9. *Мкртичян В.В.* Компьютерные модели списочных декодеров Гурусвами-Судана для обобщенных кодов Рида-Соломона и конкатенированных кодов // Вестник ДГТУ, 2007. Т.7. №4. – С. 384-394.

10. *Мкртичян В.В.* Особенности реализации программных модулей списочных декодеров Гурусвами-Судана в компьютерной модели схемы специального широковещательного шифрования. В сб. "Интегро-дифференциальные операторы и их приложения." Вып. 8. – Ростов-на-Дону, 2008. – С. 104-116.

11. *Мкртичян В.В.* О программной реализации моделей коалиционной атаки и защиты от коалиционных атак схемы специального широковещательного шифрования. В сб. " Интегро-дифференциальные операторы и их приложения." Вып. 8. – Ростов-на-Дону, 2008. – С. 94-103.

12. *Евпак С.А.*, *Мкртичян В.В.* Особенности программной реализации модели распространения данных схемы специального широковещательного шифрования. В сб. " Интегро-дифференциальные операторы и их приложения." Вып. 8. – Ростов-на-Дону, 2008. – С. 61-71.

13. *Влэдуц С.Г.*, *Ногин Д.Ю.*, *Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. – М.: МЦНМО, 2003. – 504 с.

14. *Мак-Вильямс Ф.Д.*, *Слоэн Н.Дж.* Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

15. *Деундяк В.М.*, *Мкртичян В.В.* Исследование границ применения одной схемы защиты данных. В сб. "Труды участников международной школы-семинара по геометрии и анализу". – Ростов-на-Дону: ЮФУ, 2008.

16. *Чистяков В.П.* Курс теории вероятностей. – М.: Наука, 1982. – 256 с.

УДК 681.03.245

Е.А. Ищукова

ИССЛЕДОВАНИЕ ВЛИЯНИЯ БЛОКОВ ЗАМЕНЫ НА УСТОЙЧИВОСТЬ АЛГОРИТМОВ ШИФРОВАНИЯ*

За последние два десятилетия совершен большой скачок в развитии компьютерной техники. Чтобы убедиться в этом, достаточно сравнить вычислительные мощности, которые были доступны обычному пользователю 20 лет назад и сейчас. Такое бурное развитие компьютерной техники повлекло за собой стремительное развитие других наук так или иначе связанных с вычислительными задачами. Можно сказать, что наибольшее влияние было оказано на криптографию, так как пока не было вычислительно мощных систем задачи криптографии в основном сводились к различного рода головоломкам и использовали в своей основе различные шифры замен и подстановок. Однако в конце XX века вместе с ростом вычислительных ресурсов начала развиваться и криптография. Появились принципиально новые подходы к построению схем шифрования. Широкое развитие получила симметричная криптография в связи с принятием в конце 70-х годов прошлого века в качестве государственного стандарта шифрования данных США алгоритма DES. Также был найден новый подход для шифрования данных, легший в основу асимметричных алгоритмов шифрования.

Вместе с развитием криптографии, то есть вместе с появлением все новых и новых алгоритмов шифрования появилась и необходимость выявления методов их надежности. То есть необходимо было выяснить, насколько использование того

* Работа выполнена при поддержке гранта РФФИ №06-07-89010-а

или иного алгоритма шифрования данных обеспечит надежную передачу данных с учетом достаточно быстро растущих вычислительных мощностей, доступных обычному обывателю. Все это привело к многочисленным попыткам криптографов разных стран выявить различные подходы к анализу существующих и широко используемых систем шифрования. Так зародилось отдельное направление науки криптологии, названное криптоанализом. Из всего многообразия выявленных на сегодняшний день методов и подходов к анализу симметричных алгоритмов шифрования можно выделить методы линейного и дифференциального криптоанализа (ЛК и ДК). Изначально оба эти метода были применены к алгоритму шифрования DES [1, 2, 3]. При этом было показано, что анализ алгоритма с использованием этих методов может быть проведен гораздо быстрее, чем это можно было бы сделать с использованием метода грубого перебора. Здесь, однако, следует отметить, что для применения метода грубого перебора достаточно всего одной пары текстов (открытый текст – шифрованный текст), в то время как для вышеуказанных методов требуются достаточно большие объемы данных, зашифрованных на одном и том же ключе, что делает эти методы анализа практически непригодными для использования на практике.

Знание методов линейного и дифференциального криптоанализа является обязательным для каждого криптографа, так как это позволяет значительно повысить стойкость шифра еще на этапе его проектирования. Известно, например, что разработчикам алгоритма DES был известен метод дифференциального криптоанализа [4], хотя широкая общественность узнала об этом методе больше 10 лет спустя после опубликования алгоритма DES.

На сегодняшний день применение методов линейного и дифференциального криптоанализа рассмотрено применительно к большому числу алгоритмов блочного шифрования. Однако, как правило, это алгоритмы, имеющие в своей структуре фиксированные блоки замены (или S-блоки, как их еще называют). Наше внимание остановилось на алгоритмах шифрования, в которых блоки замены не являются фиксированными и могут меняться в зависимости от некоторых параметров. К таким алгоритмам, например, относится действующий стандарт России ГОСТ 28147-89, что делает данное исследование еще более значимым.

Целью работы является исследование влияния используемого блока замены или набора блоков замены в их совокупности на стойкость исследуемого алгоритма к методам линейного и дифференциального криптоанализа.

