ПОСТРОЕНИЕ КРИТЕРИЯ ОЦЕНКИ КАЧЕСТВА ДВОИЧНЫХ БАРКЕРОПОДОБНЫХ КОДОВ

DOI: 10.36724/2072-8735-2022-16-12-11-16

Manuscript received 30 September 2022;
Accepted 24 October 2022

Гавришев Алексей Андреевич,
ФГАОУ ВО "НИЯУ "МИФИ",
Москва, Россия, ***alexxx.2008@inbox.ru***

Осипов Дмитрий Леонидович,
ФГАОУ ВО "СКФУ", г. Ставрополь, Россия,
dmtrosipov@ya.ru

Ключевые слова: *показатели оценки качества, защищенные беспроводные системы связи, двоичные коды Баркера, двоичные баркероподобные коды, линейная сложность*

Задачей данной статьи является построение критерия оценки качества двоичных баркероподобных кодов. Проведен анализ известных исследований по формированию данных кодов, обладающих близкими к двоичным кодам Баркера свойствами. Анализ показал, что в работах, посвященных вопросам применения в защищенных беспроводных системах связи известных двоичных баркероподобных кодов и формирования таких кодов, исследователи в первую очередь обращают внимание на такие их показатели оценки качества, как автокорреляционная функция, длина и количество таких кодов и другие. На основе анализа работ [5, 9-25] сформулирован исходный кортеж оценки качества двоичных баркероподобных кодов, представленный выражением (1). Однако в исходном кортеже (1) отсутствует такой важный показатель оценки качества, как оценка линейной сложности, который часто принимается за один из первичных показателей криптостойкости. Исходя из этого, целью данной статьи является повышение точности оценки двоичных баркероподобных кодов за счет применения выявленного критерия. Авторы статьи с помощью алгоритма Берлекэмпа-Месси провели оценку линейной сложности двоичных баркероподобных кодов, представленных в работах [9-23]. Установлено, что достаточно большое количество таких кодов (от 24% и до 75%) обладают недостаточной линейной сложностью, то есть являются некриптостойкими. Как следствие, их нельзя использовать в защищенных беспроводных системах связи. Полученный результат согласуется с другими исследованиями в данной области. Исходя из этого, при использовании в защищенных беспроводных системах связи известных двоичных баркероподобных кодов, а также при формировании новых двоичных баркероподобных кодов, необходимо обращать внимание, не только на известные показатели оценки качества, но также и на их линейную сложность. Авторами проведена модификация исходного кортежа, представленного выражением (1). Модифицированный кортеж представлен выражением (2). По мнению авторов, модифицированный критерий оценки качества позволит повысить точность оценки двоичных баркероподобных кодов.

Информация об авторах:
Гавришев Алексей Андреевич, *магистрант, ФГАОУ ВО "НИЯУ "МИФИ", г. Москва, Россия*
Осипов Дмитрий Леонидович, *к.т.н., доцент, ФГАОУ ВО "СКФУ", г. Ставрополь, Россия*

Для цитирования:
Гавришев А.А., Осипов Д.Л. Построение критерия оценки качества двоичных баркероподобных кодов // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №12. С. 11-16.

For citation:
Gavrishev A.A., Osipov D.L. (2022) Building a quality assessment criterion binary Barker-like codes. *T-Comm*, vol. 16, no.12, pp. 11-16. (*in Russian*)

Введение

В настоящее время к защищенным беспроводным системам связи предъявляются требования по повышенной помехозащищенности, высокой достоверности передачи информации, высокой энергетической и структурной скрытности излучений, высокой скорости передачи информации и другие. Одним из возможных путей решения задачи защиты передаваемой по беспроводным каналам связи информации от преднамеренных воздействий является использование различных сложных сигнально-кодовых структур, обладающих стойкостью к раскрытию и защищенных от несанкционированного воспроизведения [1-8].

Преимущества сложных сигнально-кодовых структур реализуются только в том случае, когда псевдослучайные последовательности (ПСП), на основе которых они формируются, отвечают критерию оценки качества ПСП, связанному с оптимальными свойствами автокорреляционной функции (АКФ). Единственным классом двоичных ПСП, обладающих оптимальными свойствами АКФ, являются двоичные коды Баркера (ДКБ). Так же известно, что энергетический выигрыш от использования сложного сигнала и скрытность функционирования радиолинии, наряду с другими факторами, напрямую зависит от другого критерия оценки качества ПСП – количества сигналов в системе. Известно, что путем подбора двоичных кодов были найдены ДКБ только для длин последовательности N=2, 3, 4, 5, 7, 11, 13.

