# ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ СВЯЗИ В ТЕЛЕФОННОЙ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Макаренко М.П., группа ТКС-01н
Руководитель доц. каф. АТ Суков С.Ф.

В настоящее время проблема конфиденциальности телефонных переговоров приобретает особое значение в связи с необходимостью защиты бизнес-интересов и личной свободы граждан. Современные методы обеспечения конфиденциальности связи для телефонных сетей общего пользования реализуется на основе различных криптографических алгоритмов. Наиболее криптостойкими алгоритмами являются DES, IDEA, ГОСТ 28147-89 и ряд других, которых не так уж и много. Некоторые из этих алгоритмов как, например, ГОСТ 28147-89 и DES закреплены стандартами своих стран — Россией и США соответственно.

Однако, обратной стороной вопроса обеспечения проблемы криптостойкости является существенная сложность и трудность программно-аппаратной реализации этих алгоритмов. В этой связи представляется актуальным разработать такую модификацию алгоритма криптографического шифрования, которая позволила бы сохранить криптостойкость.

В качестве такой модификации был разработан алгоритм криптографического шифрования на основе сети Файстеля. Сеть Файстеля позволяет использовать алгоритм как для шифрования так и для дешифрования (рис. 1).

На вход алгоритма криптографического шифрования поступает 64 бита данных. Затем 64-битный блок разбивается на младшие ($L_i$) и старшие ($H_i$) 32 бита. Эта процедура необходима для обратимости алгоритма. Под свойством обратимости, здесь, понимается то, что для процедуры шифрования и дешифрования потребуется один и тот же алгоритм.

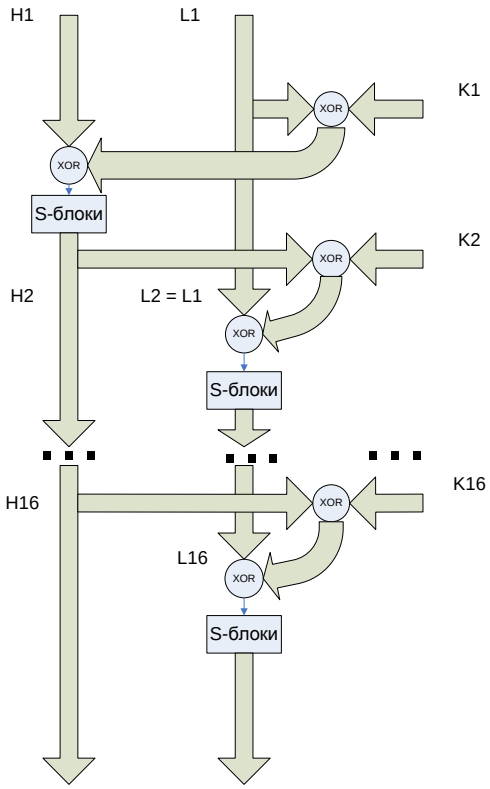


Рисунок 1 — Блок-схема алгоритма криптографического шифрования

Алгоритм состоит из шестнадцати этапов шифрования. В каждом из этих этапов шифруется то младшая то старшая часть — на нечётных этапах шифруется старшая часть, на чётных — младшая часть.

Немаловажную роль в процедурах шифрования и дешифрования играет функция шифрования, которая здесь представлена S-блоками. В таких алгоритмах как DES, ГОСТ 28147-89, IDEA и других, эта функция представлена множеством преобразований: перестановкой с расширением, перестановкой со сжатием, процедурой перестановки, процедурой замены и.т.д. Единственной процедурой, которая в наибольшей степени влияет на криптостойкость алгоритма, является подстановка в S-блоке. Она обладает очень важным криптографическим свойством — лавинным эффектом. Его суть основывается на том, чтобы как можно большее количество выходных данных зависели от как можно меньшего количества входных данных, что влияет на криптостойкость алгоритма. Процедура построения S-блоков требует

проявления лавинного эффекта в таком виде, чтобы при изменении хотя бы одного из битов входных данных, изменялась ровно половина всех бит на выходе.

В данном алгоритме, входящие 32 бита разбиваются на 8 блоков по 4 бита в каждом. И благодаря этому получается 8 S-блоков размерностью 4x4 (рис. 2).

