Розглядаються питання модернізації генераторів гамми алгоритму шифрування А5/1 стандарту GSM. Запропоновані варіанти по поліпшенню властивостей гамми, що генерується, за рахунок збільшення ступенів поліномів, що породжують. Проведений порівняльний аналіз якості тієї, що генерується ПВП оцінними і графічними тестами при використанні алгоритму А5 і його модифікацій

Ключові слова: алгоритм шифрування А5, ПВП, мовна інформація, гамування, криптографічна стійкість, регістри LFSR, генератори гамми

Рассматриваются вопросы модернизации генераторов гаммы алгоритма шифрования А5/1 стандарта GSM. Предложены варианты по улучшению свойств генерируемой гаммы, за счет увеличения степеней порождающих полиномов. Проведен сравнительный анализ качества генерируемой ПСП оценочными и графическими тестами при использовании алгоритма А5 и его модификаций

Ключевые слова: алгоритм шифрования А5, ПСП, речевая информация, гаммирование, криптографическая стойкость, регистры LFSR, генераторы гаммы

The modernization of generators of scale of existing algorithm of enciphering A5 of the standard GSM was offered. The received variants of modernization of algorithm A5 are investigated under some tests of research pseudo-casual sequences (PCS). The carried out comparative analysis with the help of the tests for research PCS of the offered modernizations of algorithm A5 has shown, that at increase of the periods LFSR the resulting period of scale is increased them least general multiple and, hence. It results in increase cryptographic stability of algorithm A5

Keywords: algorithm of enciphering A5, tests of research PCS, speech information, gammiration, cryptographic stability, registers LFSR, generators of a gamma

УДК 621.397

ЗАЩИТА РЕЧЕВЫХ СИГНАЛОВ В СИСТЕМАХ МОБИЛЬНОЙ СВЯЗИ С ПОМОЩЬЮ ГАММИРОВАНИЯ

В.С. Волотка
Ассистент*
Контактный тел.: 8 (057) 702-14-29
E-mail: vadim_pirogov@ukr.net

А.А. Астраханцев
Кандидат технических наук, доцент*
Контактный тел.: 8 (057) 702-14-29
E-mail: astrahkture@mail.ru
*Кафедра "Сети связи"
Харьковский Национальный университет радиоэлектроники
пр. Ленина 14, г. Харьков, 61166

Е.М. Семашко

1. Введение

В современных системах защиты речевой информации наиболее широко используется метод гаммирования речевых сигналов. При этом генераторы гаммы чаще всего строятся на основе регистров смещения с линейными обратными связями – LSFR. Достоинством алгоритмов, реализующих этот метод, является простота вычисления, а недостатком – низкая криптографическая стойкость по сравнению с другими более сложными криптографическими алгоритмами.

Наиболее известными среди алгоритмов, реализующих этот метод, является алгоритм А5 стандарта GSM.

Криптографическая слабость А5 обусловлена недостаточно проработанным выбором разрядов LSFR, создающих обратную связь, и управляющих механизмов тактирования регистров. Поэтому актуальна задача создания новых алгоритмов защиты речи в системах мобильной связи с более высокой криптографической стойкостью или путём модернизации существующего алгоритма А5.

2. Формулирование проблемы

Криптографическая слабость алгоритма А5 основывается на плохом выборе разрядов LFSR, образующих обратные связи и управляющих механизмом тактирования регистров, который призван обеспечить нелинейность работы алгоритма. Кроме этого, его регистры слишком коротки, чтобы предотвратить поиск ключа перебором.

Целью работы является повышение криптографической стойкости алгоритма шифрования А5 стандарта GSM.

Для достижения поставленной цели реализована схема алгоритма А5 в оболочке Matlab и создан банк ЛРР для исследования криптостойкости алгоритма и характеристик генерируемой гаммы.

3. Структура алгоритма А5

А5 – поточный шифр, используемый в системах GSM (Group Special Mobile) для закрытия связи между абонентом и базовой станцией. Он является европейским стандартом для цифровых сотовых мобильных телефонов [1].

А5 использует три LFSR длиной 19, 22 и 23 с прореженными многочленами обратной связи, т. е. с многочленами, имеющими небольшое число ненулевых коэффициентов. Выходом генератора гаммы является выход элемента сложения по модулю два – М2, на входы которого поступают последовательности с выходов трех LFSR, начальное заполнение которых определяется секретным ключом. Используется управление синхронизацией LFSR (рис. 1).