Многочисленные попытки обнаружить существование ДКБ большей длины не увенчались успехом. Поэтому, несмотря на уникальные корреляционные свойства ДКБ, при их использовании не приходится говорить о серьезном повышении помехоустойчивости и скрытности радиолинии, так как число кодов ничтожно, а их базы не превышают 13. В связи с этим, предпринимались безуспешные попытки получения ПСП, обладающих одинаковыми с ДКБ свойствами [4, 5]. В силу чего, к настоящему времени развивается направление по исследованиям так называемых двоичных баркероподобных кодов [4, 5, 9-23].

Далее в работе условимся двоичные бинарные ПСП, которые являются близкими по свойствам к ДКБ, называть двоичными баркероподобными кодами. Так как двоичные баркероподобные коды схожи с ДКБ, но не в точности им соответствуют, то актуальной задачей является выявление показателей качества двоичных баркероподобных кодов и формирование на их основе кортежа, позволяющего оценить качество двоичных баркероподобных кодов.

Задачей данной статьи является построение критерия оценки качества двоичных баркероподобных кодов.

Целью данной статьи является повышение точности оценки ДБК за счет применения выявленного критерия.

Результаты исследований

В многочисленных работах [9-23] изучаются вопросы формирования новых двоичных баркероподобных кодов, предложены новые методы их формирования, приведены примеры полученных двоичных баркероподобных кодов, проводится их исследование по различным показателям оценки качества (ПК).

Так в работах [9-11] получены различные двоичные баркероподобные коды, схожие с ДКБ, имеющие длину N>13 и обладающие сравнимым уровнем боковых лепестков АКФ. Приведены примеры полученных двоичных баркероподобных кодов. В работах [12, 13], по результатам проведения исследований, предложен новый тип двоичных баркероподобных кодов с хорошими автокорреляционными свойствами, описан процесс их синтеза и проанализирована структура.

Приведены примеры полученных двоичных баркероподобных кодов. В работах [14-16] приведены новые двоичные баркероподобные коды с квазиидеальной АКФ, длина которых значительно больше тринадцати. Приведены примеры полученных двоичных баркероподобных кодов. В работе [17] рассматривается новый класс двоичных баркероподобных кодов, которые, с одной стороны, обладают свойствами блочных циклических кодов с выявлением и исправлением ошибок, а с другой стороны обладают свойствами ДКБ, но с менее жесткими требованиями к их корреляционным свойствам. Приведены примеры полученных двоичных баркероподобных кодов. В работе [18] рассмотрен класс двоичных баркероподобных кодов с практически нулевыми боковыми пиками АКФ, не имеющих регулярной структуры с чётной разрядностью.

Приведены примеры полученных двоичных баркероподобных кодов. В работах [19, 20] представлены двоичные баркероподобные коды с хорошими автокорреляционными свойствами и специальные согласованные фильтры, предназначенные для их эффективного декодирования. Приведены примеры полученных двоичных баркероподобных кодов. В работе [21] приведены примеры двоичных баркероподобных кодов, близких к ДКБ. Показаны их автокорреляционные и спектральные характеристики. В работе [22] приведены результаты синтеза двоичных баркероподобных кодов, которые, согласно утверждению авторов данной работы, эффективнее лучших ДКБ по относительному уровню боковых пиков АКФ и, кроме того, их количество достаточно велико. Приведены примеры полученных двоичных баркероподобных кодов. В работе [23] рассмотрены методы получения двоичных баркероподобных кодов, построенных на основе взаимных псевдослучайных кодов, позволяющие расширить количество двоичных баркероподобных кодов. Показаны их автокорреляционные характеристики. Приведены примеры полученных двоичных баркероподобных кодов

Как видно из представленных работ [9-23], при формировании новых двоичных баркероподобных кодов, помимо АКФ, специалисты обращают внимание на такие их важные ПК, как длина и количество ДБК, их спектральные характеристики, пик-фактор и некоторые другие. В таблице 1 собраны примеры ПК, широко используемые в различных источниках при формировании новых двоичных баркероподобных кодов [5, 9-24].

Представленные в таблице 1 ПК возможно объединить в единый кортеж, который может служить критерием оценки качества двоичных баркероподобных кодов. Заметим, что в работах [9-23], в которых исследуются вопросы формирования новых двоичных баркероподобных кодов, в явном виде такой кортеж не предложен.