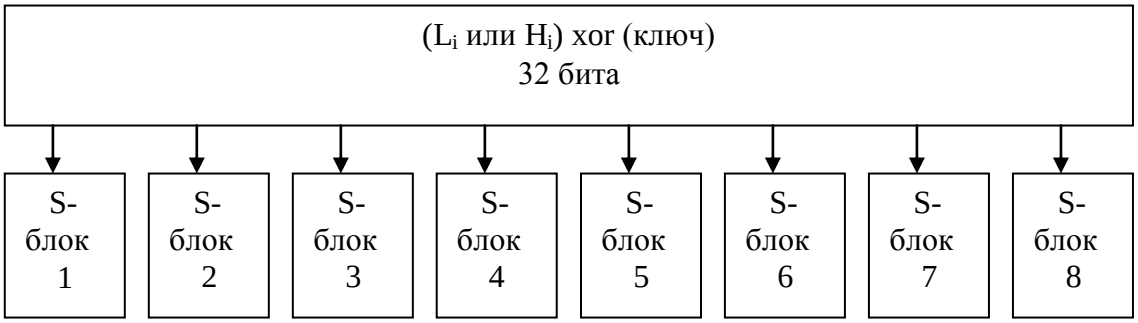


Рисунок 2 — Принцип работы S-блоков в алгоритме

S-блок представляет из себя таблицу (Табл. 1). Для примера был взят первый S-блок. Все остальные семь S-блоков обладают точно таким же криптографическим свойством как лавинный эффект.

Таблица 1 — структура S-блока

| | | | |
|---|---|---|---|
| 10 | 15 | 5 | 0 |
| 12 | 3 | 6 | 9 |
| 0 | 5 | 9 | 12 |
| 3 | 6 | 10 | 15 |

Номера строк — это биты 0 и 3, а номера столбцов — биты 1 и 2 четырёхбитного блока.

Генерирование и обмен ключей реализуется в форме алгоритма Диффи-Халлмана. Первый этап генерирования заключается в том, что каждый из абонентов выбирает большие простые числа n и g. По ним каждый из

абонентов вычисляет один и тот же ключ шифрования. Несмотря на то, что числа, с помощью которых вычисляется ключ, передаются по каналу связи, они не могут служить аргументом для вычисления ключа подслушивающей стороной. Для того, чтобы определить ключ, нужно вычислить дискретный логарифм. Способы его вычисления рассматриваются в теории конечного поля Галуа.

На основе вышеуказанных алгоритмов будет реализовано программно-аппаратное решение этой проблемы. В качестве процессора цифровой обработки сигналов был выбран процессор TMS320C54CST фирмы Texas Instrument. Общая блок-схема программно-аппаратного решения представлена на рис. 3.

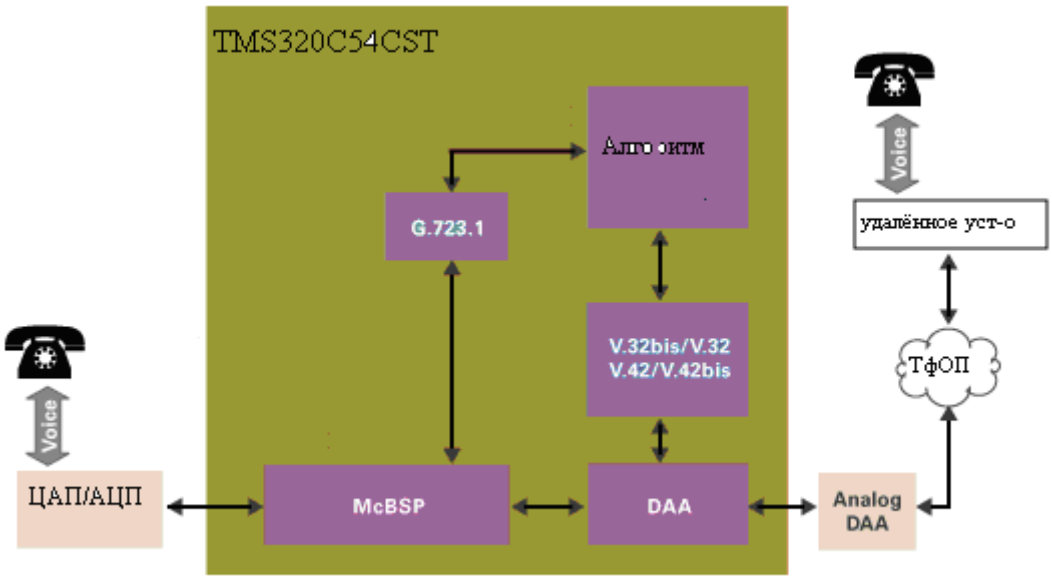


Рисунок 3 — структура программно-аппаратной реализации

Перечень ссылок

1. Брюс Шнайер. Прикладная криптография. — Триумф, 2002. — 374 с.

2. Архитектура блочных шифров/ Электронный ресурс. Способ доступа: URL: http://www.enlight.ru/crypto/articles/ib/ib04.htm.

3. Secure Phone/ Электронный ресурс. Способ доступа: URL: http://focus.ti.com/docs/solution/folders/print/332.html.