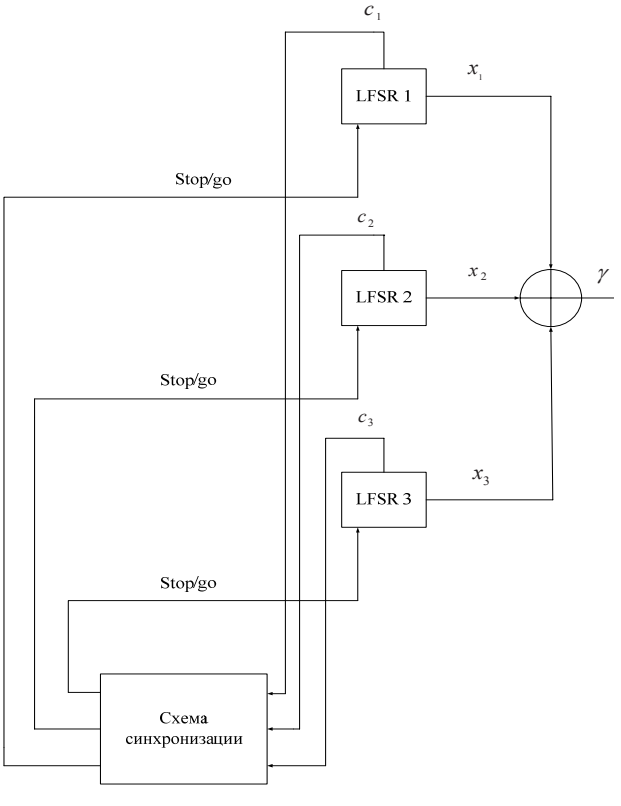

Рис. 1. Генератор гаммы алгоритма А5

Для управления синхронизацией используются биты С1, С2 и С3 с выходов LFSR. В каждом такте сдвигаются как минимум два LFSR. Если С1 = С2 = С3, сдвигаются все три регистра, в противном случае сдвигаются те два регистра i и j, для которых выполняется равенство $c_i = c_j$.

Существует две версии алгоритма А5: А5/1 и намеренно ослабленный вариант алгоритма А5 – алгоритм А5/2. Остановимся более подробно на версии А5/1.

Каждый кадр шифруется с помощью секретного ключа шифрования Кс и сквозного порядкового номера очередного кадра. Генератор ПСП А5/1 состоит из трех коротких LFSR (рис. 2), обозначаемых как LFSR-l, LFSR-2 и LFSR-3.

Образующие многочлены этих регистров имеют вид: LFSR1: $x^{19} + x^{l8} + x^{17} + x^{14} + 1$, LFSR2: $x^{22} + x^{21} + 1$, LFSR3: $x^{23} + x^{22} + x^{21} + x^8 + 1$.

Выходные биты снимаются с самых старших разрядов регистров, после чего с помощью операции XOR над битами с выходов всех трех бит гаммы шифра. Регистры работают по принципу stop-and-go, что обеспечивается с помощью применения специальной функции majority, на вход которой подаются значения битов регистров: бит С1 (восьмой разряд) для LFSR-1, бит С2 (десятый разряд) для LFSR-2 и С3 (десятый разряд) для LFSR3.

Функция majority имеет следующий вид:

$$majority(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3.$$

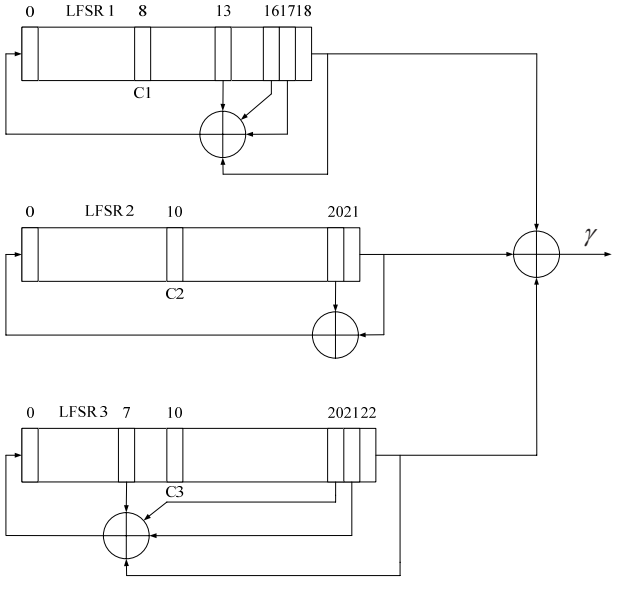

Рис. 2. Схема работы регистров алгоритма А5/1

На каждом шаге работы шифра два или три регистра сдвигаются. Таким образом, каждый регистр сдвигается в одном такте работы алгоритма с вероятностью ¾ и не сдвигается с вероятностью ¼.