Таблица 1

Примеры ПК, применяемые при оценке новых двоичных баркереподобных кодов

№	ПК двоичных баркереподобных кодов	Обозначение	Требование
1	АКФ	$R(\tau)$	Двоичные баркереподобные коды должны обладать минимальными боковыми пиками АКФ
2	Длина	N	Двоичные баркереподобные коды должны обладать максимальной длиной
3	Количество	Q	Количество двоичных баркереподобных кодов должно быть достаточно велико
4	Выбросы амплитудно-частотных спектров	$G(\omega)$	Двоичные баркереподобные коды должны обладать минимальными выбросами амплитудно-частотных спектров
5	Пик-фактор	ρ	Двоичные баркереподобные коды должны обладать минимальным значением пик-фактора

С учетом работ [5, 24, 25] и методических рекомендаций из работы [26], содержательную формулировку задачи повышения качества функционирования защищенной беспроводной системы связи возможно сформулировать следующим образом. Для повышения качества функционирования защищенной беспроводной системы связи S при использовании известных или новых двоичных баркереподобных кодов, необходимо оперировать критерием оценки качества двоичных баркереподобных кодов K, представляющим собой кортеж (1):

$$\begin{cases} K =< R(\tau),\ N,\ Q,\ G(\omega), \rho > \\ R(\tau) < R_{доп}(\tau),\ N \to \max,\ Q \to \max,\ G(\omega) < G_{доп}(\omega), \rho < \rho_{доп} \end{cases}, \quad (1)$$

где $R(\tau)$ – АКФ двоичных баркереподобных кодов, N – длина двоичных баркереподобных кодов, Q – количество двоичных баркереподобных кодов, $G(\omega)$ – выбросы амплитудно-частотных спектров двоичных баркереподобных кодов, ρ – пик-фактор двоичных баркереподобных кодов, $R_{доп}(\tau)$ – допустимая АКФ двоичных баркереподобных кодов, $G_{доп}(\omega)$ – допустимые выбросы амплитудно-частотных спектров двоичных баркереподобных кодов, $\rho_{доп}$ – допустимый пик-фактор двоичных баркереподобных кодов.

Вместе с тем, одним из важных, но редко используемых ПК двоичных баркереподобных кодов является показатель, связанный с оценкой их линейной сложности. Известно [1-7], что линейная сложность (ЛС) L часто принимается за один из первичных показателей криптостойкости, под которой понимают минимальную длину двоичного регистра сдвига с линейной обратной связью (РСЛОС), воспроизводящего данную бинарную последовательность. Разумеется, любую бинарную последовательность заданной длины N можно сгенерировать с помощью двоичного РСЛОС, поэтому с точки зрения защищенной беспроводной системы связи желательно иметь длину этого РСЛОС как можно ближе к длине самой последовательности N [1, 3, 5-7].

На практике, в соответствии с [5-7], криптостойкими (стойкими к взлому) считаются последовательности, ЛС которых больше половины длины последовательности ($L>N/2$).

Значение ЛС заданной последовательности одновременно со структурой петли обратной связи соответствующего двоичного РСЛОС можно найти с помощью известного алгоритма Берлекэмпа-Месси – итеративной процедуры, отыскивающей среди большого числа линейных структур, генерирующих заданную последовательность, РСЛОС наименьшей длины. Алгоритм Берлекэмпа-Месси состоит из следующих шагов [1, 3, 5-7]:

1) на r-й итерации алгоритма, начиная с r=1, строится регистр сдвига минимальной длины, генерирующий первые r элементов последовательности;

2) на следующей итерации проверяется, генерирует ли полученный РСЛОС наряду с r элементами и (r +1)-й;

3) при отрицательном ответе длина и петля обратной связи РСЛОС модифицируются так, чтобы вновь получить регистр наименьшей длины, генерирующий уже (r+1)-й элемент последовательности и т. д.

Заметим, что диапазон применения алгоритма Берлекэмпа-Месси достаточно широк и не ограничивается только нахождением минимальной длины РСЛОС, воспроизводящего данную бинарную последовательность [1, 3, 5-7]. В качестве примера обратим внимание на работу [27], в которой указывается, что последовательность побед кандидатов на выборах может быть приближенно представлена, как бинарная ПСП, состоящая из значений 0 и 1. На практическом примере, в том числе и с помощью алгоритма Берлекэмпа–Месси, показано, что такая бинарная ПСП имеет ЛС $L>N/2$, то есть потенциально может являться случайной [1, 3, 5-7]. Данное исследование показывает, что алгоритм Берлекэмпа–Месси потенциально возможно применять к ПСП любой природы.

