Раздел IV. Безопасность телекоммуникационных систем

УДК 681.3.016

В.Т. Корниенко

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ УСЛОВНОГО ДОСТУПА ПРИ РАССЫЛКЕ ГРУППОВОГО КЛЮЧА

Целью статьи является разработка методики повышения эффективности рассылки ключевой информации в системах условного доступа. Решение задачи основано на использовании кода Рида–Маллера. Рассмотрены вопросы прикладного использования кодов Рида–Маллера в системах кодирования в зашумленных каналах связи и процедурах формирования ключей. В приложении к обобщенному алгоритму скремблирования, предусматривающему рассылку ключей и передачу зашифрованных сообщений управления доступом и условного доступа в цифровом потоке без скремблирования, рассмотрено применение кода Рида–Маллера первого порядка для кодирования потока ключевой информации. Предложено применение кодов Рида–Маллера для повышения криптостойкости передачи и высокой корректирующей способности при декодировании информации. Описан один из возможных вариантов мажоритарного способа декодирования. Указано на применение многоуровневой иерархии ключей для снижения количества рассылок группового ключа и предложена многоуровневая иерархия процесса кодирования, заключающаяся в распараллеливании процесса кодирования для сокращения длины кодового слова Рида–Маллера и повышения кодовой скорости при заданных требованиях к вероятности ошибки. Приведен выигрыш в снижении рассылок ключей в зависимости от количества абонентов для четырехуровневой иерархии. Представлены численные расчеты в зависимости от числа информационных разрядов длины кодового слова Рида–Маллера, числа исправляемых разрядов, вероятности ошибочного приема и кодовой скорости при четырех уровнях иерархии. Эксперимент проведен на основе технологии виртуальных приборов LabVIEW. Представлены результаты проделанной работы в виде библиотечного модуля кодера Рида–Маллера первого порядка.

Система условного доступа; рассылка группового ключа; коды Рида–Маллера; многоуровневая иерархия; виртуальный прибор LabVIEW.

V.T. Kornienko

CONDITIONAL ACCESS SYSTEM EFFICIENCY INCREASING AT DISPATCH OF A GROUP KEY

The purpose is to examine ways to improve efficiency of key information dispatching in the conditional access system. The problem is solved using the Reed-Mahler codes. The applications of Reed-Muller coding in noisy channels of communication systems and procedures for key generation was denoted. Attached to the common scrambling algorithm (CSA), comprising key distribution and transmission of encrypted messages of access control and conditional access without scrambling, the use of first order Reed-Muller code is considered to encode the stream of key information. It deals with Reed-Muller codes application for improving unauthorized decryption effort and high error correction ability in information decoding. One of possible variants of a majority way of decoding was described. It is pointed that multilevel key hierarchy was applied to reduce the cost of rekeying. The paralleling encoding process was proposed as multi-level hierarchy encoding which consists in to reduce the Reed-Muller codeword length and improve code rate

with specified requirements for the probability error. The odd of winning in reducing dispatches keys depending on the number of subscribers for the four-tier hierarchy is introduced. Simulation results of the Reed-Mahler codeword length, the number of corrected bits, the probability error and the code rate versus the number of data bits for four hierarchical levels were illustrated. As a result of the LabVIEW virtual devices experiment, which are carrying out for represented parameters of code, simulation output was represented. It is introduced that library modules for Reed-Muller encoder&decoder realization by LabVIEW means were created.

Conditional access system; group key dispatch; Reed-Muller codes; multilevel key distribution; LabVIEW virtual device.

Введение. Известно, что в системах условного доступа цифрового телевещания криптостойкость обеспечивается использованием комбинации методов скремблирования и шифрования [1]. Использованием обобщенного алгоритма скремблирования (CSA) предусматривает рассылку ключей [1]. Для регулярного обновления ключа в целях повышения криптостойкости, в случаях подключения новых абонентов в систему условного доступа и в случаях удаления пользователей из системы требуется повторная рассылка ключевой информации. Применение одноуровневых протоколов групповой рассылки ключей снижает пропускную способность системы, поэтому используется многоуровневая ключевая иерархия [1]. Современные системы условного доступа поддерживают до 20 млн абонентских устройств, обеспечивая автоматическое многоканальное управление до 2048 сервисов и скорость транспортного потока до 108 Мбит/с, при этом длина ключей составляет до 256 бит.

В системах условного доступа мультиплексированный поток видео, звука и данных передается скремблированием, в то время как зашифрованные сообщения управления доступом (ECM) и условного доступа (EMM) передаются в цифровом потоке без скремблирования [1]. Во первых, воздействие помех в каналах связи приводит к искажению передаваемых сигналов и к частичной потере информации. Во вторых, несмотря на частое обновление ключевой информации в сообщении ECM и достаточно редкое обновление ключевой информации в сообщении EMM [1], данные сообщения подвержены атакам с целью завладения ключевой информации и несанкционированного доступа к содержимому каналов передачи данных, поскольку нескремблированный поток EMM и ECM, благодаря некоторым особенностям, выделяется от скремблированного потока данных. Поэтому достаточно актуальной является задача канального кодирования сообщений EMM и ECM.

Проанализировав наиболее известные помехоустойчивые коды с относительной простой реализации операций кодирования/декодирования и на стойкость к пакетам ошибок, выбор пал на семейство кодов Рида–Маллера. В ряде работ рассмотрены вопросы их прикладного использования в системах кодирования в зашумленных каналах связи [2–4] и процедурах формирования ключей известных криптосистем [5, 6].