4. Модернизация алгоритма А5

Период гаммы равен наименьшему общему кратному всех трёх периодов LFSR алгоритма А5. С увеличением длины периода повышается криптостойкость данного алгоритма.

В связи с этим было предложено модернизировать существующий генератор гаммы алгоритма А5 двумя способами. В первом случае был заменён в LFSR-2 полином $x^{22} + x^{21} + 1$ на примитивный полином более высокой степени $x^{24} + x^4 + x^3 + x + 1$. Во втором случае – заменены все три полинома LFSR примитивными полиномами более высоких степеней.

Для проведения сравнительного анализа предлагаемого метода и используемого, остановимся на используемых критериях оценивания.

5. Критерии оценивания

Для исследования ПСП применяются две группы тестов [2].

– Графические тесты. Пользователь получает определенные графические зависимости и по их виду делает вывод о свойствах тестируемой последовательности.

а) Гистограмма.

б) Распределение на плоскости.

в) Байтовая АКФ.

г) Битовая АКФ.

д) Проверка на монотонность.

е) Проверка 0 и 1.

ж) Проверка серий.

– Оценочные тесты. На основе оценочных критериев делается заключение о степени близости статистических свойств анализируемой и истинно случайной последовательности.

а) Критерий χ^2.

б) Проверка частот.

в) Анализ перестановок.

г) Проверка сегментов.

д) Последовательная корреляция.

В данной работе для исследования ПСП будут использоваться следующие тесты:

1) Проверка 0 и 1. Тест проверяет равномерность распределения символов в изучаемой последовательности. Для этого подсчитывается число 0 и 1. В качественной ПСП разброс между количеством 0 и 1 близок к нулю.

2) Проверка серий. Тест проверяет равномерность распределения символов в изучаемой последовательности, анализируя частоту встречаемости биграмм (00, 01, 10, 11) и триграмм (000, 001, 010, 011, 100, 101, 110, 111). В качественной ПСП разброс между частотами встречаемости биграмм (триграмм) должен стремиться к нулю.

А также было найдено наименьшее общее кратное (НОК) периодов LFSR для этих трёх вариантов алгоритма А5.

6. Результаты исследований

Рассматривается 3 варианта алгоритма А5.

Первый – существующий.

Второй – с заменой LFSR2 (вариант А) - LFSR1: $x^{19} + x^{18} + x^{17} + x^{14} + 1$, LFSR2: $x^{24} + x^4 + x^3 + x + 1$, LFSR3: $x^{23} + x^{22} + x^{21} + x^8 + 1$.

Третий – полностью модернизированный алгоритм А5 (вариант В) - LFSR1: $x^{24} + x^4 + x^3 + x + 1$, LFSR2: $x^{26} + x^6 + x^2 + x + 1$, LFSR3: $x^{27} + x^5 + x^2 + x + 1$.

На рис. 3 представлены результаты тестирования проверки равномерности распределения 0 и 1 в ПСП для исследуемых генераторов гаммы.

На рис. 3-5 «1» соответствует алгоритму А5, 2 – модификация полинома LFSR2, 3 – замена всех полиномов.

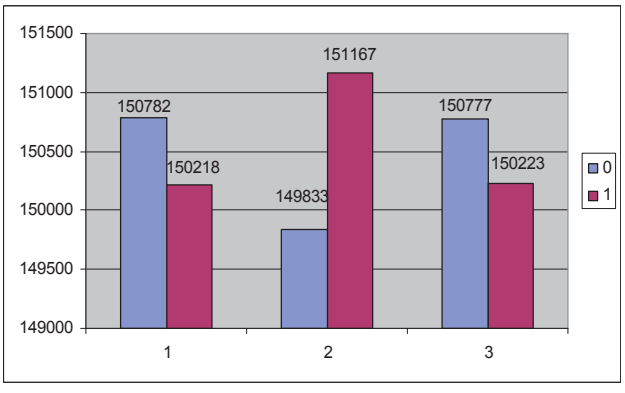

Рис. 3. Проверка числа 0 и 1 в ПСП для трёх вариантов генераторов

На рис. 4 – 5 представлены результата тестирования проверки серий (биграмм и триграмм) генераторов гаммы для алгоритма А5.

