7. Biham E., Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, Springer-Velgar, 1998. – P. 2.

Бабенко Людмила Климентьевна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: blk@fib.tsure.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 312-018.
Кафедра безопасности информационных технологий; профессор.

Babenko Lyudmila Klimentevna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: blk@fib.tsure.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 312-018.
The Department of Security of Information Technologies; professor.

Ищукова Евгения Александровна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: jekky82@mail.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Ischukova Evgeniya Aleksandrovna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: jekky82@mail.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of Security of Information Technologies; associate professor.

УДК 681.03.245

Л.К. Бабенко, Е.А. Ищукова

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ ПОТОЧНЫХ ШИФРОВ*

Рассмотрены основные моменты анализа поточных алгоритмов шифрования с использованием метода дифференциального криптоанализа на примере алгоритма A5/1. Предложена методика проведения дифференциального анализа шифра A5/1, а также других шифров, имеющих сходное строение.

Поточные шифры; дифференциальный криптоанализ; регистр сдвига с обратной линейной связью.

* Работа поддержана грантом РФФИ № 09-07-00245-а.

L.K. Babenko, E.A. Ischukova

DIFFERENTIAL CRYPTANALYSIS OF STREAM CIPHERS

In article highlights of stream ciphers differential cryptanalysis on an example of algorithm A5/1 are considered. The technique of carrying out of the differential analysis of A5/1 cipher and also other ciphers having a similar structure is offered.

Stream ciphers; differential cryptanalysis; linear feedback shift register.

Основной целью криптографической защиты информации является защита от утечки информации, которая обеспечивается путем обратимого однозначного преобразования скрываемых данных в форму, непонятную для посторонних или неавторизованных лиц. Все современные криптоалгоритмы базируются на принципе Керхгофса, согласно которому секретность шифра обеспечивается секретностью ключа, а не секретностью алгоритма шифрования. При этом стойкость криптосистемы зависит от нескольких параметров: от сложности алгоритмов преобразования, от длины ключа, а точнее, от объема ключевого пространства, от метода реализации. По принципу преобразования информации современные криптосистемы можно разделить на два больших класса: блочные и поточные. Блочные криптосистемы преобразуют информацию блоками фиксированной длины, как правило, длина блока равна 32, 64 или 128 битов. Поточные шифры оперируют с битами (реже с байтами), стараясь обеспечить шифрование в режиме реального времени или близком к нему. Высокая скорость работы поточных шифров определяет область их использования – закрытие данных, требующих оперативной доставки потребителю.

На сегодняшний день имеется достаточно большое число различных поточных шифров. Только в книге «Поточные шифры» группы авторов (А.В. Асоков, М.А. Иванов, А.А. Мирский, А.В. Рузин, А.В. Сланин, А.Н. Тютвин), вышедшей в 2003 году в издательстве «КУДИЦ-ОБРАЗ», описано более 20 шифров [1]. Наличие большого числа криптоалгоритмов, направленных на реализацию одной и той же задачи, затрудняет выбор алгоритма, эффективного для использования. Именно в связи с этим возникает необходимость проведения тщательного анализа имеющихся криптосистем поточного шифрования данных с целью выявления их основных особенностей, достоинств и недостатков. В результате такого анализа должны быть получены сравнительные характеристики существующих криптосистем, что позволит выработать рекомендации по их применению. Кроме того, появится возможность разработки новых криптосистем, которые будут учитывать недостатки уже существующих алгоритмов. Применение к разрабатываемым поточным алгоритмам шифрования современных методов криптоанализа позволит еще на этапе проектирования выявить и устранить возможные уязвимости.

Как правило, анализ поточных шифров сводится к анализу математических и статистических свойств генератора гаммы. Порождаемая, известная криптоаналитику, гамма должна обладать следующими основными свойствами: исключать восстановление ключа шифра, не допускать предсказание гаммы по известному ее отрезку (как вперед, так и назад), ничем не отличаться от случайной последовательности.

Такие характеристики, как большой период, высокая сложность и хорошие статистические свойства, – необходимы, но их недостаточно для того, чтобы шифр был криптографически стойким [2].

Помимо основных, общераспространенных методов анализа поточных шифров, существуют и другие методы криптоанализа, которые изначально применялись для анализа блочных шифров. Это, например, такие методы анализа, как линейный и дифференциальный криптоанализ. Все эти методы по отношению к поточным шифрам являются малоизученными.

