УДК 557.114:616-006

Студ. Н.С. Ильин, студ. Тышкевич Р.А.

Науч. рук. доц. Н.Н. Буснюк (кафедра информационных систем и технологий, БГТУ)

**МЕТОДЫ И АЛГОРИТМЫ ШИФРОВАНИЯ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ**

Передача информации в мобильных сетях является основным методом коммуникации в нашем современном мире. Но этот процесс также сопровождается рисками для безопасности данных. Поэтому методы и алгоритмы шифрования стали одними из важнейших средств защиты информации в мобильных сетях.

Цель нашей работы: провести анализ методов и алгоритмов шифрования в системах мобильной связи, сфокусировавшись на CDMA, кодах Уолша и методе A5/1, рассмотреть их принципы работы и возможности применения в современных системах мобильной связи.

Если есть радиотехническая система, включающая в себя множество устройств и между этими устройствами необходимо выполнять обмен информацией, необходимо разделять каналы.

Есть базовая станция и множество абонентских устройств. Между БС и мобильными телефонами образуется канал. Задача — организовать разделение каналов таким образом, чтобы работа одного устройства не создавала помех для другого устройства.

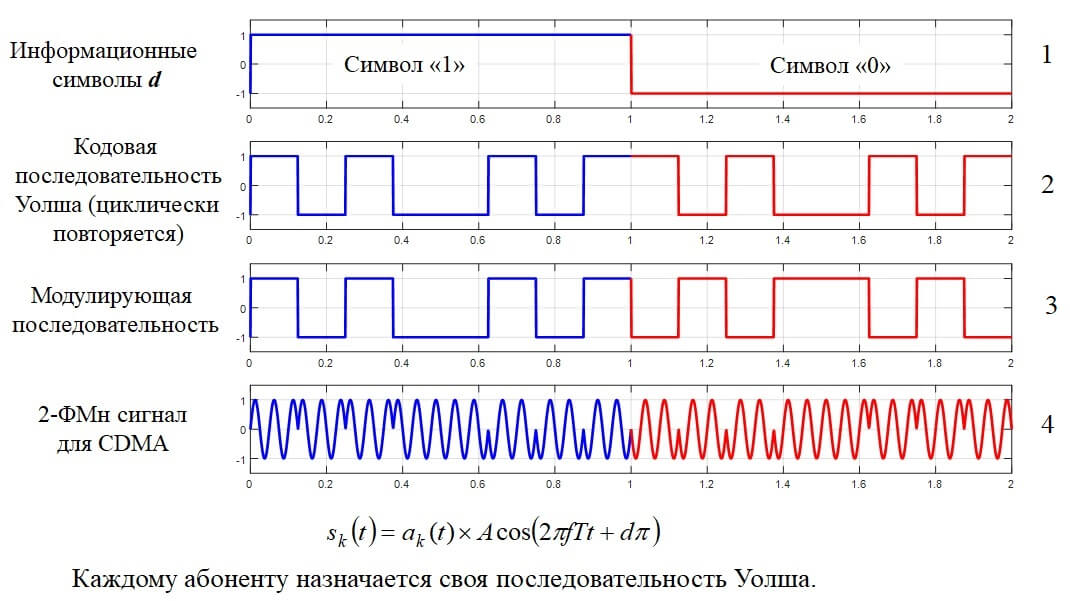
CDMA (Code Division Multiple Access) - это метод множественного доступа, используемый в сотовых и беспроводных сетях связи, который позволяет нескольким пользователям использовать одну и ту же частоту одновременно, используя разные коды для кодирования своих данных.

Каждый пользователь в сети CDMA имеет свой собственный уникальный код, который используется для передачи его данных через сеть.

Метод шифрования кодами Уолша - это один из методов шифрования, используемых в сотовых сетях связи, который позволяет передавать данные через общий канал, используя уникальные коды Уолша для каждого пользователя.

Коды Уолша - это наборы последовательностей из 1 и -1, которые используются для кодирования данных перед их передачей по сети.

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.



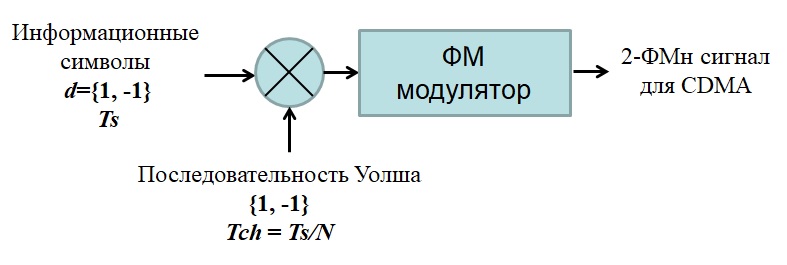
**Рисунок 1 – Принцип работы шифрования при использовании кодов Уолша**

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 = длительности символа.

Когда начинает передаваться следующий символ, кодовая последовательность начинает опять циклически повторяться от символа к символу. Когда символы “1” и “2” перемножаем с кодовой последовательностью Уолша получаем модулирующую последовательность (3).