Симметричная решетчатая структура кодов Рида–Маллера увеличивает скорость декодирования за счет рекурсивного построения и позволяет реализовать турбокодек, результаты практической реализации которого представлены для 32-битного турбокода Рида–Маллера со скоростью кодирования 38,6 Мбит/с и скоростью декодирования 70,2 кбит/с [3]. Также известна практическая реализация высококорректирующего 32-битного кодека Рида–Маллера для радистанции системы радиосигнализации со скоростью передачи пакетов до 426 бит/с [7]. Применение кода Рида–Маллера демонстрирует преимущество по сравнению с использованием шумоподобных сигналов при близких к единице отношениях сигнал/помеха и вы-

соких требованиях к достоверности передачи сообщений и, как показано в работе [8] позволяет увеличить информационную скорость передачи до двух раз. Представители семейства кодов Рида–Маллера широко используются в высокоэффективных помехоустойчивых кодеках систем мобильной связи: коды Рида–Соломона являются крайними случаем в семействе кодов Рида–Маллера относительно многочленов от одной переменной большой степени, с одной стороны, и с другой стороны – коды Адамара с многочленами от многих переменных первой степени [9–12].

Коды Рид–Маллера применяются при формировании открытых ключей криптосистемы Мак–Элиса–Сидельникова за счет использования произвольного числа блоков кода [5, 6, 13, 14]. Криптографические свойства кодов рассмотрены и в работе [15]. Известны также примеры атак на криптосистему, построенную на основе кодов Рида–Маллера [16].

Постановка задачи. Для повышения эффективности передачи ключевой информации в системе условного доступа рассмотрим использование многоуровневой иерархии ключей для снижения количества рассылок группового ключа и применение помехоустойчивого кода Рида–Маллера при передаче ключевой информации по каналу связи, приводящее к улучшению криптостойкости из-за увеличения размера зашифрованного ключа за счет его кодирования и оптимизации кодовой скорости при заданных требованиях к вероятности ошибки.

Методы решения. Предлагается методика повышения эффективности рассылки ключевой информации в системах условного доступа, которая заключается в использовании многоуровневой иерархии ключей и помехоустойчивого кодирования ключевой информации. Такой подход позволяет повысить такие показатели эффективности, как количество рассылок группового ключа, вероятность ошибочного приема и кодовую скорость.

Для рассматриваемой задачи рассылки ключевой информации в системе условного доступа используем многоуровневую иерархию ключей [1], позволяющую снизить количество рассылок группового ключа пропорционально $N_P = k \cdot log_k N - 1$, где k – число ветвлений ключевого дерева, N – количество абонентов, что показано в табл.1 коэффициентом выигрыша N_B =N / N_P в снижении рассылок в зависимости от количества абонентов для четырехуровневой иерархии (k = 4). Например, при количестве абонентов N = 1024 удается снизить количество рассылок группового ключа с 1024 до 19.

Таблица 1

Выигрыш в снижении рассылок ключей в зависимости от количества абонентов для четырехуровневой иерархии

Количество абонентов	128	256	512	1024	2048
Выигрыш в снижении числа рассылок ключа	13	17	31	54	98

Используя иерархию и при помехоустойчивом кодировании ключевой информации, заключающуюся в распараллеливании процесса кодирования (рис. 1), с учетом приведенных параметров кода Рида–Маллера первого порядка можно заключить, что кодирование 64-битного ключа ограничено 4-уровневой иерархией, 128-битного ключа – 5-уровневой иерархией, а 256-битного ключа – 6-уровневой иерархией. Это позволяет при заданных требованиях к вероятности ошибки сократить размерность кодовых слов Рида–Маллера и повысить скорость передачи при помехоустойчивом кодировании.

