МИНОБРНАУКИРОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
«__» _____ 2017г.

СКРЕМБЛИРОВАНИЕ

Методические указания по выполнению практических работ по дисциплине «информационная безопасность»

Курск2017

Практическая работа №3 «Скремблирование»

Краткие теоретические сведения

Скремблирование — это обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств, близких к свойствам случайной последовательности. Исходное сообщение можно восстановить, применив обратный алгоритм. Применительно к телекоммуникационным системам скремблирование повышает надежность синхронизации устройств, подключенных к линии связи, и уменьшает уровень помех, излучаемых на соседние линии многожильного кабеля. Есть и иная область применения скремблеров — защита передаваемой информации от несанкционированного доступа.

Для синхронной передачи двоичный сигнал должен удовлетворять двум основным требованиям:

1. частота смены символов (1, 0) должна обеспечивать надежное выделение тактовой частоты непосредственно из принимаемого сигнала;

2. спектральная плотность мощности передаваемого сигнала должна быть, по возможности, постоянной и сосредоточенной в заданной области частот с целью снижения взаимного влияния каналов.

Одним из способов обработки двоичных посылок, удовлетворяющим данным требованиям является скремблирование (scramble – перемешивание).

После скремблирования появление «1» и «0» в выходной последовательности примерно равновероятно. Скремблирование также может использоваться для определенной защиты передаваемой информации, а также для идентификации абонентов.

Скремблирование широко применяется во многих видах систем связи для улучшения статистических свойств сигнала. Обычно скремблирование осуществляется на последнем этапе цифровой обработки непосредственно перед модуляцией (Рис. 1).

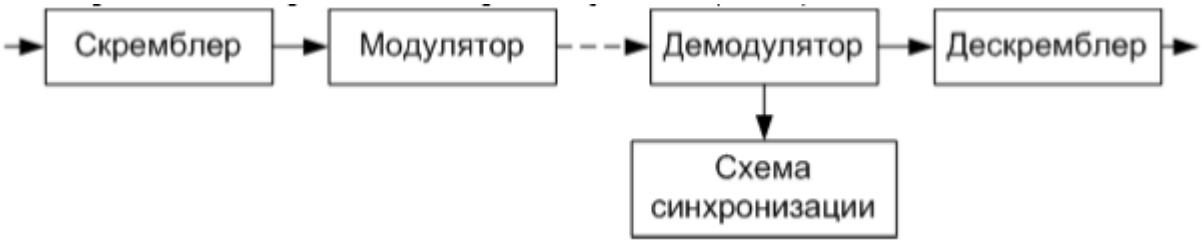


Рис. 1. Схема включения скремблера и дескремблера в канал связи

Скремблирование производится на передающей стороне с помощью устройства – скремблера, реализующего логическую операцию суммирования по модулю 2 исходного и преобразующего псевдослучайного двоичного сигнала. На приемной стороне осуществляется обратная операция – восстановление устройством, называемым дескремблером. Дескремблер выделяет из принятой последовательности исходную последовательность.

Основной частью скремблера является генератор псевдослучайной последовательности (ПСП) в виде линейного n-каскадного регистра с обратными связями, формирующий последовательность максимальной длины $2^n - 1$.

Различают два основных типа скремблеров и дескремблеров - самосинхронизирующиеся (СС) и с установкой (аддитивные). В литературе также можно встретить другие названия – скремблеры с неизолированным и изолированным от линии связи генераторами псевдослучайных последовательностей. Особенностью самосинхронизирующегося скремблера (СС скремблера) (Рис. 2) является то, что он управляется скремблированной последовательностью, т.е. той, которая передается в канал. Поэтому при данном виде скремблирования не требуется специальной установки состояний скремблера и дескремблера; скремблированная последовательность записывается в регистры сдвига скремблера и дескремблера, устанавливая их в идентичное состояние. При потере синхронизма между скремблером и дескремблером время восстановления синхронизма не превышает числа тактов, равного числу ячеек регистра скремблера.

