УДК 004.056.55:621.395.721.5

Студ. Н.С. Ильин, студ. Тышкевич Р.А.

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

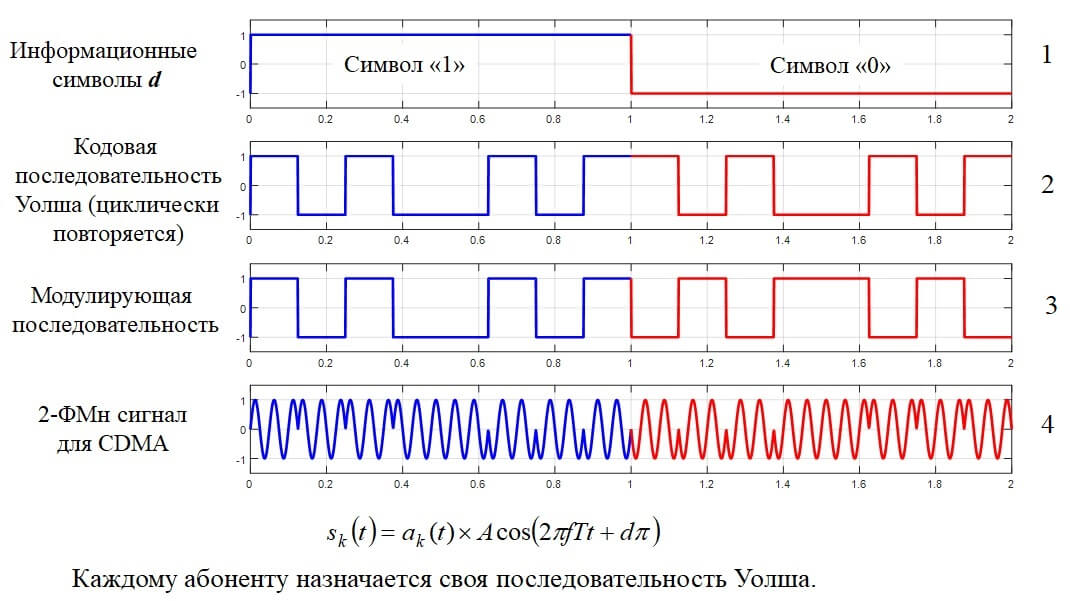
**МЕТОДЫ И АЛГОРИТМЫ ШИФРОВАНИЯ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ**

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, позволяющий передавать данные через общий канал.

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

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.



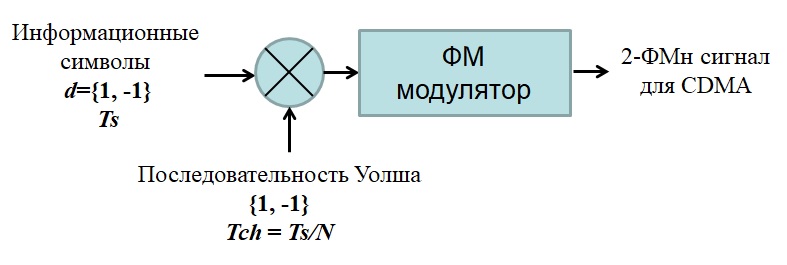
**Рисунок 1 – Принцип работы шифрования при использовании кодов Уолша**

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 равна 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”, то кодовая последовательность остается неизменной. Если символ “0”, то 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 будет в 8 раз меньше длительности символа.

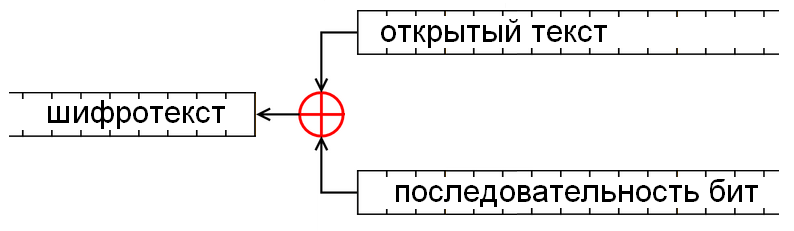
Когда сигналы доходят до приемника, используя уникальный код, применяемый на приемной стороне, можно извлечь сигнал только одного абонента, тогда как сигналы других абонентов остаются зашифрованными. Это позволяет достичь высокой емкости и надежности передачи данных.