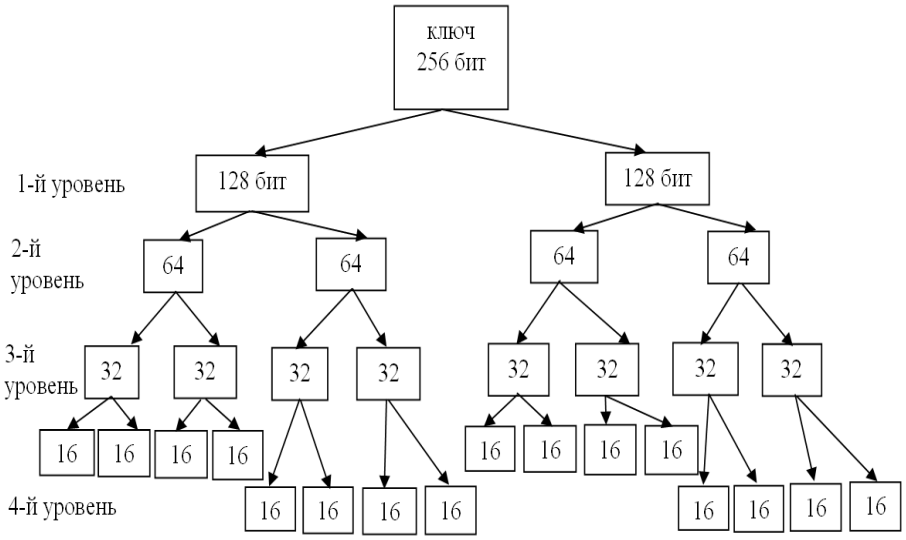

Рис. 1. Четырехуровневая иерархия при кодировании ключевого потока данных

Код Рида–Маллера характеризуется порядком h и степенью m, поэтому при общем обозначении для линейных кодов (n, k, d), имеющих кодовое расстояние d, длину $n=2^m$ символов при кодировании k информационных разрядов, код Рида–Маллера имеет специальное обозначение $R(h, m)$. Код Рида–Маллера порядка h при кодировании $n_u = m+1$ информационных разрядов представляет собой блочный неразделимый код с минимальным кодовым расстоянием $d_{min} = 2^{m-h} = 2^{nu-1-h}$ [10]. Длина кодовой комбинации натурального кода Рида–Маллера составляет $n = 2^{nu-1}$ разрядов, тогда коэффициент избыточности можно оценить как $к_{изб} = 1 - n_u / 2^{nu-1}$ и объем кода равен $A_n = 2^n$. При декодировании код Рида–Маллера позволяет исправить n_β ошибок и обнаружить без исправления $n_\alpha > n_\beta$ ошибок, при этом минимальное кодовое расстояние $d_{min} = n_\alpha + n_\beta + 1$. Вероятность ошибочного приема двоичного символа при длине кодовой комбинации кода Рида–Маллера n составляет $P_{ош} = n_\beta / n$, а кодовая скорость может быть оценена как $V_k = n_u / n$.

Рассмотрим код Рида–Маллера первого порядка (h =1) для которого задана порождающая матрица G [17], и если на вход кодера поступает сигнальный вектор a, то получим сформированный набор кодовых слов Рида–Маллера

$$R = a \odot G,$$

где $\odot$ – знак, обозначающий скалярное произведение двоичного вектора и двоичной матрицы в заданном пространстве V_n по правилу [17]

$$R = a \odot G = a_1 \cdot V_1 \oplus a_2 \cdot V_2 \oplus \cdots \oplus a_{пи} \cdot V_{пи},$$

где V_i – i-й базисный вектор (строка длины $n > n_u$) порождающей матрицы, $i=1, n_u$; $a_i \cdot V_i$ – операция логического умножения переменной a_i на вектор V_i ; $\oplus$ – операция поразрядного сложения по модулю два.

На приемной стороне канала связи в результате действия вектора ошибок e, создаваемого двоичным симметричным каналом, принятый с искажениями кодовый вектор аддитивен $R^{\wedge} = R + e$. Декодирование кодовой комбинации

Рида–Маллера может быть проведено с использованием принципа максимального правдоподобия, синдромного декодирования или на основе мажоритарной логики [18–25]. При известной проверочной матрице H, такой, что $G \cdot H^T = 0$, кодовые слова R удовлетворяют условию $R \cdot H^T = 0$. Вычисление синдрома как линейного преобразования вектора ошибок $s = R^{\wedge} \cdot H^T = (R + e) \cdot H^T = e \cdot H^T$ позволяет исправить n_β ошибок и обнаружить без исправления $n_\alpha > n_\beta$ ошибок ($d_{min} = n_\alpha + n_\beta + 1$).

Один из возможных вариантов мажоритарного способа декодирования производится следующим образом. Из символов R_i образуются $(n_u - 1)$ групп контрольных сумм пар символов по модулю два. При этом в первой группе складываются пары символов, интервал между которыми равен 2^0, во второй группе – пары с интервалом между символами равным 2^1, в третьей группе – с интервалом 2^2, в четвертой – с интервалом 2^3 и так далее до значения интервала, равного 2^{nu-2}.

Решение о значении переданного информационного символа исходной комбинации принимается по большинству значений контрольных сумм в группе. Для вынесения решений о значении старшего символа a_{nu} формируется вектор

$$W = \hat{R} \oplus a_1 \cdot V_1 \oplus a_2 \cdot V_2 \oplus \ldots \oplus a_{(n_u - 1)} \cdot V_{(n_u - 1)},$$

где $R^{\wedge}$ – вектор кодовой комбинации Рида–Маллера, возможно искаженный в процессе передачи.

Значение старшего символа a_{nu} принимается по большинству значений в кодовом векторе W.

Признаком возникновения обнаруживаемой n_α-кратной ошибки является паритет нулей и единиц, получаемых в $(n_u - 1)$ группа проверок.

Зависимости длины кодового слова Рида–Маллера от числа информационных разрядов n_u при 4-х уровнях иерархии, зависимости числа исправляемых разрядов от числа информационных, зависимости вероятности ошибочного приема от числа информационных разрядов n_u и зависимости кодовой скорости приведены в табл. 2, 3, 4 и 5 соответственно.

Как следует из приведенных зависимостей применение многоуровневой иерархии и при распараллеливании процесса кодирования, например, при длине 16-битного ключа при двухуровневой иерархии, т.е. распараллеливании на 4 канала позволяет сократить длину кодового слова Рида–Маллера в 1024 раза, порядок выигрыша же при 256-битном ключе для четырехуровневой иерархии при распараллеливании на 16 каналов имеет огромное значение.

При этом пропорционально увеличивается кодовая скорость, обеспечивая коэффициент выигрыша для размеров ключа от 64 до 256 бит для четырехуровневой иерархии в огромное число порядков. Ценою таких преимуществ является уменьшение числа обнаруживаемых и исправляемых ошибок, но этот факт не существенно сказывается на вероятности ошибки, которая может быть уменьшена всего лишь с 0,25 до 0,24. Как следует из рассмотрения несколько лучших показателей, можно достичь при распараллеливании процесса кодирования по небольшому количеству информационных разрядов, например по 5, 6, 7, 9 с добавлением нулями недостающих разрядов информационного кода. Но это является предметом отдельного рассмотрения.

