XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.VI: С.47-48, 2005.

УДК 621.319.019

А.В.Карабешкин (6 курс, каф. РЭСЗИ), Ю.В.Ветров, к.т.н., доц.

АЛГОРИТМ ШИФРОВАНИЯ ИНФОРМАЦИИ В СТАНДАРТЕ GSM

Стремительное развитие сетей мобильной связи, начавшееся еще в конце XX века и продолжающееся по сей день, ставит вопросы закрытия каналов связи от несанкционированных пользователей на качественно новый уровень. Стандарт GSM стал де-факто основным стандартом мобильной связи в России.

В работе рассматривается структурная схема построения поточного алгоритма A5, применяемого в стандарте GSM для шифрования канала «мобильная станция – базовая станция». Алгоритм основан на РСЛОС (Регистрах сдвига с линейными обратными связями), являющимися основным базовым блоком большинства поточных шифров. Сам по себе РЛСОС линейное устройство, поэтому зависимость между выходной последовательностью и внутренним состоянием генератора линейна. Соответственно, взлом такого РСЛОС является тривиальной задачей. Потому в систему из нескольких РСЛОС вносятся нелинейности. Одним из видов нелинейностей является объединение выходов нескольких РСЛОС нелинейной функцией. Примером такого подхода является генератор Геффе [1]. Однако в таком случае корреляция между выходом системы и внутренним состоянием РСЛОС остается сильной. В табл. 1 показаны результаты анализа Генератора Геффе с общим числом состояний 251.

Как видно из табл. 1, время анализа генератора Геффе с общим числом состояний 251 существенно меньше, чем время анализа РСЛОС с общим числом состояний 232. Это связано с тем, что генератор Геффе состоит из трех РСЛОС, а благодаря обнаруженной корреляции между выходом и внутренним состоянием генератора мы смогли анализировать каждый РСЛОС отдельно, таким образом, мы свели задачу анализа 251 состояний, к задаче анализа 215+217+219 состояний. (Такими были выбраны образующие РСЛОС генератора Геффе).

Таким образом, мы можем сделать вывод о том, что внесение нелинейности описанного вида в систему не может обеспечить необходимой криптографической стойкости.

Вторым методом внесения нелинейности в структуру поточного криптоалгоритма, основанного на РСЛОС является нелинейное управление тактовой частотой РСЛОС. На каждом такте работ системы каждый из РСЛОС может как тактироваться, так и нет, в зависимости от внутреннего состояния других РСЛОС системы. При таком методе организации нелинейности системы мы добиваемся требуемой криптографической стойкости, даже не внося в систему нелинейность первого вида. Чаще всего выходы РСЛОС систему просто объединяются с помощью операции сложения по модулю 2.

Таблица 1. Соотношения времен анализа одиночного РСЛОС и Генератора Геффе.

Время полного перебора значений одиночных РСЛОС		Время криптоанализа генератора Геффе	
Разрядность	Время перебора ключевого пространства	№ эксперимента	Время анализа
18	63 мс	1	23,5 сек
24	4,5 сек	2	21,9 сек
27	56,265 сек	3	26,7 сек
30	8 мин 38 сек	4	42,9 сек

32	31 мин 28 сек	5	37,5 сек

Такой подход был применен разработчиками алгоритма А5 стандарта GSM. Однако алгоритм не лишен недостатков. Основным является недостаточная длина используемых РСЛОС. В алгоритме используются 3 РСЛОС разрядности 19, 22, 23. Кроме того, к недостаткам можно причислить слишком частую инициализацию алгоритма, связанную с организацией информационного обмена между базовой станцией и мобильной станцией. Кроме того, несмотря на то, что общее количество состояний генератора А5 – 64, что равняется суммарной длине трех РСЛОС, длина используемого ключа составляет 54 бит, что существенно снижает стойкость алгоритма.

Кроме того, в странах Ближнего Востока, России и США используется специальным образом ослабленный вариант алгоритма А5 – алгоритм А5/2. Основным отличием от алгоритма А5/1, используемого в странах ЕС, является существенно уменьшенная нелинейность алгоритма.

Несмотря на все замечания по структуре алгоритма А5, можно сказать, что идеи лежащие в его основе неплохи. Алгоритм удовлетворяет всем статистическим тестам, соответствующие исследования были проведены в рамках работы. Единственной принципиальной слабостью алгоритма является выбор РСЛОС небольшой разрядности. Фактически ключ длиной 54 бита может быть вскрыт прямым перебором на современной ЭВМ, за разумное время. Вместе с тем, ничто не мешает для увеличения стойкости алгоритма выбрать РСЛОС большей разрядности, и, не меняя основной структуры алгоритма, добиться существенного увеличения стойкости.

Кроме того, ключ для шифрования вырабатывается в ходе аутентификации абонента в сети GSM. Аутентификация проходит по симметричному алгоритму, который вычисляет 128-битный отклик на входное воздействие в виде RAND запроса с базовой станции (128 бит) и имеющегося в SIM – карте ключа аутентификации (128 бит). Из этого 128 – битного отклика используются только 96 бит, для генерации отклика sRes на запрос RAND, а также ключа шифрования Ki алгоритма А5. Таким образом, у нас есть запас в 32 бита, который мы можем использовать. А значит, мы можем увеличить стойкость алгоритма шифрования А5, не изменяя процедуру аутентификации абонента в сети GSM, а значит, не изменяя схему распределения ключей.

Все исследования касающееся алгоритма А5 носят предположительный характер. Это связано с тем, что консорциум GSM не опубликовал описания алгоритма А5 в открытой печати. Поэтому в исследованиях была использована схема алгоритма приведенного в [1].

ЛИТЕРАТУРА:

1. Б.Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. – М.: ТРИУМФ, 2002 год.