УДК 621.391.1

И.Д. ГОРБЕНКО, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук,
А.Е. СЕМЕНКО, В.Л. МОРОЗОВ

МЕТОД СИНТЕЗА ПРОИЗВОДНЫХ СИСТЕМ СИГНАЛОВ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СИМВОЛОВ

Введение

В условиях интенсивного противодействия сторон, интересы и конкуренция которых могут проявляться в различных сферах, в том числе, как показали последние события, в сфере ведения информационных и гибридных войн, особое значение приобретает наличие и применение защищенных телекоммуникационных систем (ТКС). В существенной мере такие системы базируются на применении защищенных радиоканалов. При этом под защищенностью систем необходимо понимать, в широком смысле, прежде всего их способность обеспечивать необходимые показатели по помехозащищенности, имитостойкости, информационной, энергетической и структурной скрытности функционирования системы.

К ТКС предъявляются все более жесткие требования по обеспечению эффективности их функционирования в условиях сложных внешних воздействий: естественных и преднамеренных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот. Значительное число современных систем относятся к многопользовательским системам. В таких системах множество каналов размещаются в пределах общего частотно-временного ресурса, так что каждый абонент имеет возможность передавать и принимать информацию одновременно с другими абонентами и независимо от них. Одним из способов повышения эффективности использования диапазона частот, с учетом электромагнитной совместимости, является использование множественного доступа с кодовым разделением абонентов (CDMA), работающих в общей полосе частот. Указанный способ доступа абонентов к различным информационным ресурсам и технологиям является наиболее перспективным по многим характеристикам: высокая помехозащищенность каналов и обеспечение конфиденциальности передаваемых данных; высокая скорость передачи и эффективность использования полосы частот; высокая энергетическая экономичность и абонентская емкость сети. Поскольку кодовое разделение каналов ТКС основано на различии сигналов, предоставляемых абонентам системы, то построение таких систем и их характеристики определяются выбором сигналов и их свойствами.

Большое значение при решении задач обеспечения требуемой помехозащищенности и информационной безопасности имеют исследования, связанные с использованием новых видов сигналов, получивших название сложных, широкополосных, многомерных и шумоподобных.

Структура современных информационных сетей и систем характеризуется, как правило, значительным пространственным распределением большого числа взаимодействующих абонентов. В этих условиях важную роль в обеспечении качества обслуживания конечных абонентов играют технологии обработки, хранения, защиты, переноса информации в сети в условиях естественных и искусственных помех (воздействий) и ограниченного физического ресурса линий связи. К ТКС, особенно к системам критического назначения, предъявляются более жесткие требования по обеспечению эффективности их функционирования (скорости передачи информации, достоверности приема информации, живучести, помехозащищенности, информационной безопасности) в условиях сложных внешних и внутренних воздействий: естественных и преднамеренных помех, помех от других радиотехнических систем.

Повышенные требования к быстрому принятию решения и доведению до исполнителей (пользователей) информации в условиях внутренних и внешних воздействий, обусловленных действием станций (абонентов), работающих в общем диапазоне частот, и станций, осуществляющих целенаправленное противодействие функционированию критических

приложений ТКС, в значительной мере не учитываются существующими информационными технологиями. В ряде приложений телекоммуникационных систем для решения задач информационной безопасности привлекаются системы и средства криптографической защиты информации, что требует значительных материальных затрат и осуществления совокупности организационных, инженерно-технических мероприятий, методов и средств.

Задача построения защищенной ТКС – создать систему, устойчивую к воздействию множества различных, актуальных для данной системы, воздействий (помех). Объективно существует противоречие между жесткими требованиями по обеспечению достоверности, скрытности, конфиденциальности, целостности, подлинности данных, хранящихся и передаваемых по проводным и беспроводным линиям связи ТКС, с одной стороны, и существующими моделями, методами и технологиями управления телекоммуникационными сетями, информационной безопасностью, услугами и качеством обслуживания – с другой стороны. Сказанное обусловлено, в том числе, тем, что в процессе информационного обмена в ТКС в течение длительного времени соответствие: бит сообщение-сигнал является фиксированным, а в качестве физических переносчиков информации – сигналов, используются сигналы, построенные с применением линейных правил (законов). Вышеуказанное позволяет нарушителю на основе определения параметров, используемых в системе сигналов, осуществить постановку помех с минимальными для себя энергетическими затратами. Объективно существуют угрозы информационной безопасности, а именно: возможность несанкционированного доступа к информационным активам, нарушение целостности, конфиденциальности, доступности данных со стороны злоумышленников, что может привести к существенному ухудшению показателей функционирования ТКС.