Таблица 2

Длина кодового слова Рида–Маллера в зависимости от числа информационных разрядов при 4-х уровнях иерархии

Число информационных разрядов ключа	8	12	16	32	64	128	256
Без распараллеливания	128	2048	32768	$2{,}14\cdot10^{9}$	$9{,}22\cdot10^{18}$	$1{,}7\cdot10^{38}$	-
Для первого уровня иерархии (2 канала)	16	64	256	65536	$4{,}29\cdot10^{9}$	$1{,}85\cdot10^{19}$	-
Для второго уровня иерархии (4 канала)	-	-	32	512	131072	$8{,}59\cdot10^{9}$	-
Для третьего уровня иерархии (8 каналов)	-	-	-	64	1024	262144	$1{,}71\cdot10^{10}$
Для четвертого уровня иерархии (16 каналов)	-	-	-	-	128	2048	524288

Таблица 3

Число исправляемых разрядов в зависимости от числа информационных разрядов при 4-х уровнях иерархии

Число информационных разрядов ключа	8	12	16	32	64	128	256
Без распараллеливания	31	511	4095	536870911	$2{,}31\cdot10^{18}$	-	-
Первый уровень иерархии (2 канала)	2	14	62	16382	$1{,}07\cdot10^{9}$	-	-
Четвертый уровень иерархии (16 каналов)	-	-	-	-	16	496	131056

Таблица 4

Вероятность ошибочного приема в зависимости от числа информационных разрядов при 4-х уровнях иерархии

Число информационных разрядов ключа	8	12	16	32	64	128	256
Без распараллеливания	0,2422	0,2495	0,2499	0,25	0,25	0,25	0,25
Первый уровень иерархии (2 канала)	0,125	0,2188	0,2422	0,2499	0,25	0,25	0,25
Четвертый уровень иерархии (16 каналов)	-	-	-	-	0,125	0,2422	0,2499

Таблица 4

Кодовая скорость в зависимости от числа информационных разрядов при 4 уровнях иерархии

Число информационных разрядов ключа	8	12	16	32	64	128	256
Без распараллеливания	0,0625	0,0059	0,0005	10^{-8}	-	-	-
Первый уровень иерархии (2 канала)	0, 5	0,1875	0,0625	0,0005	$1{,}49 \cdot 10^{-8}$	-	-
Четвертый уровень иерархии (16 каналов)	-	-	-	-	0, 5	0,0625	0,0005

В предлагаемом варианте применения кода Рида–Маллера при кодировании 64-, 128- и 256-битных ключей при 4-уровневой иерархии в 16 кодовых словах соответствующей длины 128, 2048 и 524288 бит соответственно в каждом слове передается 4, 8 и 16 бит информации, а при декодировании могут быть исправлены соответственно 16, 496 и 131056 ошибок, при этом вероятность ошибочного приема двоичного символа в канале составляет 0,125, 0,242 и 0,249 соответственно. Кодирование ключевой информации осуществляется в зависимости от длины ключа. В первой кодовом слове передается количество информационных байт в пакете, а затем идут кодовые слова данных, а прием информации начинается с синхропосылки, состоящей из преамбулы, необходимой для тактовой синхронизации, и старт-стопного сигнала, определяющего начало пакета информации.

Экспериментальное исследование. Используя известные подходы для применения технологии создания виртуальных приборов LabVIEW при реализации кодеков в системах передачи данных [26–28], в качестве примера рассмотрим приведенный эксперимент кодера Рида–Маллера строки текстового сообщения на основе виртуального прибора LabVIEW. Для чтения текстовой строки, преобразования строковых данных в коды символов, преобразования кодов символов в двоичный 8-разрядный код и осуществления операции кодирования с распараллеливанием обработки можно использовать алгоритм, реализованный во фрагменте диаграммной панели виртуального прибора LabVIEW, приведенной на рис. 2.

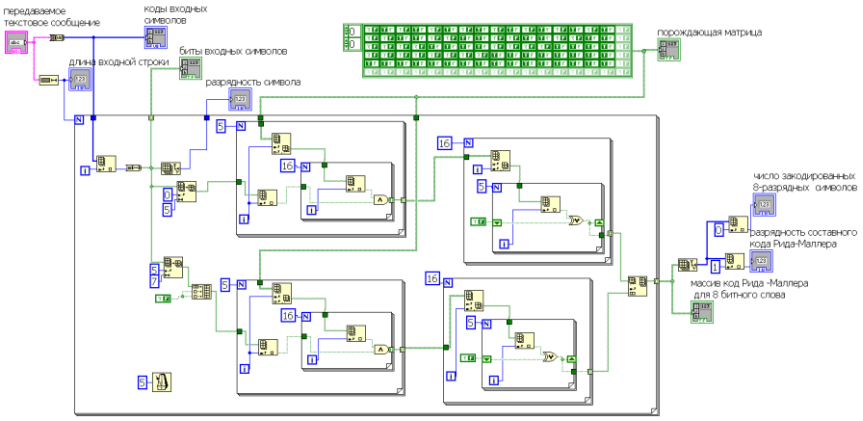

Рис. 2. Фрагмент диаграммной панели виртуального прибора кодера Рида–Маллера для кодирования текстового потока данных

Поскольку в приведенном примере алгоритма Рида–Маллера кодом R(1,4) используется 5 информационных бит, то двоичный 8-разрядный код текстового символа разбивается на 5 и 3 бита, к последним из которых добавляются 2 разряда, которые заполняются нулями или могут быть дополнительными служебными битами, и таким образом кодирование 8-разрядного информационного блока распараллеливается на два канала. Приведенный пример позволяет осуществить помехоустойчивую передачу 8 бит данных 32-разрядным кодом с исправлением 6-элементного вектора ошибки или обнаружением 8-элементного вектора ошибки.