Осциллограмму (3) и будем подавать на модулятор. Если символ “1”, тогда кодовая последовательность какая была, такая и осталась. Если символ “0”, тогда последовательность перевернулась.

Когда осциллограмму (3) подаем 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 будем 8 раз меньше длительности символа.

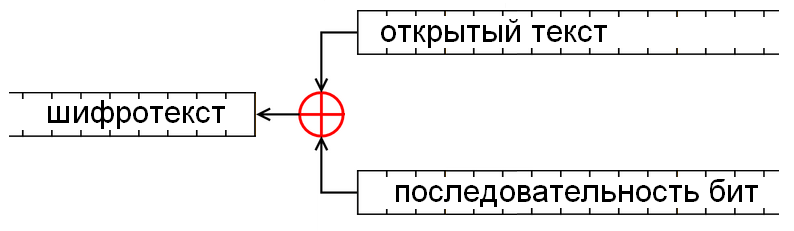
Когда сигналы доходят до приемника, используя уникальный код, применяемый на приемной стороне, можно извлечь сигнал только одного абонента, тогда как сигналы других абонентов остаются зашифрованными. Это позволяет достичь высокой емкости и надежности передачи данных.

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

GSM - это стандарт цифровой сотовой связи, который используется для передачи данных в мобильных сетях. Он поддерживает передачу голоса и данных, а также обеспечивает безопасность передачи данных при помощи шифрования.

Рассмотрим подробнее алгоритм A5/1.

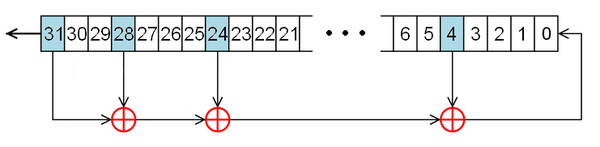
Метод шифрования A5/1 - это алгоритм шифрования, который используется для защиты данных в сетях мобильной связи и является поточным.



**Рисунок 3 – Схема поточного шифра**

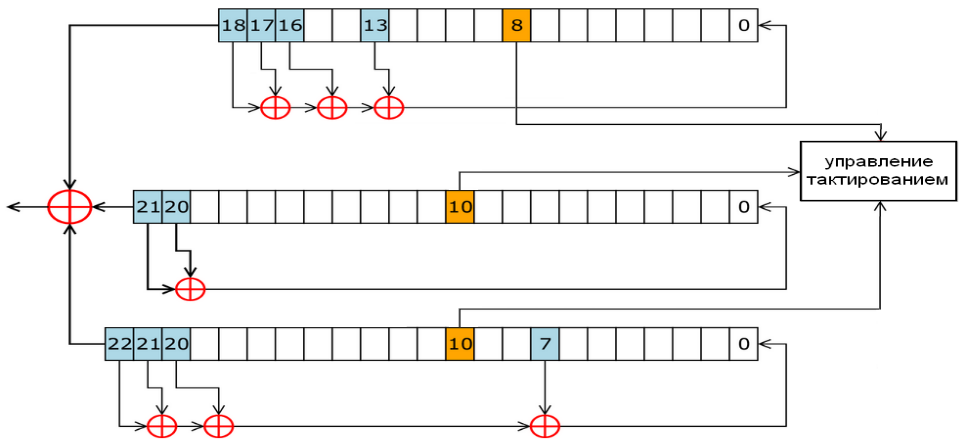
Поточный шифр - это один из типов шифров, который шифрует данные путем генерации последовательности случайных битов.

Формирование выходной последовательности происходит путём сложения потока исходного текста с генерируемой последовательностью.



**Рисунок 4 - Регистр сдвига с линейной обратной связью**

Регистр сдвига с линейной обратной связью состоит из собственно регистра (последовательности бит заданной длины) и обратной связи (многочлен обратной связи x32+x29+x25+x5+1). 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 – Система регистров в алгоритме А5/1**

А5/1 использует последовательность ключей, которая генерируется на основе трех регистров сдвига. 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.

ЛИТЕРАТУРА

1. "Методы и алгоритмы шифрования в системах мобильной связи" / А.И. Курочкин, О.С. Шалыто. – Москва: Издательство МГТУ им. Н.Э. Баумана, 2014. – 184 с.
2. "Алгоритмы шифрования в сетях мобильной связи" / И.А. Кузнецов, Е.А. Плаксина, А.В. Романов. – Москва: Издательство "ИНФРА-М", 2012. – 192 с.
3. "Шифрование в мобильных сетях" / А.А. Гришин, С.В. Михайлов. – Санкт-Петербург: Издательство Политехнического университета, 2015. – 168 с.
4. "Безопасность мобильных сетей GSM и UMTS: алгоритмы шифрования" / Д.В. Ковалев, А.С. Мещеряков. – Москва: Издательство "Экзамен", 2013. – 144 с.