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

GSM – это стандарт цифровой сотовой связи, который используется для передачи голоса и данных в мобильных сетях, применяется в основном на территории Европы.

Рассмотрим подробнее алгоритм A5/1.

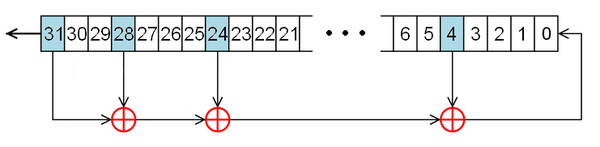
Метод шифрования A5/1 — это алгоритм шифрования, который используется для защиты данных в сетях мобильной связи и является поточным.



**Рисунок 3 – Схема поточного шифра**

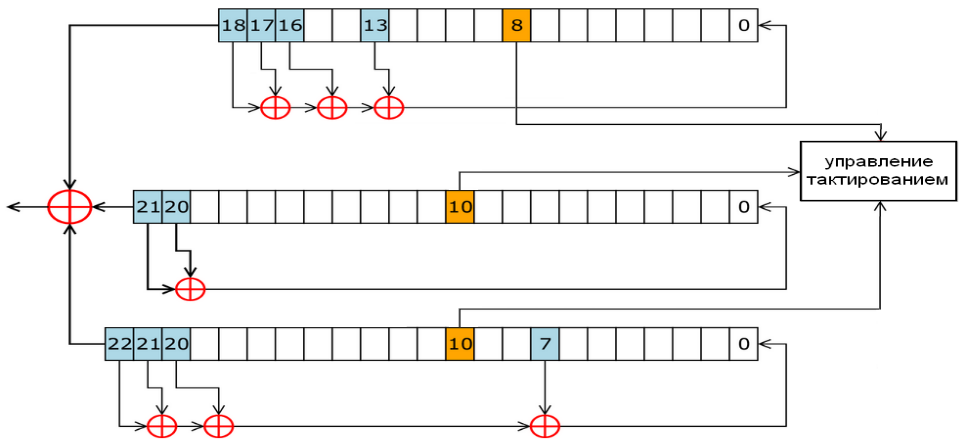
Поточный шифр — это один из типов шифров, который шифрует данные путем генерации последовательности случайных битов.

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



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

В отличие от этого, LFSR использует регистр сдвига для генерации последовательности битов, которые также комбинируются с исходным текстом для шифрования. LFSR — это один из самых распространенных методов генерации псевдослучайных чисел. Он использует регистр для хранения текущего состояния и генерирует новый бит путем сложения нескольких предыдущих битов в регистре, которые выбираются с помощью многочлена обратной связи. На каждом такте происходят 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.

В заключении можно отметить, что изучение методов и алгоритмов шифрования в стандартах мобильной связи CDMA и GSM позволило увидеть различия в принципах их работы. Метод A5/1, используемый в GSM, показал уязвимость к криптоанализу из-за короткой длины ключа в 64 бита и возможности его перебора в приемлемые сроки. Коды Уолша, используемые в CDMA, имеют более длинные последовательности и, следовательно, более криптостойкие ключи. Каждый из рассмотренных методов шифрования имеет свои преимущества и недостатки, и выбор конкретного метода зависит от конкретных требований к безопасности, скорости и эффективности передачи данных в конкретной ситуации. Например, метод A5/1 имеет низкую криптостойкость, и его безопасность может быть подвержена атакам. С другой стороны, коды Уолша обладают высокой стойкостью к атакам, но их использование может привести к значительным задержкам в передаче данных из-за большой длины последовательностей. 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. "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.