Проведем оценку ЛС двоичных баркереподобных кодов. Заметим, что двоичные баркереподобные коды, для которых выполняется выражение $L>N/2$, далее станем называть криптойстойкими (стойкими к взлому), в соответствии с [1, 6, 7], а двоичные баркереподобные коды, для которых не выполняется выражение $L>N/2$ – некриптостойкими (не стойкими к взлому) [1, 6, 7]. Для упрощения вычислений в качестве двоичных баркереподобных кодов возьмем те двоичные баркереподобные коды, которые приведены в работах [9-23]. Оценку ЛС проведем с помощью алгоритма Берлекэмпа–Месси, программная реализация которого представлена в [28].

В таблице 2 представлены данные, полученные при оценке ЛС двоичных баркереподобных кодов, начиная с наиболее криптостойких двоичных баркереподобных кодов, и заканчивая наименее крипостойкими двоичными баркереподобными кодами.

Как видно из таблицы 2, для двоичных баркереподобных кодов, приведенных в источниках [9-23], не смотря на их различное количество, процент некриптостойких двоичных баркереподобных кодов, то есть таких двоичных баркереподобных кодов, которые обладают недостаточной ЛС, составляет от 24 % и до 75 %. По полученным результатам можно прийти к выводу, что достаточно большое количество двоичных баркереподобных кодов потенциально могут являться некриптостойкими.

Таблица 2

Результаты проведенных расчетов ЛС двоичных баркереподобных кодов из [9-23]

№	Источник	Общее количество двоичных баркереподобных кодов, приведенных в источнике	Количество некриптостойких двоичных баркереподобных кодов	Процентное соотношение некриптостойких кодов к общему количеству приведенных
1	[12, 13]	33	8	24 %
2	[11]	12	3	25 %
3	[14-16]	41	14	34 %
4	[10]	33	14	42 %
5	[22]	74	34	45 %
6	[19, 20]	20	10	50 %
7	[9]	30	15	50 %
8	[17]	34	17	50 %
9	[21]	28	16	57 %
10	[18]	54	32	59 %
11	[23]	12	9	75 %

Полученные результаты в целом согласуются с другими исследованиями в данной области, которые показывают, что некоторые известные линейные и нелинейные ПСП, отличные от двоичных баркереподобных кодов и используемые для защищенных беспроводных систем связи, являются некриптостойкими, то есть обладают недостаточной ЛС [1-8].

Таким образом, можно утверждать, что при использовании в защищенных беспроводных системах связи известных и новых двоичных баркереподобных кодов, необходимо учитывать такой важный ПК, как ЛС. С учетом сказанного, модифицируем критерий оценки качества двоичных баркереподобных кодов, описываемый выражением (1), введя в него ЛС. По мнению авторов, ЛС, в силу ее важности для оценки защищенных беспроводных систем связи, необходимо разместить сразу после АКФ и длины двоичных баркереподобных кодов. Модифицированный критерий оценки качества двоичных баркереподобных кодов представим в виде следующего кортежа (2):

$$\begin{cases} K = < R(\tau), N, L, Q, G(\omega), \rho > \\ R(\tau) < R_{доп}(\tau),\ N \to \max,\ L > \dfrac{N}{2}, Q \to \max,\ G(\omega) < G_{доп}(\omega), \rho < \rho_{доп} \end{cases}, \quad (2)$$

где $R(\tau)$ – АКФ двоичных баркереподобных кодов, N – длина двоичных баркереподобных кодов, L – линейная сложность двоичных баркереподобных кодов, Q – количество двоичных баркереподобных кодов, $G(\omega)$ – выбросы амплитудно-частотных спектров двоичных баркереподобных кодов, ρ – пик-фактор двоичных баркереподобных кодов, $R_{доп}(\tau)$ – допустимая АКФ двоичных баркереподобных кодов, $G_{доп}(\omega)$ – допустимые выбросы амплитудно-частотных спектров двоичных баркереподобных кодов, $\rho_{доп}$ – допустимый пик-фактор двоичных баркереподобных кодов.