В качестве объекта изучения был выбран шифр A5/1, как один из наиболее ярких представителей поточных шифров. Шифр A5/1 – это поточный шифр, используемый для шифрования связи GSM (Group Special Mobile – мобильная групповая специальная связь). GSM – европейский стандарт для мобильных цифровых сотовых телефонов. Он используется для шифрования канала «телефон/базовая станция». Каждый кадр шифруется с помощью секретного ключа шифрования Кс и сквозного порядкового номера очередного кадра. Длина ключа составляет 54 бита, длина инициализирующего вектора – 22 бита. Ключ и инициализирующий вектор используются для инициализации трех РСОЛС, которые неупорядоченно сдвигаются.

В основу шифра A5/1 положен генератор, который состоит из трех регистров сдвига с обратной линейной связью (РСЛОС) длиной 19, 22 и 23 битов. Выходом является результат операции сложения по модулю 2 (операция XOR) над тремя РСЛОС. Образующие многочлены этих регистров имеют вид

РСОЛС 1: $x^{19} + x^{18} + x^{17} + x^{14} + 1$,
РСОЛС 2: $x^{22} + x^{21} + 1$,
РСОЛС 3: $x^{23} + x^{22} + x^{21} + x^{8} + 1$.

Выходные биты снимаются со старших разрядов регистров, после чего с помощью операции XOR над битами с выходов всех трех регистров формируется выходной 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 x1 (восьмой разряд) для РСОЛС 1, бит x2 (десятый разряд) для РСОЛС 2 и бит x3 (десятый разряд) для РСОЛС 3.

Функция majority имеет следующий вид:

$$\text{Majority}\,(x1,x2,x3) = x1x2+x1x3+x2x3.$$

Результатом работы этой функции является 1 бит, который определяет, какие регистры будут тактироваться и сдвигать содержащуюся информацию вправо, а какие нет, т.е. если бит с выхода функции совпадает со значением бита x регистра, то информация в регистре сдвигается, иначе нет. Фактически эта функция является функцией большинства, т.е. она принимает то значение, которое преобладает на ее входах. 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.

Процесс формирования гаммы, необходимой для шифрования одного кадра, состоит из следующих шагов.

1) Все три регистра сбрасываются в ноль, а затем тактируются 64 раза без учета режима stop-and-go. Во время этого этапа каждый бит ключа Кс последовательно записывается в самый младший бит каждого регистра после операции XOR с сигналом обратной связи. Так как длина ключа шифрования составляет 54 бита, то недостающие биты образуются с помощью дополнения ключа нулевыми битами.

2) Все три регистра тактируются 22 раза без учета режима stop-and-go. Во время этого этапа биты номера кадра последовательно записываются в самый младший разряд каждого регистра после операции XOR с сигналом обратной связи.

3) Осуществляется 100 тактов работы алгоритма с использованием режима stop-and-go, что обеспечивает перемешивание ключевой информации.

4) Осуществляется 228 тактов работы алгоритма с использованием режима stop-and-go для формирования гаммы. Затем осуществляется шифрование, когда с помощью операции XOR сформированная последовательность накладывается на информацию, содержащуюся в кадре [1].

На сегодняшний день существуют несколько подходов к криптоанализу алгоритма A5/1. Стандартным предположением является то, что криптоаналитику известны определенные биты выходной последовательности A5/1 в определенных кадрах данных. Существует также предположение, что криптоаналитик может получить все выходные биты в течение некоторого начального отрезка разговора, и его задачей является определение ключа для того, чтобы расшифровать оставшуюся часть разговора.

Рассмотрим возможность и особенности применения метод дифференциального криптоанализа к этому шифру. Дифференциальный криптоанализ был впервые описан Э. Бихамом и А. Шамиром в начале 90-х гг. прошлого века применительно к алгоритму шифрования DES. Позднее оказалось, что данный метод анализа может быть применен к широкому классу шифров, в том числе и к поточным. Идея дифференциального ктиптоанализа (ДК) заключается в том, чтобы проследить изменение несходства между двумя отдельными текстами при их зашифровании с использованием того или иного алгоритма. Под несходством двух текстов понимают значение, полученное в результате сложения этих текстов по модулю два. Также в литературе такое несходство часто можно встретить под названием дифференциал, или разность. Разность (дифференциал) двух сообщений принято обозначать знаком Δ.

