УДК 004.056.55:621.395.721.5

Студ. Н.С. Ильин, Р.А. Тышкевич
Науч. рук. доц. Н.Н. Буснюк
(Кафедра информационных систем и технологий, БГТУ)

МЕТОДЫ И АЛГОРИТМЫ ШИФРОВАНИЯ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ

В данной работе рассмотрим и сравним основные методы и алгоритмы шифрования в двух основных стандартах мобильной связи CDMA и GSM, сфокусировавшись на кодах Уолша и методе A5/1, рассмотрим их принципы работы и возможности применения в современных системах мобильной связи.

Метод шифрования кодами Уолша - это один из методов шифрования, используемых в сотовых сетях связи технологии CDMA. Одним из преимуществ метода шифрования кодами Уолша является возможность передачи большего количества данных через общий канал связи, что позволяет увеличить количество пользователей, которых можно обслуживать одновременно.

Коды Уолша - это наборы последовательностей из 1 и -1, которые используются для кодирования данных перед их передачей по радиосети. Для выполнения математических действий символ «-1» заменяется на значение «0» (рис. 1).

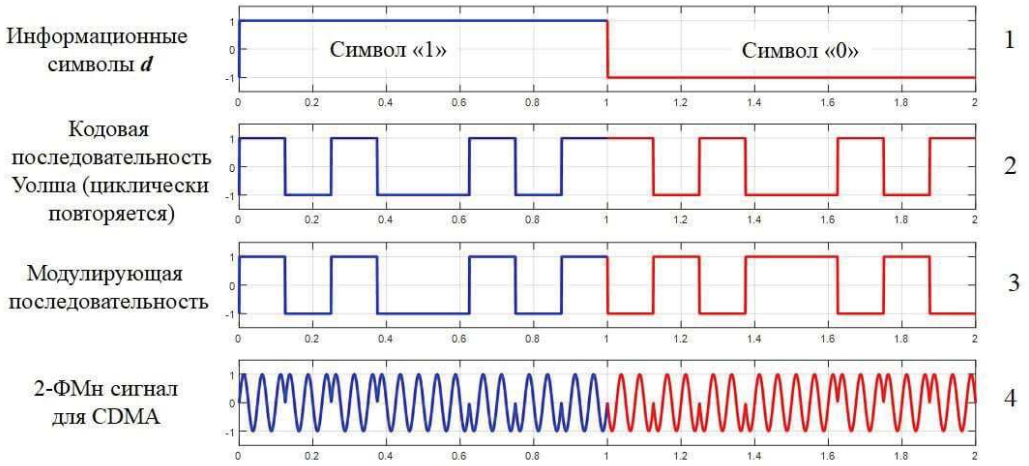

Рисунок 1 – Принцип работы шифрования при использовании кодов Уолша

На осциллограмме (1) присутствует информационный сигнал, т.е. полезная информация. Информационный сигнал (1) перемножаем с кодовой последовательностью Уолша (2). У последовательности Уолша есть длина, у нее 8 импульсов на последовательности. Вся длина последовательности должна уложиться в длину символа. Длительность последовательности равна длительности символа.

Когда начинает передаваться следующий символ, кодовая последовательность начинает опять циклически повторяться от символа к символу. Когда символы “1” и “0” перемножаем с кодовой последовательностью Уолша, получаем модулирующую последовательность (3).

Осциллограмму (3) подают на модулятор. Если символ “1”, то кодовая последовательность остается неизменной. Если символ “0”, то последовательность перевернулась.

Когда осциллограмму (3) подают на модулятор, формируется сигнал с двоичной фазовой модуляцией (2-ФМн), но фаза здесь меняется не каждый информационный символ, а будет определяться частотой следования импульсов кодовой последовательности.