Основными путями решения данного противоречия является повышение помехозащищенности и информационной безопасности ТКС на основе усовершенствования методологических основ построения ТКС путем создания новых моделей, методов и технологий управления телекоммуникационными сетями, информационной безопасностью, услугами и качеством обслуживания, разработки методов информационного обмена, методов синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствам.

Для большинства приложений ТКС, в частности для широкополосных систем с многостанционным доступом, интерес представляют не пары, а большие множества последовательностей с хорошими взаимнокорреляционными свойствами, улучшенными ансамблевыми и структурными свойствами.

В статье предлагается метод синтеза дискретных последовательностей с заданными взаимнокорреляционными, структурными и ансамблевыми свойствами для применения в телекоммуникационных системах, в которых предъявляются повышенные требования к обеспечению скрытности, помехозащищенности, помехоустойчивости, информационной безопасности функционирования системы.

Концепция синтеза криптографических дискретных последовательностей символов

Различение или кодовое разделение абонентов многопользовательской ТКС основано на том, что каждому абоненту выделяется алфавит сигналов (кодовых последовательностей), с помощью которого он передает информацию. Наиболее часто используемым критерием различимости является минимум эвклидового расстояния [1]. Критерий состоит в том, что два сигнала являются легко различимыми тогда и только тогда, когда среднеквадратичное расстояние между ними велико. Необходимость совместного рассмотрения сигналов $Y(t)$ и $X(t)$ возникает при использовании манипуляции, например, в тех случаях, когда сигнал $X(t)$ модулируется двоичной последовательностью или когда им самим модулируется некоторая несущая. Таким образом, в качестве меры различимости сигналов используют величину [1]:

$$T^{-1}\int_0^T [Y(t) \pm X(t)]^2 = -T^{-1}\{\int_0^T \left[Y^2(t) + X^2(t) \right] dt \pm 2\int_0^T X(t) Y(t) dt\}, \quad (1)$$

где T – период сигналов $X(t)$ и $Y(t)$.

Первый интеграл в правой части (1) есть сумма энергий сигналов $X(t)$ и $Y(t), 0 \le t \le T$. Следовательно, при фиксированных энергиях сигнал $Y(t)$ сильно отличается как от сигнала $X(t)$, так и от сигнала $-X(t)$ только в том случае, когда параметр

$$R = \int_0^T X(t) Y(t) dt \quad (2)$$

мал.

Параметр R при решении задач поиска, обнаружения, оценки параметров (в этом случае используется согласованная фильтрация или корреляционный прием) представляет собой отклик согласованного с сигналом $Y(t)$ фильтра на входной сигнал $X(t)$. Например, если в многопользовательской ТКС с кодовым разделением сигналы $X(t)$ и $Y(t)$ выделены двум различным станциям (абонентам), то параметр R является мерой уровня взаимных помех, создаваемых каждым из сигналов приему другого.

В ТКС в качестве физического переносчика информации нашли применение различные системы (множества линейных рекуррентных последовательностей, множества Касами, Голда, Камалетдинова и др.), обладающие сравнительно небольшими значениями боковых лепестков авто- и взаимнокорреляционных функций [2]. Однако указанные сигналы обладают низкой структурной скрытностью, ограниченными ансамблевыми свойствами, а также существуют только для ограниченного числа значений периода сигнала. В случае усечения (увеличения) периода таких сигналов их корреляционные свойства ухудшаются. Поэтому актуальна задача разработки теории и практики синтеза и анализа систем дискретных сигналов с требуемыми корреляционными, структурными, ансамблевыми свойствами.

Исследования показали [3, 6, 7], что требуемые (в тех или иных условиях) показатели эффективности функционирования системы могут быть реализованы, в том числе, посредством применения широкополосных радиосистем, для которых расширение спектра осуществляется с применением нелинейных дискретных последовательностей.

В некоторых ТКС число одновременно используемых сигналов может превышать несколько сотен. Известны большие множества периодических последовательностей (множества Касами, Голда), обладающие сравнительно небольшими значениями боковых лепестков взаимнокорреляционных функций. Для генерации таких последовательностей применяются сдвиговые регистры с линейной обратной связью. Правила построения указанных классов последовательностей указывают на низкую структурную скрытность формируемых последовательностей и, следовательно, сигналов, обеспечивающих передачу информации в телекоммуникационных системах. Здесь под структурной скрытностью понимается сложность определения злоумышленником правила (закона) построения дискретной последовательности, используемой для манипуляции информационных битов.