Возвращаясь к анализу шифра A5/1, вспомним, что объединенные 86 битов ключа K и инициализирующего вектора IV используются для линейной инициализации начального значения 64 битов трех регистров S, входящих в структуру шифра A5/1. Из этого можно сделать вывод, что на вход шифра A5/1 можно подать достаточно большое число различных комбинаций дифференциалов (разностей) вида $(\Delta K, \Delta IV) \rightarrow \Delta S$. В среднем 2^{22} возможных вариантов разностей (ΔK, ΔIV) будут давать после инициализации одно и то же значение ΔS.

Самой лучшей разностью (для которой $\Delta S \neq 0$ после загрузки ключа и номера кадра) является входная разность $(\Delta K, \Delta IV) = (0000015F102D07E2_x, 08EDB3_x)$ [3]. С вероятностью 1 она ведет к двум внутренним состояниям регистров $S^1 = (R^1_1, R^1_2, R^1_3)$ и $S^2 = (R^2_1, R^2_2, R^2_3)$, разность которых равна $\Delta S = S^1 \oplus S^2 = (R^1_1 \oplus R^2_1, R^1_2 \oplus R^2_2, R^1_3 \oplus R^2_3) = (0, 000800x, 0)$. Таким образом, $R^1_1 \oplus R^2_1 = 0$, $R^1_2 \oplus R^2_2 = 000800x$, $R^1_3 \oplus R^2_3 = 0$.

Каждое из этих двух состояний $S^1 = (R^1_1, R^1_2, R^1_3)$ и $S^2 = (R^2_1, R^2_2, R^2_3)$ тактируется 100 раз в режиме stop-and-go. Так как первые биты разностей для всех трех регистров состояний равны нулю, то в самом начале нет разницы в битах, которые поступают в блок синхронизации, и поэтому число раз, когда состояние S^1 было тактировано, равно числу раз, когда было тактировано S^2. С каждым тактированием значение разности в регистре R_2 меняется путем сдвига содержимого регистра. Так продолжается до тех пор, пока в бит регистра R_2, участвующий в операции отвода, не попадет значение 1. В следующий раз, когда регистр R_2 сдвинется после

этого события, бит разности загружается в регистр R_2 и разность внутренних состояний становится равной (0, 200001x, 0). После следующего сдвига R_2 разность между R^1_2 и R^2_2 составит 000003x, то есть в битах R_2 [0,1].

Разность между значениями R_2 будет продолжать меняться, то есть сдвигаться тогда, когда R^1_2 и R^2_2 сдвигаются (сдвиг в регистрах R^1_2 и R^2_2 будет происходить одновременно, так как в контрольных битах нет разницы). Так будет происходить до тех пор, пока значение 1 в разности не достигнет контрольного бита. Исследования показывают, что с вероятностью $0{,}197 = 2^{-2.346}$ разность между состояниями станет равной (0, 001800x, 0), то есть все регистры были сдвинуты одинаковое число раз, и разность больше не влияет на контрольный бит.

С этого момента опять нет разницы в контрольных битах, и разность R_2 меняется с вероятностью 1 до тех пор, пока R_2 не станет равным 300000x. Эта разность преобразуется в значение (0, 000500x, 0) и проходит через контрольный бит с вероятностью $0{,}135 = 2^{-2.890}$. Затем разность проходит по кругу регистр и достигает значения (0, 00000Fx, 0). Эта разность меняется до значения (0, 000011x, 0) с вероятностью $0{,}092 = 2^{-3.439}$. Преобразование разности внутренних состояний регистров приведено в табл. 1.

Таблица 1

Преобразование разностей внутреннего состояния A5/1 при заданной разности (ΔK, ΔIV) = (0000015F102D07E2$_x$, 08EDB3$_x$)

Событие	Число раз, когда R2 был сдвинут	Значение разницы	Вероятность
После инициализации ключа	0	(0, 000800x, 0)	1
Разность поступает в R2[21]	10	(0, 200001x, 0)	1
Разность покидает R2[21]	11	(0, 000003x, 0)	1
Разность начинает сдвигаться	20	(0, 000600x, 0)	1
Разность проходит сдвиг	22	(0, 001800x, 0)	$2^{-2.346}$
Разность покидает R2[21]	32	(0, 000005x, 0)	1
Разность начинает сдвигаться	40	(0, 000500x, 0)	1
Разность проходит сдвиг	43	(0, 002800x, 0)	$2^{-2.346}$
Разность покидает R2[21]	53	(0, 00000Fx, 0)	1
Разность начинает сдвигаться	60	(0, 000780x, 0)	1
Разность проходит сдвиг	64	(0, 007800x, 0)	$2^{-2.346}$
Разность покидает R2[21]	74	(0, 000011x, 0)	1

После 100 тактов, во время которых выходной результат отбрасывался, шифр A5/1 начинает выводить поток битов ключа Кс. Когда выходной поток начинает

вырабатываться, разность в выходном потоке может быть определена (если два значения имели предсказанную разность).