Заключение

В данной работе рассмотрены известные источники [9-23], посвященные исследованиям формирования двоичных баркереподобных кодов, обладающих близкими к ДКБ свойствами. Отмечено, что в работах, посвященных вопросам применения в защищенных беспроводных системах связи известных двоичных баркереподобных кодов и формирования новых двоичных баркереподобных кодов, исследователи в первую очередь обращают внимание на такие их показатели качества, как АКФ, длина и количество двоичных баркереподобных кодов, а также на спектральные характеристики и пик-фактор. На основе анализа работ [5, 9-25] сформулирован исходный кортеж оценки качества двоичных баркереподобных кодов, представленный выражением (1). Однако в исходном кортеже (1) отсутствует такой важный ПК двоичных баркереподобных кодов, как оценка ЛС. Авторы работы с помощью алгоритма Берлекэмпа-Месси провели оценку ЛС двоичных баркереподобных кодов, представленных в работах [9-23].

В результате проведенных исследований установлено, что достаточно большое количество известных двоичных баркереподобных кодов (от 24 % и до 75 %) обладают недостаточной ЛС, то есть являются некриптостойкими. Как следствие, их нельзя использовать в защищенных беспроводных системах связи. Полученный результат согласуется с другими научными работами в данной области [1-8]. Эти исследования показывают, что ряд линейных и нелинейных ПСП, отличных от двоичных баркереподобных кодов и используемых для защищенных беспроводных систем связи, обладают недостаточной ЛС, то есть являются некриптостойкими.

По итогам проведенных исследований следует заключить, что при использовании в защищенных беспроводных системах связи известных двоичных баркереподобных кодов, а также при формировании новых двоичных баркереподобных кодов, необходимо обращать внимание не только на их АКФ, длину, количество, спектральные характеристики, пик-фактор и другие ПК, но также и на их линейную сложность. Исходя из этого, проведена модификация исходного критерия оценки качества двоичных баркереподобных кодов, представленного выражением (1). Модифицированный критерий оценки качества двоичных баркереподобных кодов представлен выражением (2). Сформированный критерий оценки качества позволит повысить точность оценки двоичных баркереподобных кодов при их использовании в защищенных беспроводных системах связи, а также при формировании новых двоичных баркереподобных кодов.

Литература

1. *Панькова В.В., Саломатин С.Б.* Криптографический анализ кодовых структур кривой Эрмита на соответствие требованиям систем защиты информации // Доклады БГУИР. 2014. № 3 (81). С. 58-63.

2. *Сиващенко С.И.* Скрытность радиосистем со сложными и хаотическими сигналами // Системи управління, навігації та зв'язку. 2009. № 3(11). С. 56-58.

3. *Игнатьев Ф.В., Ипатов В.П., Флотская И.Ю.* Об эквивалентной линейной сложности последовательностей Кердока // Известия СПБГЭТУ ЛЭТИ. 2010. № 9. С. 11-17.

4. *Ковалев М.А., Макаров А.А., Павский В.Ф., Петелин Ю.В.* О существовании троичных псевдослучайных последовательностей, подобных двоичным кодам Баркера // Труды Военно-космической академии имени А.Ф. Можайского. 2016. В. 650. С. 54-56.

5. *Орёл Д.В.* Моделирование стохастических систем двоичных квазиортогональных кодовых последовательностей на основе метода функциональных преобразований // Автореф. дис. ... канд. техн. наук. Ставрополь. 2013. 19 С.

6. *Едемский В.А.* Синтез чередующихся троичных последовательностей с хорошими автокорреляционными свойствами и высокой эквивалентной линейной сложностью // Журнал радиоэлектроники. 2014. № 2. 7 С.

7. *Гавришев А.А., Жук А.П.* Применение алгоритма Берлекэмпа-Месси для количественного анализа защищенных систем связи // Прикладная информатика. 2019. Т. 14. № 4 (82). С. 118-134. DOI: 10.24411/1993-8314-2019-10031.

8. *Gao Juntao, Hu Yupu, Li Xuelian* Linear spans of optimal sets of frequency hopping sequences // RAIRO-Theor. Inf. Appl. 2012. No. 46. Pp. 343–354.

9. *Бронов С.А., Малеев А.В., Михайленко Я.В.* Синтез уникальных фазоманипулированных сигналов для интеллектуальной системы обнаружения подвижных объектов // Журнал научных публикаций аспирантов и докторантов. 2008. № 9 (27). С. 208-212.