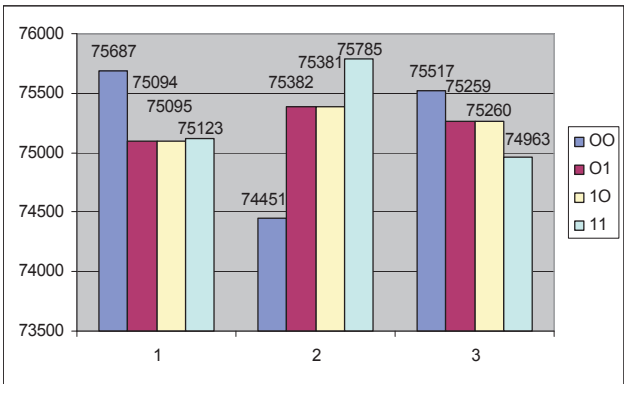

Рис. 4. Проверка серий (биграмм) в ПСП для трёх вариантов генераторов

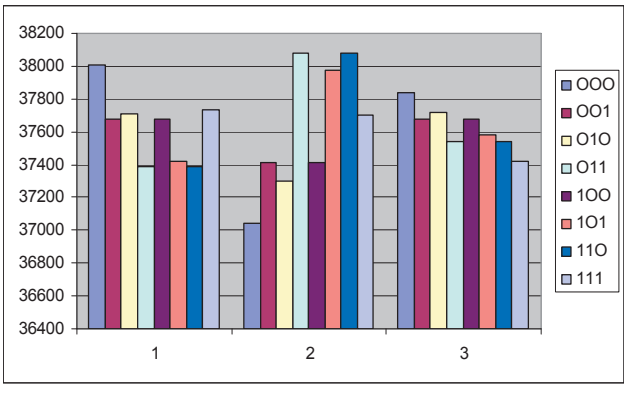

Рис. 5. Проверка серий (триграмм) в ПСП для трёх вариантов генераторов

С помощью программного продукта Mathematica 5.0 было произведено нахождение наименьшего общего кратного периодов LFSR для трёх вариантов алгоритма А5.

Полученные результаты:

1 – 18446702292280803327,

2 – 73786822363236007935,

3 – 7195986431758566174915.

Таким образом, наименьшее общее кратное периодов LFSR принадлежит случаю 3.

Сравнив между собой полученные результаты, можно сделать вывод о том, что среди рассмотренных наилучшим по всем тестам является вариант В генератора ПСП.

7. Выводы

Проведенный сравнительный анализ с помощью тестов для исследования ПСП предложенных модернизаций алгоритма А5 показал, что при увеличении периодов LFSR увеличивается их НОК и, следовательно, результирующий период гаммы. Это приводит к повышению криптостойкости алгоритма А5.

Исследования показали, что вариант «В» модернизации алгоритма А5 оказался наилучшим по всем из проведенных тестов для исследования ПСП.

Научная новизна определяется тем, что предлагаются новые схемы закрытия речевой информации в стандарте GSM.

Практическая значимость полученных результатов состоит в возможности повышения конфиденциальности переговоров в стандарте GSM, за счет использования более совершенных генераторов гаммы.

Литература

1. Лесков А. В., Иванов М. А., Мирский А. А., Рузин А. В., Сланин А. В., Тютвин А.Н. Поточные шифры. – М.: КУДИЦ-ОБРАЗ, 2003. – 336 с. – (СКБ – специалисту по компьютерной безопасности)
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ – ОБРАЗ, 2001 – 386 с.
3. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, А.С. Агиевич. Математические и компьютерные основы криптологии: Учеб. пособие / – Мн.: Новое знание. – 2003. – 382 с.
4. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь, 1999. – 368 с.: ил.
5. Шнайер Б. Прикладная криптология. – М.: Триумф, 2002. – 374 с.
6. Чугунков И. В. Система оценки качества генераторов псевдослучайных кодов // Научная сессия МИФИ-2000. т. 1, 577 с.
7. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. – М.: "Издательство "Полигон", 2000.