Проблема заключается в том, что точная разность неизвестна так же, как неизвестно точное число раз, когда регистр R_2 был сдвинут во время инициализации. Однако наиболее вероятное число сдвигов регистра R_2 равно 79 [3]. Это число сдвигов посчитано с вероятностью 0,092, то есть с вероятностью 0,197*0,135*0,092*0,092 = 0,000225≈1/4442 разность между состояниями регистров будет равна (0, 000044x, 0). Было замечено, что существуют несколько подобных разностей, в которых число сдвигов регистра R_2 немного отличается (и их вероятность немного ниже 1/4442).

Если разность, определенная нами, выполняется, то первый выходной бит потока равен нулю, то есть (0, 000044x, 0) → 0 с вероятностью 1. Фактически, первые три бита выходного потока неизбежно не будут иметь разницы с вероятностью по крайней мере 0,58 (выходной поток не будет обязательно различаться, даже если различается число сдвигов каждого регистра).

На основании рассмотренного можно сформулировать методику осуществления дифференциального криптоанализа алгоритма шифрования A5/1, которая сводится к следующему:

1. Подобрать такую пару (ΔK, ΔIV), которая после инициализации ключа и инициализирующего вектора дают разность внутренних состояний регистров $\Delta R_1 = 0$, ΔR_2 = 000800x, $\Delta R_3 = 0$. Для этого необходимо построить и решить систему уравнений. Для решения можно использовать метод Гаусса.
2. Проследить возможный путь преобразования ΔK и ΔIV в режиме инициализации stop-and-go. Состояние регистров после инициализации обозначим как ΔZ.
3. Проследить преобразование разности ΔZ и определить наиболее вероятное значение $\Delta\gamma$.
4. Подобрать такие γ и γ', для которых $\gamma \oplus \gamma' = \Delta\gamma$. При этом считать, что γ и γ' были соответственно получены из таких пар (K, IV) и (K', IV'), для которых $K \oplus K' = \Delta K$, а $IV \oplus IV' = \Delta IV$.
5. С учетом знания, в какие такты в регистрах R_1, R_2 и R_3 был произведен сдвиг для пары γ и γ', найти все возможные состояния регистров Z и Z'. Для этого необходимо построить и решить все возможные системы уравнений. Для решения можно использовать метод Гаусса.
6. Отобрать те состояния, для которых $Z \oplus Z' = \Delta Z$.
7. Восстановить K, K', IV и IV'.
8. Искомым значением будет пара, для которой: $K \oplus K' = \Delta K$ и $IV \oplus IV' = \Delta IV$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Асосков 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.

2. *Бабенко Л.К., Наумов И.В.* Реализация и тестирование поточного шифра WG // Материалы IX Международной научно-практической конференции «Информационная безопасность». Ч.2. – Таганрог, 2007. – С. 121–125.

3. *Biham E, Dunkelman O.* Differential Cryptanalysis in Stream Ciphers / Eli Biham, Orr Dunkelman. – Dept. of Electrical Engineering ESAT/SCD-COSIC. Kasteelpark Arenberg 10.

4. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002. – 816 с.

Бабенко Людмила Климентьевна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: blk@fib.tsure.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 312-018.
Кафедра безопасности информационных технологий; профессор.

Babenko Lyudmila Klimentevna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: blk@fib.tsure.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 312-018.
The Department of Security of Information Technologies; professor.

Ищукова Евгения Александровна
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: jekky82@mail.ru.
347928, г. Таганрог, ул. Чехова, 2, корпус "И".
Тел.: 8 (8634) 371-905.
Кафедра безопасности информационных технологий; доцент.

Ischukova Evgeniya Aleksandrovna
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: jekky82@mail.ru.
Block “I”, 2, Chehov str., Taganrog, 347928, Russia.
Phone: 8 (8634) 371-905.
The Department of Security of Information Technologies; associate professor.