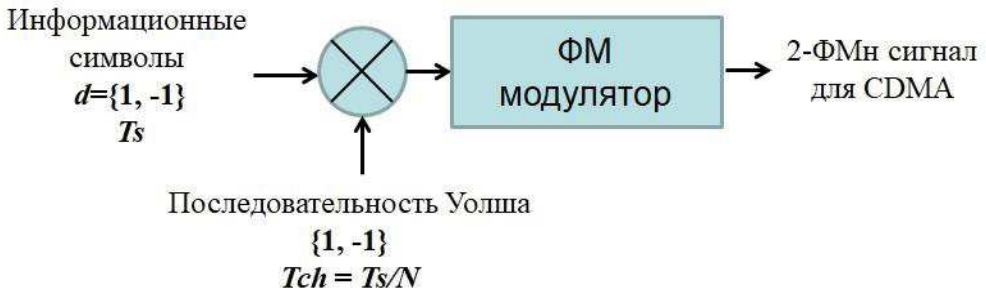

Рисунок 2 – Структура модулятора CDMA

На рисунке 2 есть последовательность Уолша, *Ts* – это длительность информационного символа, а *Tch* – длительность чипа. *N* – длина кодовой последовательности. Длительность чипа будет в 8 раз меньше длительности символа.

Когда сигналы доходят до приемника, используя уникальный код, применяемый на приемной стороне, можно извлечь сигнал только одного абонента, тогда как сигналы других абонентов остаются зашифрованными. Это позволяет достичь высокой емкости и надежности передачи данных.

В качестве алгоритма шифрования в GSM используются алгоритмы из семейства A5.

GSM – это стандарт сотовой связи, использующий методы множественного доступа FDMA и TDMA, применяется в основном на территории Европы.

Рассмотрим подробнее алгоритм A5/1.

Метод шифрования A5/1 - это алгоритм шифрования, который используется для защиты данных в сетях мобильной связи и является поточным.

Поточный шифр - это один из типов шифров, который шифрует данные путем генерации последовательности случайных битов. Фор-

мирование выходной последовательности происходит путём сложения потока исходного текста с генерируемой последовательностью (рис. 3).

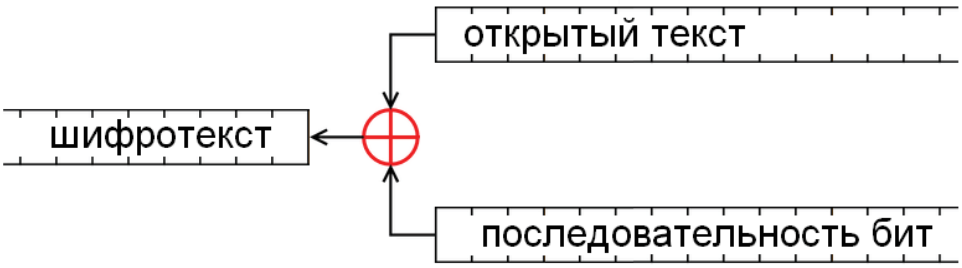

Рисунок 3 – Схема поточного шифра

A5/1 использует последовательность ключей, которая генерируется на основе трех регистров сдвига (рис. 4). Каждый регистр имеет различную длину и заполняется случайными битами из ключа, который задается при инициализации алгоритма. Ключ длиной 64 бита состоит из двух частей: 54 бита используются для генерации последовательности ключей, а оставшиеся 10 бит являются битами идентификатора абонента.