10. *Wei Hsiang Wu, Ho Yin Chan, Wai Ho Mow* Spreading sequences with dual low correlation windows for quasi-synchronous code-division multiple-access communication // Patent US 8,306,092. 2012. 25 P.

11. *Siti Julia Rosli, Hasliza Rahim, Ruzelita Ngadiran, K. N. Abdul Rani, Muhammad Imran Ahmad, Wee Fwen Hoon* Design of Binary Coded Pulse Trains with Good Autocorrelation Properties for Radar Communications // MATEC Web of Conferences 150. 2018. No. 06016. P. 3. DOI: 10.1051/matecconf/201815006016.

12. *Голубничий А.Г.* Правила кодирования и структура обобщённых бинарных последовательностей Баркера // Проблеми інформатизації та управління. 2013. № 4 (44). С. 20-26.

13. *Голубничий А.Г.* Корреляционные свойства обобщённых бинарных последовательностей Баркера // Проблеми інформатизації та управління. 2015. № 2(50). С. 48-55.

14. *Волынская А.В.* Результаты математического моделирования процесса поиска кодовых последовательностей с заданными корреляционными свойствами // Вестник Уральского государственного университета путей сообщения. 2009. № 3-4. С. 64-71.

15. *Храповицкий И.А., Максимов В.В.* Новые композитные коды Баркера // The scientific heritage. 2020. № 49. С. 28-35.

16. *Максимов В.В., Храповицкий И.А.* Исследование композитных кодов Баркера // The scientific heritage. 2020. № 48. С. 15-22.

17. *Дикарев А.В.* Двоичные последовательности с одинаковым коэффициентом подобия // Вісник ДУІКТ. 2013. №4. С. 34-39.

18. *Головков А.А., Уваров В.А., Зуев А.Г.* Расширение класса кумулятивных кодов // DSPA: Вопросы применения цифровой обработки сигналов. 2012. Т. 2. № 1. С. 52-57.

19. *Lehtinen M.S., Damtie B., Nygrem T.* Optimal binary phase codes and sidelobe-free decoding filters with application to incoherent scatter radar // Annales Geophysicae. 2004. No. 22. Pp. 1623–1632.

20. *Baylie Damtie, Markku Lehtinen, Mikko Orispaa, Juha Vierinen* Optimal long binary phase code-mismatched filter pairs with applications to ionospheric radars // Bull. Astr. Soc. India. 2007. No. 35. Pp. 619–623.

21. *Pierfrancesco Lombardo* Forme d'onda con modulazione di fase // Radiotecnica e Radiolocalizzazione. RRSN – DIET, Univ. di Roma "La Sapienza". URL: https://elearning.uniroma1.it/ (дата обращения: 01.01.2022).

22. *Чепрукова Ю.В., Соколов М.А.* Бинарные R2-коды, их характеристики и применение // Информационно-управляющие системы. 2014. № 1. С. 76-83.

23. *Дятко А.А., Шумский П.Н., Ярмолик С.Н.* Фазоманипулированные сигналы на основе взаимных кодов и их внутрепериодная обработка // Труды БГТУ. Физико-математические науки. 2011. № 6. С. 102-106.

24. *Студеникин А.В., Жук А.П.* Моделирование дискретных ортогональных кодовых последовательностей для систем передачи информации // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 1. С. 36-43. DOI: 10.36724/2409-5419-2021-13-1-36-43.

25. *Гайчук Д.В., Белоконь А.В., Белоконь Л.В.* Разработка требований к ансамблям сигналов-переносчиков информации в двухлучевых ДКМ радиоканалах // Двойные технологии. 2009. №4 (49). С. 56-58.

26. *Макаренко С.И.* Справочник научных терминов и обозначений.СПб.: Наукоемкие технологии, 2019. 254 с.

27. *Давыдов А.А.* Партийная принадлежность президентов США, 1852-2016: анализ и прогнозирование // Телескоп: журнал социологических и маркетинговых исследований. 2017. № 3. С. 13-17.