Все вышеприведенные численные значения получены в результате экспериментального тестирования разработанного виртуально прибора. В итоге, пользуясь возможностями LabVIEW, создан библиотечный модуль – вложенный виртуальный прибор кодера Рида–Маллера первого порядка (рис. 3), который можно использовать при создании других виртуальных приборов для анализа помехоустойчивых систем передачи информации. Реализация описанного кодека возможна на базе доступной высокопроизводительной системы цифровой обработки сигналов на базе сигнального процессора NI SPEEDY-33, программируемой DSP-модулем LabVIEW, но это также предмет отдельного рассмотрения.

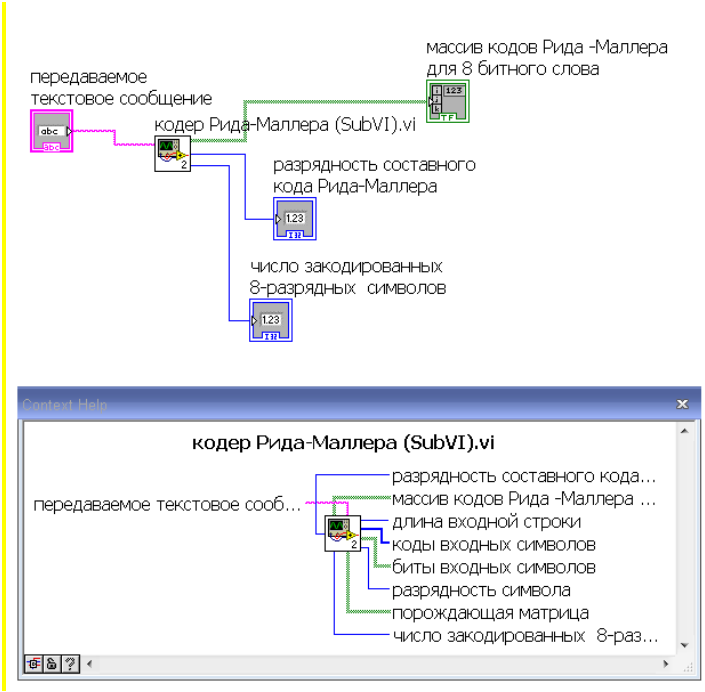

Рис. 3. Библиотечный модуль – вложенный виртуальный прибор кодера Рида–Маллера

Заключение. Таким образом, разработанная методика повышения эффективности рассылки ключевой информации в системах условного доступа, заключающаяся в повышении таких показателей эффективности, как количество рассылок группового ключа, вероятность ошибочного приема и кодовая скорость, позволяет достичь следующих результатов:

1) использование четырехуровневой иерархии при рассылке ключей позволяет снизить количество рассылок группового ключа при количестве абонентов $N = 1024$ в 54 раза;

2) использование 4-уровневой иерархии при кодировании Рида–Маллера ключей размерностью 64, 128 и 256 бит в 16 кодовых словах соответствующей длины 128, 2048 и 524288 бит позволяет передавать соответственно в каждом слове 4, 8 и 16 бит информации, а при декодировании исправлять соответственно 16, 496 и 131056 ошибок;
3) применение кодов Рида–Маллера для кодирования ключей из-за увеличения длины закодированного ключа позволяет повысить криптостойкость передачи;
4) использование 4-уровневой иерархии кодирования позволяет получить коэффициент выигрыша по вероятности ошибочного приема двоичного символа в канале при рассылке коротких 64-битных ключей в 2 раза и несущественные коэффициенты выигрыша при рассылке длинных 128- и 256-битных ключей соответственно в 1,03 и 1,004 раза;
5) использование 4-уровневой иерархии кодирования позволяет повысить кодовую скорость при рассылке коротких 64-битных ключей от 10^{-18} до 0,5 и при рассылке длинных 128- и 256-битных ключей соответственно до 0,06 и 0,0004.
6) создан библиотечный модуль LabVIEW кодера Рида–Маллера первого порядка, который можно использовать при создании других виртуальных приборов для анализа помехоустойчивых систем передачи информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Cruickshank H., Howarth M.P., Iyengar S., Sun Z.* A Comparison between satellite DVB conditional access and secure IP multicast // ESA Contract 16996/02/NL/US Octalis, 2003.
2. *Нейдорф Р.А., Новиков С.П., Чудаков В.С.* Практическая методика расчета данных для выбора принципов кодирования и их параметров в зашумленных каналах связи сетецентрических систем // Известия ЮФУ. Технические науки. – 2011. – № 3 (116). – С. 109-120.
3. *Яременко А.В., Осокин А.Н.* Реализация турбокодека на программируемой логической интегральной схеме // Вестник науки Сибири. Сер. 6. Информационные технологии и системы управления. – 2011. – № 1 (1).
4. *Зяблов В.В., Рыбин П.С.* Сравнение методов передачи по параллельным каналам // Труды 30-й конференции молодых ученых и специалистов ИППИ РАН им. А.А. Харкевича Российской академии наук «Информационные технологии и системы» (ИТиС’07). – М.: ИППИ РАН, 2007. – С. 99-103.
5. *Чижов И.В.* Эквивалентные подпространства кода Рида–Маллера и пространство ключей криптосистемы Мак–Элиса–Сидельникова // Тезисы докладов VIII Сибирской научной школы-семинара с международным участием. Компьютерная безопасность и криптография – SIBECRYPT’09, 2009. – С. 36-38.
6. *Чижов И.В.* Ключевое пространство криптосистемы Мак–Эллиса–Сидельникова // Дискретная математика. – 2009. – Т. 21 (3). – С. 132–158.
7. Руководство по настройке, установке и эксплуатации радиомодема гранит Р-43АЦ. ООО «Радиокоммуникационные системы».
8. *Биккенич Р.Р., Хворов С.Д.* Помехоустойчивость системы с псевдослучайными сигналами и кодом Рида–Маллера // Телекоммуникации. – 2011. – № 11. – С. 42-48.
9. *Ромащенко А.Е., Румянцев А.Ю., Шень А.А.* Заметки по теории кодирования. – М.: МЦНМО, 2011. – 80 с.
10. *Соловьева Ф.И.* Введение в теорию кодирования: Учебное пособие. – Новосибирск: Новосибирский гос. университет, 2006. – 127 с.
11. *Richard D. van Nee* OFDM codes for peak-to-average power reduction and error correction // IEEE Globecom, London, U.K., 1996. – P. 740-744.
12. *Davis J.A., Jedwab J.* Peak-to-mean power control and error correction for OFDM transmission using Goley sequences and Reed–Muller codes // Electron. Lett. – 1997. – Vol. 33. – P. 267-268.
13. *Сидельников В.М.* Открытое шифрование на основе двоичных кодов Рида–Маллера // Дискретная математика. – 1994. – Т. 6. – Вып. 3. – С. 3-20.