Необходимость применения защищенных радиоканалов вынуждает исследователей поновому посмотреть как на режимы функционирования защищенных радиоканалов, так и на аспекты формирования и применения сложных сигналов. Поэтому, на наш взгляд, сегодня необходимы новые подходы и новые взгляды на процессы применения и функции сложных сигналов в целях построения защищенных ТКС. Основополагающим здесь, на наш взгляд, является новое понимание методов обеспечения информационной скрытности и имитостойкости, то есть функций, которые в традиционных системах реализуются с применением систем и средств криптографической защиты информации. Продуктивным шагом, с точки зрения нового направления использования систем сложных сигналов, является синтез так называемых систем криптографических сигналов. Синтез таких сигналов основывается на

применении ключевых данных. При этом сигналы должны обладать: абсолютной структурной скрытностью относительно законов их формирования и смены сигналов в динамическом режиме; улучшенными ансамблевыми свойствами (существовать практически для любого значения периода, иметь значительный объем системы сигналов); необходимыми для обеспечения требуемого значения помехоустойчивости корреляционными свойствами; возможностью их восстановления в пространстве и времени с применением ключей и других параметров, которые используются в синтезе сигналов.

Для защищенных радиоканалов рассматриваемые системы сигналов определяются приложениями, в которых они применяются. В частности, это могут быть как отдельные сигналы или пары сигналов, так и большие множества дискретных сигналов с необходимыми, но объективно ограниченными значениями «плотной упаковки», взаимнокорреляционными и ансамблевыми свойствами.

Под криптографическим дискретным сигналом предлагается понимать последовательность символов произвольного алфавита и произвольного периода, единственным правилом построения которого есть случайность или псевдослучайность. Такой дискретный сигнал обладает необходимыми, но ограниченными значениями «плотной упаковки», корреляционными и ансамблевыми свойствами. При таком подходе структурная скрытность сигнала обеспечивается посредством случайности или псевдослучайности.

В работе [4] сформулирована и решена задача синтеза нелинейных криптографических дискретных сигналов (КС), обеспечивающих требуемые значения помехозащищенности, информационной и структурной скрытности функционирования ТКС. В общем случае задача синтеза оптимальных бинарных криптографических сигналов заданного периода формулируется следующим образом. Необходимо найти множество дискретных двоичных последовательностей – криптографических последовательностей (КП) с заданным числом символов, обладающих допустимым уровнем максимальных боковых лепестков периодической функции автокорреляции (ПФАК). Далее, решение задачи синтеза сводится к предварительному отбору некоторого ограниченного множества дискретных последовательностей, которое кажется многообещающим в плане обеспечения необходимых взаимнокорреляционных свойств.

Необходимо отметить, что в процессе исследований была высказана гипотеза о возможности применения криптографического алгоритма в целях синтеза системы сигналов. Для этих целей был обоснован выбор Национального криптографического стандарта блочного симметричного преобразования ДСТУ 7624:2014, определяющий шифр „Калина” [5].

В табл. 1 приведены результаты синтеза КС для некоторых значений периода последовательностей. Анализ данных табл. 1 показывает, что для периода последовательности, например 64, число пар КС, соответствующее установленному предельному значению 17, составляет более $12 \cdot 10^6$ (12214869). Для последовательностей с трехуровневой функцией взаимной корреляции (ФВК) число пар, соответствующее данной «границе», составляет лишь 975. Таким образом, ансамбль нелинейных КС более чем в 10^5 раз превышает ансамбль указанных линейных сигналов. Превышение объема криптографических сигналов над ансамблем из М-последовательностей составляет более 10^7 раз.

Синтез производных систем сигналов на основе криптографических дискретных последовательностей символов

Среди систем фазоманипулированных сигналов многие образованы на базе систем Уолша [2]. Известно, что авто- и взаимнокорреляционные функции последовательностей Уолша имеют большие боковые пики. Для улучшения корреляционных свойств сигналов формируют производные системы сигналов (ПСС) посредством перемножения последовательностей Уолша (исходных последовательностей) на сигнал, который обладает определенными свойствами (производящий сигнал), в частности имеет малые боковые пики автокорреляционной функции.