28. An Online Calculator of Berlekamp-Massey Algorithm. URL: https://github.com/bozhu/BMA (дата обращения: 01.07.2022).

BUILDING A QUALITY ASSESSMENT CRITERION BINARY BARKER-LIKE CODES

Aleksei A. Gavrishev, *National Research Nuclear University MEPhI, Moscow, Russia,* ***alexxx.2008@inbox.ru***
Dmitrii L. Osipov, *North-Caucasus Federal University, Stavropol, Russia,* ***dmtrosipov@ya.ru***

Abstract
The objective of this article is to construct a criterion for evaluating the quality of binary Barker-like codes. The analysis of well-known studies on the formation of these codes with properties close to binary Barker codes is carried out. The analysis showed that in the works devoted to the use of well-known binary Barker-like codes in secure wireless communication systems and the formation of such codes, researchers primarily pay attention to such quality assessment indicators as the autocorrelation function, the length and number of such codes, and others. Based on the analysis of works [5, 9-25], the initial tuple of quality assessment of binary Barker-like codes is formulated, represented by the expression (1). However, the original tuple (1) lacks such an important quality assessment indicator as the linear complexity assessment, which is often taken as one of the primary indicators of crypto resistance. Based on this, the purpose of this article is to increase the accuracy of the evaluation of binary Barker-like codes by applying the identified criterion. The authors of the article, using the Berlekamp-Massey algorithm, evaluated the linear complexity of binary Barker-like codes presented in [9-23]. It has been established that a sufficiently large number of such codes (from 24% to 75%) have insufficient linear complexity, that is, they are non-cryptographic. As a result, they cannot be used in secure wireless communication systems. The result obtained is consistent with other studies in this field. Proceeding from this, when using well-known binary Barker-like codes in secure wireless communication systems, as well as when forming new binary Barker-like codes, it is necessary to pay attention not only to the known quality assessment indicators, but also to their linear complexity. The authors have modified the original tuple represented by expression (1). The modified tuple is represented by expression (2). According to the authors, the modified quality assessment criterion will improve the accuracy of the evaluation of binary Barker-like codes.

Keywords: *quality assessment indicators, secure wireless communication systems, binary Barker codes, binary Barker-like codes, linear complexity.*