14. *Чижов И.В.* Пространство ключей криптосистемы Мак–Элиса–Сидельникова: автореф. дисс. … канд. физ.-мат. наук. – М., 2010.
15. *Canteaut A., Carlet C., Charpin P., Fontaine C.* On cryptographic properties of the cosets // IEEE Trans. Inf. Theory. – 2001. – Vol. 47, No 4. – P. 1949-1513.
16. *Бородин М., Чижов И.* Эффективная атака на криптосистему Мак–Элиса, построенную на основе кодов Рида–Маллера // Дискретная математика. – 2014. – Т. 1, № 26. – С. 10-20.
17. *Морелос–Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2005. – 320 с.
18. *Helleseth T., Klove T., Levenshtein V. I.* Error-correction capability of binary linear codes // IEEE Trans. Inf. Theory. – 2005. – Vol. 51, No. 4. – P. 1408-1423.
19. *Kenji Yasunaga, Toru Fujiwara.* On Correctable Errors of Binary Linear Codes // IEEE Transactions on information theory. – 2010. – Vol. 56, No. 6. – P. 2537.
20. *Alexander J. Grant, Richard D. van Nee.* Efficient Maximum-Likelihood Decoding of Q-ary Modulated Reed–Muller Codes // IEEE Communications letters. – 1998. – Vol. 2, No. 5. – P. 134-138.
21. *Dumer I., Kabatiansky G., Tavernier C.* Fast list decoding of Reed–Muller codes up to their distances // Proc. XI Int. Workshop Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria. 2008. – P. 82-85.
22. *Dumer I., Kabatiansky G., Tavernier C.* List decoding of Reed–Muller codes up to the Johnson bound with almost linear complexity // Proc. 2006 IEEE Int. Symp. Information Theory, USA. 2006. – P. 138-142.
23. *Kabatiansky G., Tavernier C.* List decoding of Reed–Muller codes of the first order // Proc. IX Int. Workshop Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria. 2004. – P. 230-235.
24. *Paterson K.G., Jones A.E.* Efficient decoding algorithms for generalized Reed–Muller codes // Technical Report HPL-98-195. Hewlett–Packard Labs., Bristol, 1998.
25. *Ashikhmin, Litsyn S.N.* Fast decoding algorithms for first order Reed–Muller and related codes // Desifn, Codes and Cryptography. – 1996. – Vol. 7. – P. 187-214.
26. *Корниенко В.Т.* Использование виртуальных приборов LabVIEW в учебном процессе для скремблирования цифрового потока данных // Известия ЮФУ. Технические науки. – 2013. – № 11 (148). – С. 182-186.
27. *Корниенко В.Т.* Оценка коэффициента сжатия кодера Хаффмана в виртуальном лабораторном эксперименте LabVIEW // Сборник научных трудов по итогам международной научно-практической конференции «Новые технологии и проблемы технических наук». – Красноярск, 2014. – С. 107-110.
28. *Корниенко В.Т.* Повышение эффективности передачи данных в системах с интерфейсом Wiegand // Сборник научных трудов по итогам Международной научно-практической конференции «Технические науки в мире: от теории к практике». – Ростов-на-Дону, 2014. – С. 67-69.