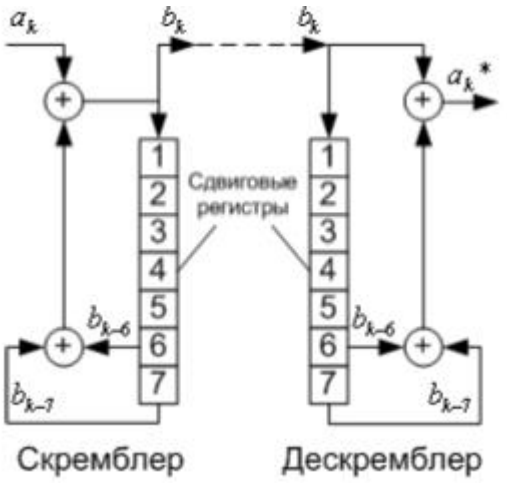


Рис. 2. Самосинхронизирующиеся скремблер и дескремблер.

На приемной стороне выделение исходной последовательности происходит путем сложения по модулю 2 принятой скремблированной последовательности с последовательностью на выходе сдвигового регистра. Например, для схемы Рис. 2 входная последовательность a_k с помощью скремблера в соответствии с соотношением $b_k = a_k xor\left(b_{k-6} xor b_{k-7}\right)$ преобразуется в посылаемую двоичную последовательность b_k. В приемнике из этой последовательности таким же регистром сдвига, как на приеме, формируется последовательность $a_k^* = b_k xor\left(b_{k-6} xor b_{k-7}\right)$. Эта последовательность на выходе дескремблера идентична первоначальной последовательности a_k.

Как следует из принципа действия схемы, при одной ошибке в последовательности b_k ошибочными получаются также последующие шестой и седьмой символы (в данном примере). В общем случае влияние ошибочно принятого бита будет сказываться α раз, где α - число обратных связей. Таким образом, СС скремблер-дескремблер обладает свойством размножения ошибок. Данный недостаток СС скремблера-дескремблера ограничивает число обратных связей в регистре сдвига; практически это число не превышает $\alpha = 2$

.

Второй недостаток СС скремблера связан с возможностью появления на его выходе при определенных условиях так называемых «критических ситуаций», когда выходная последовательность приобретает периодический характер с периодом, меньшим длины ПСП. Чтобы предотвратить это, в скремблере и дескремблере предусматриваются специальные дополнительные схемы контроля, которые выявляют наличие периодичности элементов на входе и нарушают ее.

Недостатки, присущие СС скремблеру-дескремблеру, практически отсутствуют при аддитивном скремблировании (Рис. 3), однако, этот тип скремблеров-дескремблеров требует предварительной идентичной установки состояний регистров скремблера и дескремблера. В скремблере с установкой (АД-скремблере), как и в СС скремблере, производится суммирование входного сигнала и ПСП, но результирующий сигнал не поступает на вход регистра. В дескремблере скремблированный сигнал также не проходит через регистр сдвига, поэтому размножения ошибок не происходит.

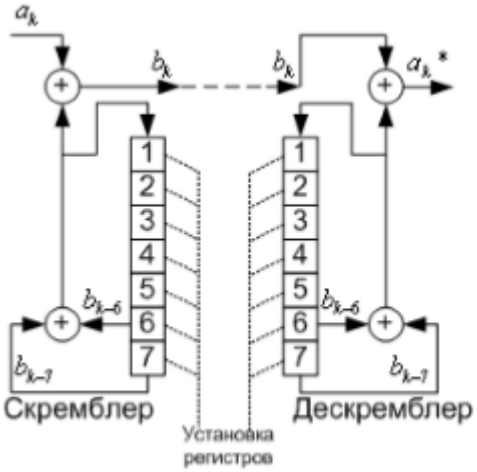


Рис. 3. Аддитивные скремблер и дескремблер.

Суммируемые в скремблере последовательности независимы, поэтому их период всегда равен наименьшему общему краткому величин периодов входной последовательности и ПСП и критическое состояние отсутствует. Отсутствие эффекта размножения ошибок и необходимости в специальной логике защиты от нежелательных ситуаций делают способ аддитивного скремблирования предпочтительнее, если не учитывать затрат на решение задачи фазирования скремблера и дескремблера. В качестве сигнала установки в ЦСП используют сигнал

цикловой синхронизации. Скремблирование так же влияет на энергетический спектр двоичного сигнала (Рис. 4).