References

1. Pankova V.V., Salomatin S.B. (2014). Cryptographic analysis of the code structures of Hermite curve for compliance with the requirements of information security systems. *Doklady BGUIR*. No. 3 (81), pp. 58-63 (In Russian)
2. Sivashchenko S.I. (2009). Secrecy of radio system with difficult and chaotic signals. *Systemy upravlinnja, navigacii' ta zv'jazku - Systems of control, navigation and communication*. No. 3(11), pp. 56-58 (in Russian)
3. Ignatiev F.V., Ipatov V.P., Flotskaya I.Y. (2010). On the equivalent linear complexity of Kerdock sequences. *Proceedings of Saint Petersburg Electrotechnical University*. No. 9, pp. 11-17 (In Russian)
4. Kovalev M.A., Makarov A.A., Pavskij V.F., Petelin Yu.V. (2016). On the existence of ternary pseudorandom sequences similar to Barker's binary code. *Trudy Voenno-kosmicheskoj akademii imeni A.F. Mozhajskogo*. I. 650. Pp. 54-56 (In Russian).
5. Oryol D.V. (2013). Modeling of stochastic systems of binary quasi-orthogonal code sequences based on the method of functional transformations. Abstract of Ph. D. thesis in eng sci. Stavropol. 19 p. (In Russian)
6. Edemskii V.A. (2014). Synthesis of interleaved ternary sequences with low auto - correlation and high linear complexity. *Zhurnal radioelektroniki* [Journal of Radio Electronics]. No. 2. 7 p. (In Russian)
7. Gavrishev A.A., Zhuk A.P. (2019). The application of the algorithm Berlekamp-Massey for the quantitative analysis of secure communication systems. *Journal of Applied Informatics*. Vol. 14. No. 4 (82), pp. 118-134. DOI: 10.24411/1993-8314-2019-10031 (In Russian)
8. Gao Juntao, Hu Yupu, Li Xuelian (2012). Linear spans of optimal sets of frequency hopping sequences. *RAIRO-Theor. Inf. Appl*. No. 46, pp. 343-354.
9. Bronov S.A., Maleev A.V., Mihajlenko Ya.V. (2008). Synthesis of unique phase-manipulated signals for an intelligent mobile object detection system. *Zhurnal nauchnyh publikacij aspirantov i doktorantov*. No. 9 (27), pp. 208-212. (In Russian)
10. Wei Hsiang Wu, Ho Yin Chan, Wai Ho Mow (2012). Spreading sequences with dual low correlation windows for quasi-synchronous code-division multiple-access communication. Patent US 8,306,092. 25 p.
11. Siti Julia Rosli, Hasliza Rahim, Ruzelita Ngadiran, K. N. Abdul Rani, Muhammad Imran Ahmad, Wee Fwen Hoon (2018). Design of Binary Coded Pulse Trains with Good Autocorrelation Properties for Radar Communications. *MATEC Web of Conferences 150*. No. 06016. P. 3. DOI: 10.1051/matecconf/201815006016.
12. Golubnichij A.G. (2013). Coding rules and structure of generalized binary Barker sequences. *Problemi informatizacii ta upravlinnya*. No. 4 (44), pp. 20-26. (In Russian)
13. Golubnichij A.G. (2015). Correlation properties of generalized binary Barker sequences. *Problemi informatizacii ta upravlinnya*. No. 2(50), pp. 48-55. (In Russian)
14. Volynskaya A.V. (2009). Results of mathematical modelling of code chain search process with ajusted correlated behavior. *Vestnik Ural'skogo gosudarstvennogo universiteta putej soobshcheniya*. No. 3-4, pp. 64-71. (In Russian)
15. Khrapovitsky I., Maksimov V. (2020). New composite Barker codes. *The scientific heritage*. No. 49, pp. 28-35. (In Russian).
16. Maksymov V., Khrapovitsky I. (2020). Research of composite Barker codes. *The scientific heritage*. No. 48, pp. 15-22. (In Russian)
17. Dikarev A.V. (2013). Binary sequences with the same similarity coefficient. *Visnik DUIKT*. No. 4, pp. 34-39. (In Russian)
18. Golovkov A.A., Uvarov V.A., Zuev A.G. (2012). Extension of the class of cumulative codes. *DSPA: Voprosy primeneniya cifrovoj obrabotki signalov*. Vol. 2. No. 1, pp. 52-57. (In Russian)
19. Lehtinen M.S., Damtie B., Nygrern T. (2004). Optimal binary phase codes and sidelobe-free decoding ?lters with application to incoherent scatter radar. *Annales Geophysicae*. No. 22, pp. 1623-1632.
20. Baylie Damtie, Markku Lehtinen, Mikko Orispaa, Juha Vierinen (2007). Optimal long binary phase code-mismatched filter pairs with applications to ionospheric radars. *Bull. Astr. Soc. India*. No. 35, pp. 619-623.
21. Pierfrancesco Lombardo Forme d'onda con modulazione di fase. Radiotecnica e Radiolocalizzazione. *RRSN - DIET, Univ. di Roma "La Sapienza"*. URL: https://elearning.uniroma1.it/ (date of access: 01.01.2022).
22. Cheprukov Yu.V., Socolov M.A. (2014). Binary R2-Codes, Their Features and Application. *Informacionno-upravlyayushchie sistemy*. No. 1, pp. 76-83. (In Russian)
23. Dyatko A.A., Shumskij P.N., Yarmolik S.N. (2011). Phase-manipulated signals based on mutual codes and their intra-period processing. *Trudy BGTU. Fiziko-matematicheskie nauki*. No. 6, pp. 102-106. (In Russian)
24. Studenikin A.V., Zhuk A.P. (2021). Modeling of discrete orthogonal code sequences for information transmission systems. *High technologies in Earth space research*. Vol. 13. No. 1, pp. 36-43. DOI: 10.36724/2409-5419-2021-13-1-36-43. (In Russian)
25. Gajchuk D.V., Belokon A.V., Belokon L.V. (2009). Working out of requirements to ensembles of signals-carriers of the information in two-beam shortwave radio channels. *Dvojnye tekhnologii*. No. 4 (49), pp. 56-58. (In Russian)
26. Makarenko S.I. (2019). Handbook of Scientific Terms and Designations. SPb.: Naukoemkie tekhnologii Publ. 254 p. (In Russian)
27. Davydov A.A. (2017). The party affiliation of the presidents of the United States, 1852-2016: analysis and forecasting. *Teleskop: zhurnal sociologicheskih i marketingovyh issledovanij*. No. 3, pp. 13-17. (In Russian)
28. An Online Calculator of Berlekamp-Massey Algorithm. URL: https://github.com/bozhu/BMA (date of access: 01.05.2022).

Information about authors:

Aleksei A. Gavrishev, *Master's Student, National Research Nuclear University MEPhI, Moscow, Russia*

Dmitrii L. Osipov, *Ph. D., North-Caucasus Federal University, Stavropol, Russia*