REFERENCES

1. *Cruickshank H., Howarth M.P., Iyengar S., Sun Z.* A Comparison between satellite DVB conditional access and secure IP multicast, *ESA Contract 16996/02/NL/US Octalis*, 2003.
2. *Neydorf R.A., Novikov S.P., Chudakov V.S.* Prakticheskaya metodika rascheta dannykh dlya vybora printsipov kodirovaniya i ikh parametrov v zashumlennykh kanalakh svyazi setetsentricheskikh sistem [Practical design procedure of the data for the choice of principles of coding and their parameters in communication channels with noise of setetsentrichesky systems], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2011, No. 3 (116), pp. 109-120.
3. *Yaremenko A.V., Osokin A.N.* Realizatsiya turbokodeka na programmiruemoy logicheskoy integral'noy skheme [Implementation of turbocodes on programmable logic integrated circuit], *Vestnik nauki Sibiri. Ser. 6. Informatsionnye tekhnologii i sistemy upravleniya* [Journal of science of Siberia. Series 6. Information technology and systems management], 2011, No. 1 (1).
4. *Zyablov V.V., Rybin P.S.* Sravnenie metodov peredachi po parallel'nym kanalam [Comparison of methods of transmission over parallel channels], *Trudy 30-y konferentsii molodykh uchenykh i spetsialistov IPPI RAN im. A.A. Kharkevicha Rossiyskoy akademii nauk «Informatsionnye tekhnologii i sistemy» (ITiS'07)* [Proceedings of the 30th conference of young scientists and experts of the Institute. A.A. Kharkevich, Russian Academy of Sciences "Information technologies and systems (ITAS'07)]. Moscow: IPPI RAN, 2007, pp. 99-103.

5. *Chizhov I.V.* Ekvivalentnye podprostranstva koda Rida–Mallera i prostranstvo klyuchey kriptosistemy Mak–Elisa–Sidel'nikova [Equivalent subspace code, reed–Muller and the space key cryptosystem Mac–ELISA–Sidelnikova], *Tezisy dokladov VIII Sibirskoy nauchnoy shkoly-seminara s mezhdunarodnym uchastiem. Komp'yuternaya bezopasnost' i kriptografiya – SIBECRYPT'09, 2009* [Abstracts of the VIII Siberian scientific school-seminar with international participation. Computer security and cryptography – SIBECRYPT'09, 2009], pp. 36-38.
6. *Chizhov I.V.* Klyuchevoe prostranstvo kriptosistemy Mak–Ellisa–Sidel'nikova [The key space of the cryptosystem Mac–Ellis–Sidelnikova], *Diskretnaya matematika* [Diskretnaya Matematika], 2009, Vol. 21 (3), pp. 132-158.
7. Rukovodstvo po nastroyke, ustanovke i ekspluatatsii radiomodema granit R-43ATs. OOO» Radiokommunikatsionnye sistemy» [Setup guide, installation and operation of radio granite P-AC. LTD." radio communication system"].
8. *Bikkenich R.R., Khvorov S.D.* Pomekhoustoychivost' sistemy s psevdosluchaynymi signalami i kodom Rida-Mallera [Immunity system with pseudorandom signals and code reed-Muller], *Telekommunikatsii* [Telecommunications], 2011, No. 11, pp.42-48.
9. *Romashchenko A.E., Rumyantsev A.Yu., Shen' A.A.* Zametki po teorii kodirovaniya [Notes on coding theory]. Moscow: MTsNMO, 2011, 80 p.
10. *Solov'eva F.I.* Vvedenie v teoriyu kodirovaniya: Uchebnoe posobie [Introduction to coding theory: tutorial]. Novosibirsk: Novosibirskiy gos. universitet, 2006, 127 p.
11. *Richard D. van Nee* OFDM codes for peak-to-average power reduction and error correction, *IEEE Globecom, London, U.K., 1996,* pp. 740-744.
12. *Davis J.A., Jedwab J.* Peak-to-mean power control and error correction for OFDM transmission using Goley sequences and Reed–Muller codes, *Electron. Lett.,* 1997, Vol. 33, pp. 267-268.
13. *Sidel'nikov V.M.* Otkrytoe shifrovanie na osnove dvoichnykh kodov Rida–Mallera [Open encryption based on binary reed–Muller codes], *Diskretnaya matematika* [Diskretnaya Matematika], 1994. Vol. 6, Issue 3, pp. 3-20.
14. *Chizhov I.V.* Prostranstvo klyuchey kriptosistemy Mak–Elisa–Sidel'nikova: Avtoref. diss. kand. fiz.-mat. nauk [Space key cryptosystem Mac–ELISA–Sidelnikov: abstract. cand. phys. and math. sci. diss. Moscow, 2010.
15. *Canteaut A., Carlet C., Charpin P., Fontaine C.* On cryptographic properties of the cosets, *IEEE Trans. Inf. Theory,* 2001, Vol. 47, No. 4, pp. 1949-1513.
16. *Borodin M., Chizhov I.* Effektivnaya ataka na kriptosistemu Mak–Elisa, postroennuyu na osnove kodov Rida–Mallera [An effective attack on the cryptosystem Mac–ELISA, based on reed–Muller codes], *Diskretnaya matematika* [Diskretnaya Matematika], 2014, Vol. 1, No. 26, pp. 10-20.
17. *Morelos–Saragosa R.* Iskusstvo pomekhoustoychivogo kodirovaniya. Metody, algoritmy, primenenie [The art of error-correcting coding. Methods, algorithms, application]. Moscow: Tekhnosfera, 2005, 320 p.
18. *Helleseth T., Klove T., Levenshtein V. I.* Error-correction capability of binary linear codes, *IEEE Trans. Inf. Theory,* 2005, Vol. 51, No. 4, pp. 1408-1423.
19. *Kenji Yasunaga, Toru Fujiwara.* On Correctable Errors of Binary Linear Codes, *IEEE Transactions on information theory,* 2010, Vol. 56, No. 6, pp. 2537.
20. *Alexander J. Grant, Richard D. van Nee.* Efficient Maximum-Likelihood Decoding of Q-ary Modulated Reed–Muller Codes, *IEEE Communications letters,* 1998, Vol. 2, No. 5, pp. 134-138.
21. *Dumer I., Kabatiansky G., Tavernier C.* Fast list decoding of Reed–Muller codes up to their distances, *Proc. XI Int. Workshop Algebraic and Combinatorial Coding Theory, Pamporovo, Bulgaria. 2008,* pp. 82-85.
22. *Dumer I., Kabatiansky G., Tavernier C.* List decoding of Reed–Muller codes up to the Johnson bound with almost linear complexity, *Proc. 2006 IEEE Int. Symp. Information Theory, USA. 2006,* pp. 138-142.
23. *Kabatiansky G., Tavernier C.* List decoding of Reed–Muller codes of the first order, *Proc. IX Int. Workshop Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria. 2004,* pp. 230-235.
24. *Paterson K.G., Jones A.E.* Efficient decoding algorithms for generalized Reed–Muller codes, *Technical Report HPL-98-195. Hewlett–Packard Labs., Bristol, 1998*.
25. *Ashikhmin, Litsyn S.N.* Fast decoding algorithms for first order Reed–Muller and related codes, *Desifn, Codes and Cryptography,* 1996, Vol. 7, pp. 187-214.