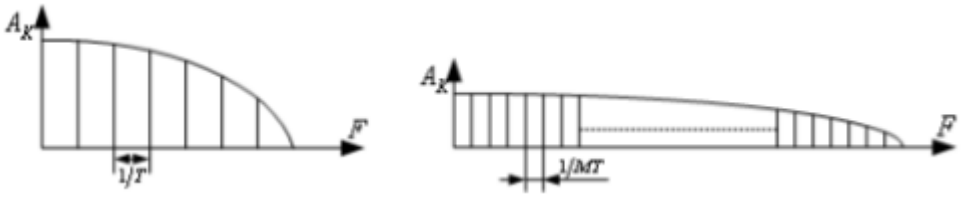
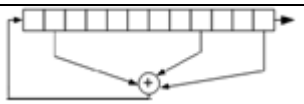
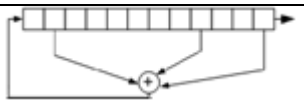
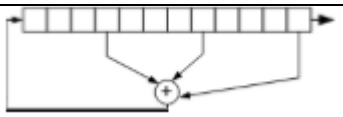
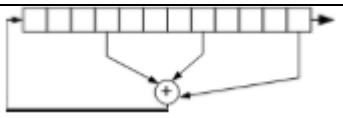
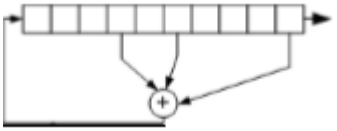
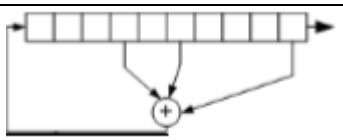
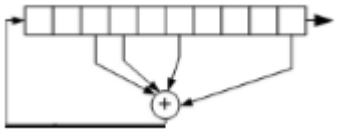
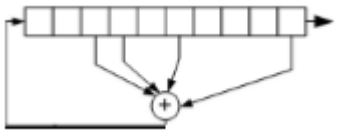
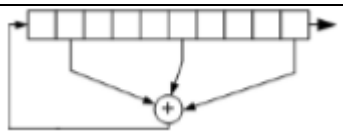
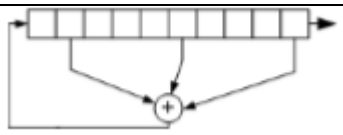
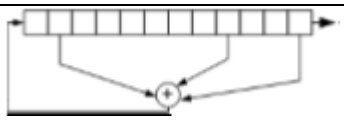
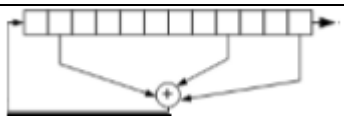
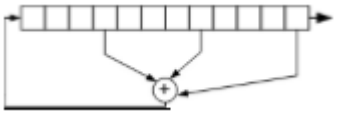
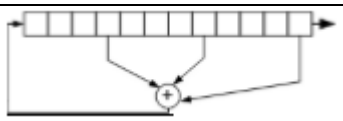
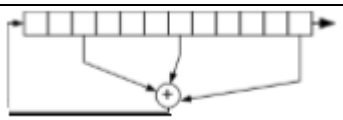
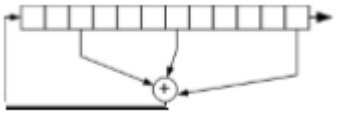
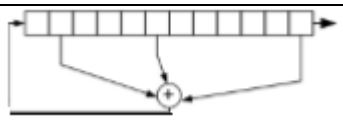


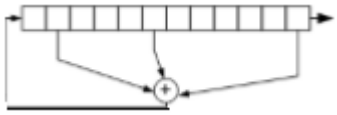
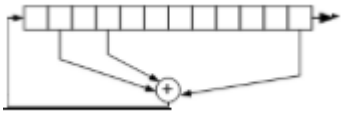
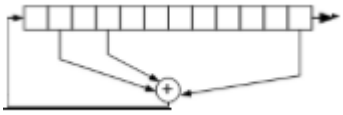
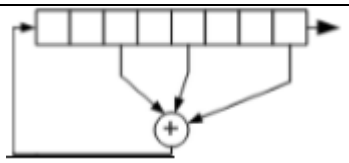
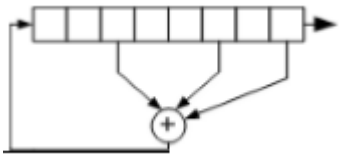
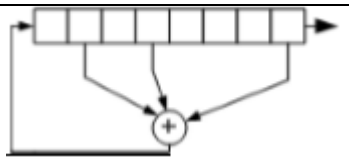
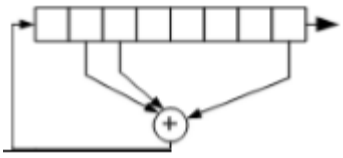
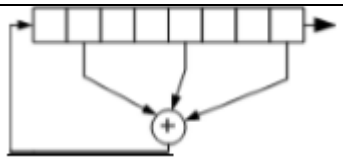
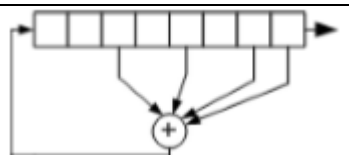
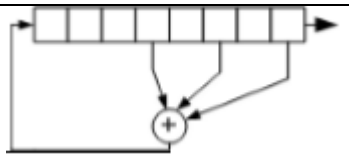
Рисунок 4 – Спектр сигнала а) до скремблирования; б) после скремблирования