Таблица 1

Период КС	Граничные значения («Плотная упаковка»)	ПФАК	АФАК	ПФВК		АФВК
		Число КС, удовлетворяющих границе «плотной упаковки»	Число КС, удовлетворяющих границе «плотной упаковки»	Общее число пар сигналов	Число КС, удовлетворяющих границе «плотной упаковки»	Число КС, удовлетворяющих границе «плотной упаковки»
31	9	7 743	3 622	29 977 024	1 465 137	14 537 423
64	17	10 868	7 166	59 056 712	12 214 869	54 822 445
127	23	3482	1302	6 062 162	47 053	1 619 780
511	59	3819	1951	7 292 380	122 835	3 466 713
1 023	100	8 513	6 194	36 235 584	5 293 538	35 083 491

Авторами сформулирована гипотеза о возможности использовать в качестве производящих – нелинейных криптографических последовательностей (КП), теоретические основы синтеза которых приведены в [4].

Метод синтеза производных систем сигналов на основе использования КС включает следующие этапы:

1. Отбор M криптографических последовательностей (КП) фиксированного периода N, обладающих минимальными значениями максимальных боковых лепестков ($R_{max.}$) ПФАК.

2. Формирование набора кодов Уолша (матрица N·N), в котором каждая строка соответствует отдельному коду.

3. Перемножение последовательностей (каждой из строк кода Уолша – исходных последовательностей) на криптографический сигнал с образованием N ПСС.

4. Исследование корреляционных свойств, образованных ПСС (в частности, ПФАК, АФАК). Для исследования функций взаимной корреляции, образуют матрицу размерностью N·N. Число таких матриц: L·N.

В качестве иллюстрации данного метода синтеза ПСС, рассмотрим код Уолша размерностью N = 64 (табл. 2).

В табл. 3 приведены КП (M = 14), отобранные из множества последовательностей, по критерию минимума значений максимальных боковых лепестков ПФАК ($R_{max} < 10$). Здесь же приведены расчеты статистических характеристик корреляционных функций (ПФАК) отобранных КС.

В табл. 4 приведены результаты исследований статистических характеристик корреляционных функций различных классов сигналов, в том числе ПСС при использовании в качестве производящих, криптографических сигналов. Расчеты проводились для различных значений периодов последовательностей (от 30 до 2052).

Анализ данных табл. 3 показывает, что статистические характеристики ПСС близки к соответствующим характеристикам линейных и нелинейных классов сигналов. При этом значения максимальных боковых пиков функций взаимной корреляции ПСС меньше, чем у широко используемых в современных ТКС линейных М-последовательностей.

Таблица 2

N = 64	1111111111111111111111111111111111111111111111111111111111111111 1010101010101010101010101010101010101010101010101010101010101010 1100110011001100110011001100110011001100110011001100110011001100 1001100110011001100110011001100110011001100110011001100110011001 1111000011110000111100001111000011110000111100001111000011110000 1010010110100101101001011010010110100101101001011010010110100101 1100001111000011110000111100001111000011110000111100001111000011 1001011010010110100101101001011010010110100101101001011010010110 1111111100000000111111110000000011111111000000001111111100000000 1010101001010101101010100101010110101010010101011010101001010101 1100110000110011110011000011001111001100001100111100110000110011 1001100101100110100110010110011010011001011001101001100101100110 1111000000000111111110000000011111111000000001111111100000000111 1010010101011010101001010101101010100101010110101010010101011010 1100001100111100110000110011110011000011001111001100001100111100 1001011001101001100101100110100110010110100101100110100101101001 1111111111111111000000000000000011111111111111110000000000000000 1010101010101010010101010101010110101010101010100101010101010101 1100110011001100001100110011001111001100110011000011001100110011 1001100110011001011001100110011010011001011001101001100101100110 1111000011110000000011110000111111110000111100000000111100001111 1010010110100101101011010010110101010010110100101010110100101101 1100001111000011001111000011110011000011110000110011110000111100 1001011010010110011010010110100110010110100101100110100101101001 1111111100000000000000000111111111111111100000000000000000111111 1010101001010101010101011010101010101010010101010101010101101010 1100110000110011001100111100110011001100001100110011001100111001 1001100101100110011001101001100110011001011001100110011001101001 1111000000000111100001111111110000111100000000111100001111111000 1010010101011010010110101010010110100101010110100101101010100101 1100001100111100001111001100001111000011001111000011100001111000 1001011001101001011010011001011001101001100101101001011001101001 1111000000000111100001111111110000111100000000111100001111111000 1010010101011010010110101010010110100101010110100101101010100101 1100001100111100001111001100001111000011001111000011100001111000 1001011001101001011010011001011001101001100101101001011001101001 1111111111111111111111111111111111000000000000000000000000000000 1010101010101010101010101010101010010101010101010101010101010101 1100110011001100110011001100110000110011001100110011001100110011 1001100110011001100110011001100101100110011001100110011001100110 1111000011110000111100001111000000001111000011110000111100001111 1010010110100101101001011010010101011010010110100101101001011010 1100001111000011110000111100001100111100001111000011110000111100 1001011001101001011010011001011001101001100101101001011001101001