26. *Kornienko V.T.* Ispol'zovanie virtual'nykh priborov LabVIEW v uchebnom protsesse dlya skremblirovaniya tsifrovogo potoka dannykh [Application of labview virtual devices in educational process for scrambling of digital data flow*], Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 11 (148), pp. 182-186.
27. *Kornienko V.T.* Otsenka koeffitsienta szhatiya kodera Khaffmana v virtual'nom laboratornom eksperimente LabVIEW [Evaluation of the compression ratio of the Huffman encoder in the virtual laboratory experiment LabVIEW], *Sbornik nauchnykh trudov po itogam mezhdunarodnoy nauchno-prakticheskoy konferentsii «Novye tekhnologii i problemy tekhnicheskikh nauk»* [Proceedings of the international scientific-practical conference "New technologies and problems of technical Sciences"]. Krasnoyarsk, 2014, pp. 107-110.
28. *Kornienko V.T.* Povyshenie effektivnosti peredachi dannykh v sistemakh s interfeysom Wiegand [Improving the efficiency of data transmission in systems with Wiegand interface], *Sbornik nauchnykh trudov po itogam Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Tekhnicheskie nauki v mire: ot teorii k praktike»* [Proceedings of the International scientific-practical conference "Technical Sciences in the world: from theory to practice"]. Rostov-on-Don, 2014, pp. 67-69.

Статью рекомендовал к опубликованию д.пед.н. И.А. Стеценко.

Корниенко Владимир Тимофеевич – Южный федеральный университет; e-mail: vtkornienko@sfedu.ru; г. Таганрог, ул. Дзержинского, 170, кв. 53; тел.:+79515271225; кафедра РТС ИРТСиУ; к.т.н.; доцент.

Kornienko Vladimir Timofeevich – Southern Federal University; e-mail: vtkornienko@sfedu.ru; 170, Dzerginsky street, fl. 53, Taganrog, Russia; phone: +79515271225; the department RTS IRTS&C; cand. of eng. sc.; associate professor.

УДК 621.396.624

К.Е. Румянцев, А.П. Плёнкин

БЕЗОПАСНОСТЬ РЕЖИМА СИНХРОНИЗАЦИИ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ*

Исследования посвящены двухпроходной системе квантового распределения ключа (СКРК) с фазовым кодированием состояний фотонов в режиме вхождения в связь. Сигналы синхронизации представляют собой периодическую последовательность оптических импульсов. Формирование фотонных импульсов и применение однофотонных фотодетекторов обеспечивает повышенную защищённость от несанкционированного доступа режима синхронизации. Считаются известными период следования и длительность фотонного импульса. Временной кадр, равный периоду следования оптических импульсов, разбивается на ряд временных окон. Каждое окно опрашивается несколько раз, определяя объём выборки. При каждом опросе временного окна фиксируется число принимаемых фотоэлектронов (ФЭ) и/или импульсов темнового тока (ИТТ). В процессе синхронизации окно, в котором зарегистрировано максимальное число ФЭ и/или ИТТ, принимается за сигнальное окно. При анализе алгоритма синхронизации считается, что момент появления фотонного импульса случаен. Учитывается, что фотонный импульс может одновременно принадлежать двум соседним окнам. Случайные процессы в шумовых и сигнальных временных окнах описываются законом Пуассона. Моделированием процесса синхронизации определены границы применимости аналитических выражений для расчёта вероятности обнаружения сигнального временного окна в режиме синхронизации СКРК для двух крайних случаев момента появления фотонного импульса: фотонный импульс полностью располагается внутри анализируемого временного окна или распределяется между двумя соседними окна-

* Работа выполнена в рамках государственного задания Министерства образования и науки РФ высшим учебным заведениям в части проведения научно-исследовательских работ. Тема № 213.01-11/2014-9.