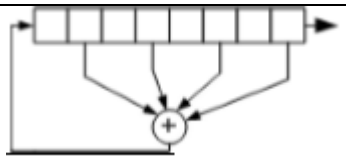
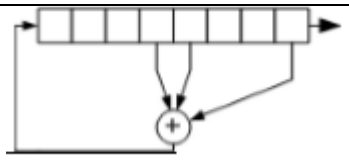
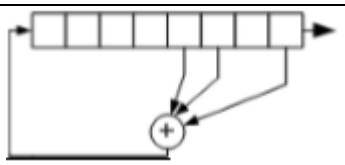
На рисунке 4, а. изображен пример энергетического спектра для периодического сигнала с периодом *T*, содержащим 6 двоичных элементов с длительностью T_0. После скремблирования ПСП с $M = 2^n - 1$ элементами спектр существенно «обогащается» (Рис. 4, б). При этом число составляющих спектра увеличилось в *M* раз, причём, уровень каждой составляющей уменьшается в такое же число раз.

Задание для выполнения

№	Тип скремблера/ дескремблера	Кол - во рег - ов	Сдвиговый регистр	Передаваемое сообщение
1	Самосинхронизирующийся	10		0010010110
2	Аддитивный	10		0010010110
3	Самосинхронизирующийся	10		0000100100
4	Аддитивный	10		0000100100
5	Самосинхронизирующийся	10		1111111111
6	Аддитивный	10		1111111111

№	Тип скремблера/ дескремблера	Кол - во рег - ов	Сдвиговый регистр	Передаваемое сообщение
7	Самосинхронизирующийся	10		1111011110
8	Аддитивный	10		1111011110
9	Самосинхронизирующийся	10		0000100100
10	Аддитивный	10		0000100100
11	Самосинхронизирующийся	12		1111111111
12	Аддитивный	12		1111111111
13	Самосинхронизирующийся	12		000101001101
14	Аддитивный	12		000101001101
15	Самосинхронизирующийся	12		110101001001
16	Аддитивный	12		110101001001
17	Самосинхронизирующийся	12		110001010001

№	Тип скремблера/ дескремблера	Кол - во рег - ов	Сдвиговый регистр	Передаваемое сообщение
18	Аддитивный	12		110001010001
19	Самосинхронизирующийся	12		001011010100
20	Аддитивный	12		001011010100
21	Самосинхронизирующийся	8		00110010
22	Аддитивный	8		00110010
23	Самосинхронизирующийся	8		00101010
24	Аддитивный	8		00101010
25	Самосинхронизирующийся	8		00100011
26	Аддитивный	8		00100011
27	Самосинхронизирующийся	8		10010110

№	Тип скремблера/ дескремблера	Кол - во рег - ов	Сдвиговый регистр	Передаваемое сообщение
28	Аддитивный	8		10010110
29	Самосинхронизирующийся	8		11100111
30	Аддитивный	8		11100111

Контрольные вопросы

1. Что такое скремблер и дескремблер?

2. Для каких целей используют скремблеры и дескремблеры?

3. Какие типы скремблеров и дескремблеров вам известны?

4. Какие преимущества и недостатки самосинхронизирующихся скремблеров и дескремблеров вам известны?

5. Какие преимущества и недостатки аддитивных скремблеров и дескремблеров вам известны?

Библиографический список

1. Панасенко, С. Алгоритмы шифрования [Текст] / С. Панасенко. Спб: БХВ-Петербург, 2009, 576 стр.

2. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография [Текст] / А.Г. Ростовцев, Е.Б. Маховенко. М: АНО НПО "Профессионал", 2005, 480 стр.

3. Рябко, Б. Я., Фионов, А. Н. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б. Я. Рябко, А. Н. Фионов. М: Научный мир, 2004, 179 стр.

4. Смарт, Н. Криптография [Текст] / Н. Смарт. М: Техносфера, 2006, 528 стр.