Таблица 3

1	1110001111101000011111011100110011000101000110101101001001100101
2	1000010010000100101111001101000000011001001000001011100111001101
3	0000100100001001011100110100000001100100100000101110011100111011
4	0000100100001001011100110100000001100100100000101110011100111011
5	0001001000010010111001101000000011001001000001011100111001110110
6	0100100001001011100110100000001100100100000101110011100111011000
7	0000100101110011010000000110010010000010111001110011101100010110
8	0001001011100110100000001100100100000101110011100111011000101101
9	0010010111001101000000011001001000001011100111001110110001011010
10	0100101110011010000000110010010000010111001110011101100010110100
11	0000000010100010011000001111100001101101110001101000010111100101
12	0000000101000100110000011111000011011011100011010000101111001010
13	0000001010001001100000111110000110110111000110100001011110010100
14	0100011110001100000100110010000000011011111011100101011000010110

Расчет статистических характеристик корреляционных функций (ПФАК) КС

1)64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8 0
PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875 DISP: 0.5763694553724894 |DISP|: 0.3384787011890674

2)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

3)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

4)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

5)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

6)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

7)64 4 -8 4 4 0 0 4 -4 4 0 -8 4 0 4 0 4 0 -8 0 0 8 0 0 -8 -4 -4 4 8 4 4 4 -4 4 4 4 8 4 -4 -4 -8 0 0 8 0 0 -8 0 4 0 4 0 4 -8 0 4 -4 4 0 0 4 4 -8 4
PFAKmin: 4 PFAKmax: -8 MO: 0.0703125 |MO|: 0.4296875 DISP: 0.5553298776598447 |DISP|: 0.350712702793093

8)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

9)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

10)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0
PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

11)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

12)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

13)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8
PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

14)64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -8 -4 4 -4 -4 4 0 0 4 4 -4 8
PFAKmin: -4 PFAKmax: 8 MO: 0.0 |MO|: 0.5 DISP: 0.6236095697723273 |DISP|: 0.3618734420321171

Результаты исследования ПФВК ПСС на основе КП показывают, что число пар сигналов для периода последовательностей 64 символов, для которых значения R_{max} не превышают 17 (это так называемая граница «плотной упаковки», достигаемая в классе лучших, с точки зрения ВКФ, последовательностей с трехуровневой ПФВК), составляет 604 пары (около 30 % из общего числа возможных сочетаний пар сигналов). Число пар сигналов, для которых значения R_{max} не превышают 20 – 1577, что составляет 77 % от общего числа пар сигналов. При границе $R_{max} < 25$ максимальное количество отобранных пар сигналов составляет 1984 (96,8 %). Значения максимальных боковых пиков ПФВК $R_{max} < 25$ имеют место для последовательностей, получивших наибольшее распространение в современных телекоммуникационных системах – М-последовательности.

Выводы

Рассмотренный класс сложных производных сигналов, полученный с применением предложенного метода на основе использования нелинейных криптографических сигналов, обладает, с одной стороны, структурными свойствами, аналогичными свойствам случайных (псевдослучайных) последовательностей, а с другой – улучшенными ансамблевыми и корреляционными свойствами.

Характеристики авто- и взаимных функций корреляции таких сигналов не уступают характеристикам лучших, с точки зрения корреляционных свойств, дискретных последовательностей (М-последовательностей, множеств Голда и Касами, ансамблей Камалетдинова и др.). Кроме того, системы криптографических сигналов (КС) существуют и обладают указанными выше свойствами для широкого спектра значений периода последовательностей. Также необходимо отметить особое свойство таких систем сигналов – возможность их восстановления в пространстве и времени с применением ключей и ряда других параметров, которые используются в процессе синтеза сигналов.