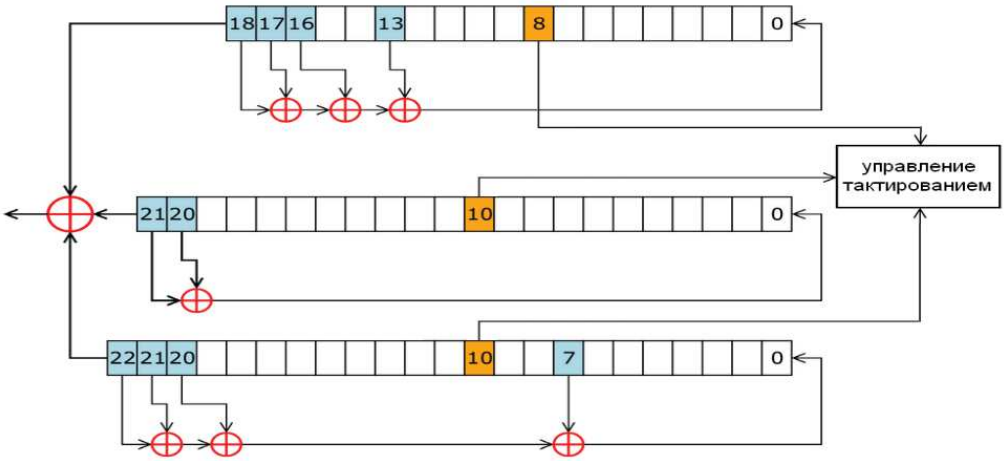

Рисунок 4 – Система регистров в алгоритме A5/1

Регистр сдвига с линейной обратной связью состоит из собственно регистра (последовательности бит заданной длины) и обратной связи (многочлен обратной связи $x^{32}+x^{29}+x^{25}+x^{5}+1$) (рис. 5). На каждом такте происходит следующие действия: крайний левый бит (старший бит) извлекается, последовательность сдвигается влево и в опустевшую правую ячейку (младший бит) записывается значение функции обратной связи. Эта функция является суммированием по модулю два определённых битов регистра и записывается в виде многочлена, где степень указывает номер бита. Извлечённые биты формируют выходную последовательность.

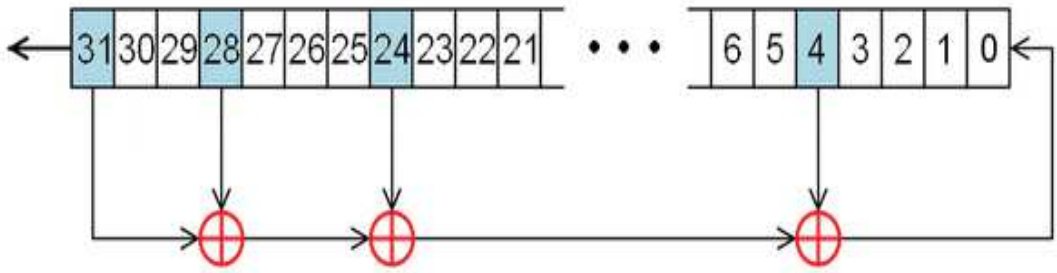

Рисунок 5 - Регистр сдвига с линейной обратной связью

Вывод. Надежность поточного алгоритма шифрования определяется только длиной и секретностью ключа, поэтому алгоритм шифрования в стандарте GSM кажется проще. Однако применяемые методы сверточного кодирования для генерации ключей повышают их секретность.

Алгоритм шифрования по технологии CDMA более многошаговый, применяет целое семейство функций Уолша и несколько рандомных последовательностей. Он сложнее в реализации, но оба подхода нашли свое применение в последующих поколениях систем мобильной связи: 3G и 4G.

В целом, для обеспечения безопасности передачи данных в мобильных сетях необходимо использовать комплексный подход, комбинируя различные методы и алгоритмы шифрования, и периодически менять используемые ключи и последовательности, чтобы обеспечить максимальную безопасность передаваемой информации.

ЛИТЕРАТУРА

1. А.И. Курочкин, О.С. Шалыто. Методы и алгоритмы шифрования в системах мобильной связи. – Москва: Издательство МГТУ им. Н.Э. Баумана, 2014. – 184 с.

2. И.А. Кузнецов, Е.А. Плаксина, А.В. Романов. Алгоритмы шифрования в сетях мобильной связи – Москва: Издательство "ИНФРА-М", 2012. – 192 с.

3. А.А. Гришин, С.В. Михайлов. Шифрование в мобильных сетях – Санкт-Петербург: Издательство Политехнического университета, 2015. – 168 с.

4. Д.В. Ковалев, А.С. Мещеряков. Безопасность мобильных сетей GSM и UMTS: алгоритмы шифрования.– Москва: Издательство "Экзамен", 2013. – 144 с.