код	10401**2**11211	–2; 1

Получается, что для одной и той же строки кольцевого кода и одного и того же исходного вектора, смещаемого на разное число разрядов, можно сформировать три комплекта различных либо по значению, либо по расположению, либо по знаку простых спецификаторов. Напомним, что алгоритм формирования спецификаторов — прерогатива владельца информации.

Применение особых кольцевых кодов для защиты данных от несанкционированного доступа

Если использовать не один, а некоторый банк предварительно заготовленных предыскажающих фильтров и обращаться к ним по секретному ключу, то с высокой достоверностью удается добиться закрытия данных от несанкционированного доступа. На первом же этапе предыскажения строки имеет смысл реализовать часть криптографических операций:

- деление кодовых блоков на подблоки;
- перемежение подблоков и блоков;
- частичные подблоковые предыскажения;
- формирование секретного ключа и т. п.

Защита информации от несанкционированного доступа выполняется в режиме работы абонентов точка-точка или точка-многоточка.

Выводы

1. При использовании кольцевых кодов предыскажению с одинаковым результатом может подвергаться либо исходный вектор, либо любая строка.

2. Смещение исходного вектора кольцевого кода позволяет кроме основного ВПС получить $N - 1$ дополнительных векторов особых частных показателей сдвигов с новыми свойствами.

3. Применением особых кольцевых кодов обеспечивается получение широкого спектра различных спецификаторов.

4. Для предыскажений удобно иметь банк предыскажающих двоичных последовательностей-фильтров.

5. Один и тот же фильтр посредством XOR-преобразования служит и для внесения предыскажения в кодовое слово, и для его удаления.

6. Глубина предыскажения может быть любой и диктоваться требованиями защиты данных от несанкционированного доступа.

7. Для защиты информации от несанкционированного доступа одновременно с предыскажением можно использовать принципы криптографии.

Литература

*1. **Дикарев, А. В.** Коды на основе двоичных колец / А. В. Дикарев // Системи управління, навігації та зв'язку.— 2014.— Вип. 1(29).— С. 50–53.*

*2. **Дикарев, А. В.** Постулаты кольцевых кодов / А. В. Дикарев // Зв'язок.— 2013.— Вип. №5(105).— С. 53–56.*

*3. **Дикарев, А. В.** Идентификация семейств кольцевых кодов // А. В. Дикарев // Телекомунікаційні та інформаційні технології.— 2015.— №2.— С. 52–57.*

*4. **Дикарев, А. В.** Некоторые закономерности кольцевых кодов // А. В. Дикарев / Системи управління, навігації та зв'язку.— 2014.— Вип. 3(31).— С. 51–55.*

Рецензент: доктор техн. наук, профессор **Б. Ю. Жураковский**, Государственный университет телекоммуникаций, Киев.

О. В. Дікарев

ОСОБЛИВІ КІЛЬЦЕВІ КОДИ — ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ

Доведено, що завдяки внесенню попередніх спотворень у кільцеві коди останні набувають нових корисних властивостей і можуть кваліфікуватись як особливі кільцеві коди, котрі з вихідними класичними кодами пов'язані певною функціональною залежністю. Надаючи особливим кодам деяких властивостей криптографії, маємо змогу використовувати їх не тільки для виявлення та виправлення канальних помилок, а й для захисту інформації від несанкціонованого доступу.

Ключові слова: кільцевий код; ідентифікатор; кодове слово; вектор; фільтр.

A. V. Dikarev

THE SPECIAL RING CODES — AVERTING A DANGER OF NOT AUTORISED ACCESS

It is shown, that as a result of entering of predistortions into ring codes the last get new useful properties owing to what they can be qualified as special ring codes. Initial "classical" and special ring codes are connected by functional dependence.

Giving to special codes certain properties of cryptography, begins possible to use them not only for detection and correction of errors, but also for protection of data against not authorised access.

Keywords: a ring code; the identifier; a code word; a vector; the filter.

УДК 381.3.004

М. М. БРАЇЛОВСЬКИЙ, канд. техн. наук, доцент;
С. В. КОЗЕЛКОВ, доктор техн. наук, професор, заслужений винахідник України,
лауреат Державної премії України в галузі науки і техніки;
Н. В. КОРШУН, канд. техн. наук, доцент,
Державний університет телекомунікацій, Київ

ОПТИМІЗАЦІЯ ВИБОРУ ПАРАМЕТРІВ ЯКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КАНАЛАХ ЗВ'ЯЗКУ

Запропоновано критерій вибору параметрів якості складної системи, який дозволяє давати узагальнену оцінку якості такої системи в діапазоні можливих відхилень значень частинних критеріїв від екстремальних і завдяки цьому враховувати ступінь погіршення одних параметрів за рахунок поліпшення інших.

Ключові слова: оптимізація; система захисту інформації; параметри якості; канали зв'язку.

Вступ

Коли та чи інша природна система (організм) протягом тривалого часу залишається цілісною, не руйнуючись під впливом зовнішніх чинників, то її вважають життєздатною. Адже, як відомо, функціонування в природних умовах відсіює нежиттєздатні організми. Для того щоб вижити, організм має адаптуватись до навколишніх умов. Те саме стосується й технічних систем. Тому при їх проектуванні, розробці та модернізації доводиться