Приведенные характеристики систем сигналов, синтезируемых с применением разработанного метода, позволяют говорить об улучшении качественных показателей функционирования телекоммуникационной системы: помехозащищенности и информационной безопас-

ности. Улучшение указанных показателей достигается, в частности, за счет возможности формирования, с применением полученного метода, больших ансамблей дискретных последовательностей практически любого периода с необходимыми (для тех или иных приложений системы) значениями боковых лепестков функций авто-, взаимной и стыковой функции корреляции в периодическом и апериодическом режимах работы, а также статистическими характеристиками корреляционных функций (КФ), не уступающих аналогичным характеристикам лучших, с точки зрения КФ, линейных классов сигналов. Указанное дает возможность повысить помехоустойчивость приема сигналов.

Таблица 4

Тип сигналов	Характеристики	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{(R)}}{\sqrt{N}}$
Нелинейные характеристические последовательности	АФАК	1,6 – 2,4	0,3 – 3,4	1,4 – 7,7	1,9 – 10,8
	ПФАК	0,02 – 0,5	0,02 – 0,3	0,03 – 0,3	0,06 – 05
	АФВК	1,3 – 3,3	0,5 – 0,7	2,4 – 18,2	3,6 – 27
	ПФВК	0,8 – 3,3	0,7 – 0,8	5,8 – 45,3	5,9 – 45,3
ПСС	АФАК	0,8 – 2,4	0,4 – 0,5	0,9 – 1	1 – 1,1
	ПФАК	0,7 – 2,5	0,2 – 0,7	0,2 – 0,5	0,3 – 0,9
	АФВК	1 – 2,5	0,2 – 0,7	0,2 – 0,5	0,3 – 0,7
	ПФВК	1,4 – 2,8	0,2 – 0,7	0,4 – 0,5	0,6 – 0,9
Нелинейные криптографические последовательности	АФАК	0,7 – 2,5	0,4 – 0,5	0,9 – 1	0,9 – 1,2
	ПФАК	0,9 – 2,5	0,3 – 0,7	0,2 – 0,5	0,3 – 0,9
	АФВК	1,2 – 2,7	0,4 – 0,7	0,3 – 0,5	0,5 – 0,7
	ПФВК	1,5 – 2,8	0,5 – 0,7	0,3 – 0,5	0,8 – 0,9
Линейные М-последовательности	АФАК	0,7 – 1,25	0,32	0,26	0,41
	ПФАК	$1/\sqrt{N}$	$1\sqrt{N}$	0	0
	АФВК	1,4 – 5,0	0,54	0,48	0,73
	ПФВК	1,9 – 6,0	0,8	0,62	1

Разработаны математическое и программное обеспечение, реализующее предложенный метод, и вычислительные алгоритмы синтеза систем сложных нелинейных дискретных криптографических сигналов, а также производных систем сигналов, для которых в качестве производящих используют КС. Разработанное программное обеспечение позволяет: генерировать нелинейные КС практически для любого периода; определять значения минимальных и максимальных боковых выбросов различных корреляционных функций; сравнивать полученные значения с известными, потенциально достижимыми границами для соответствующих корреляционных функций; присваивать реализациям синтезированных последовательностей, а также параметрам, используемым для синтеза сигналов, уникальные идентификаторы (специальные радиоданные), которые необходимы при оптимальной обработке сигналов; рассчитывать статистические характеристики различных корреляционных функций синтезированных сигналов; проводить исследования ансамблевых характеристик синтезированных сигналов. Программное и математическое обеспечение, полученное в ходе исследований, реализующее методы синтеза и исследования свойств систем нелинейных сигналов, в том числе ПСС, практически готово к возможному использованию в составе опытных образцов и элементов современных цифровых коммуникационных средств.

Список литературы: 1. *D.V. Sarvate, M.V. Pursley* Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. Vol. Com 68-5, 1980. 2. *Варакин, Л. Е.* Системы связи с шумоподобными сигналами / Варакин Л. Е. – 1985. – 384 с. 3. *Горбенко, И.Д.* Синтез систем сложных сигналов с заданными свойствами корреляционных функций для приложений многопользовательских систем с кодовым разделением абонентов / А.А.Замула, Е.А. Семенко // Системи обробки інформації. – Х. : ХУПС, 2014. – Вип. 9 (125).– С. 25 – 30. 4. *Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. Vol. 75, 2016 Issue 2. pages 169-178. 5. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015. 6. *Karpenko, O., Kuznetsov, A., Sai V. Stasev Yu*.. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. Vol. 71, 2012 Issue 1. pages 91-98. 7. *Stasev, Yu.V., Kuznetsov, A.A., Nosik, A.M.* Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Vol.43, Issue 1, January 2007, Pages 1 – 11.

Харьковский национальный университет
имени В.Н. Каразина

Поступила в редколлегию 25.11.2016