В работе [5] показано за счет каких механизмов становится возможным применение дифференциального криптоанализа к блочным алгоритмам шифрования на примере одного раунда алгоритма шифрования DES. Из приведенного примера видно, что операция сложения данных с ключом по модулю два, влияющая на сохранность в секрете шифруемых данных, не принимается во внимание при рассмотрении дифференциального криптоанализа. Дело в том, что при рассмотрении дифференциального криптоанализа рассматривается сумма двух текстов. А так как к каждому тексту прибавляется один и тот же секретный ключ, то при рассмотрении дифференциала (то есть разности двух текстов), происходит взаимное исключение ключей в виду свойств используемой операции сложения по модулю два. Метод дифференциального криптоанализа очень подробно рассмотрен в работе [6]. В этой работе разработан подробный алгоритм анализа S-блоков замены. Приведем этот алгоритм здесь, ввиду того, что мы будем использовать его в дальнейшей работе.

1. Берется очередной блок замены, на вход которого поступает n бит.

2. В таблице анализа для данного блока замены все исходные значения полагаются равными 0.
3. Определяется первое возможное значение входной разности $\Delta A=0$.
4. Определяется значение первого входа $X=0$ в анализируемый S-блок.
5. Вычисляется второе значение входа $X' = X \oplus \Delta A$.
6. Для входов X и X' в соответствии с принципом работы S-блока определяются соответственно выходы Y и Y'.
7. Вычисляется значение выходной разности $\Delta C = Y \oplus Y'$.
8. В таблице анализа увеличивается на 1 значение, стоящее на пересечении строки с номером ΔA и столбца с номером ΔC.
9. Значение X увеличивается на 1.
10. Если $X<2^n$, то происходит переход к пункту 5.
11. Значение ΔA увеличивается на 1.
12. Если $\Delta A < 2^n$, то происходит переход к пункту 4.
13. Если не все блоки замены проанализированы, то происходит переход к пункту 1, иначе алгоритм заканчивает свою работу.

В ходе исследования, проведенного в работе [6] был проведен анализ алгоритма шифрования DES (алгоритма, в котором все блоки замены фиксированы) с использованием РМВ. Для алгоритма шифрования ГОСТ 28147-89 (в котором блоки замены не фиксированы) были разработаны алгоритмы поиска дифференциалов, а также алгоритмы поиска правильных пар текстов и секретного ключа на их основании. Однако один важный вопрос так и не был освещен в данной работе. Существуют ли блоки замены для алгоритма шифрования ГОСТ 28147-89, которые могут значительно ослабить стойкость алгоритма и позволить вычислить ключ с использованием метода дифференциального криптоанализа. На этот вопрос мы постараемся дать ответ в ходе работы над данным дипломным проектом. Для этого необходимо выделить критерии, на основе которых на начальном этапе анализа мы будем проводить отбор блоков замены, разделяя их на три класса:

– стойкие блоки замены;
– нестойкие блоки замены;
– блоки замены средней стойкости.

Из исследования [6] видно, что если для блоков замены, используемых в алгоритме шифрования, при рассмотрении дифференциальных свойств, есть возможность преобразования ненулевой входной разности в нулевую выходную, то это ослабляет защитные свойства алгоритма шифрования и позволяет успешно проводить атаку с использованием метода дифференциального криптоанализа. Поэтому те блоки замены, для которых при рассмотрении дифференциальных свойств будет возможна замена ненулевой входной разности на нулевую выходную, мы будем относить к нестойким блокам замены.

Также известно, что чем равномернее распределение вероятностей в таблице анализа, тем более блок устойчив к дифференциальному криптоанализу. Поэтому те блоки, для которых будет наблюдаться равномерное распределение (а это значит, что в таблице не будет значений совпадений больше двух) будем относить к классу стойких. А те блоки замены, для которых в таблице анализа будут присутствовать значения вероятностей, равные 1 (за исключением значений для входной разности, равной нулю, так как она всегда (с единичной вероятностью) будет давать на выходе 0), будем относить к классу нестойких. Все остальные блоки замены мы будем относить к классу блоков замены средней стойкости.

В работе [12] авторами рассмотрены основные аспекты применения метода линейного криптоанализа к современным блочным алгоритмам шифрования. Как

и в случае дифференциального криптоанализа, при линейном криптоанализе первым важным шагом является анализ нелинейных элеметов, роль которых в большинстве блочных алгоритмов шифрования выполняют S-блоки замены. При этом для алгоритмов шифрования, в которых блоки замены фиксированы (например, алгоритм шифрования DES), этот анализ можно выполнить один раз и в дальнейшем пользоваться результатами анализа. Для тех алгоритмов шифрования, в которых блоки замены не зафиксированы (например, алгоритм шифрования ГОСТ 28147-89) анализ необходимо выполнять каждый раз для нового набора блоков. Таблицы анализа заполняются в соответствии с формулой (1)

$$Q_{(i)} = (Y_{(i)}, \alpha_{(i)}) \oplus (X_{(i)}, \beta_{(i)}) \oplus (K_{(i)}, \chi_{(i)}). \quad (1)$$

По вертикали таблицы записываются возможные значения единичного вектора β для входных данных X, по горизонтали – все возможные значения единичного вектора α для выходных данных Y. Все остальные ячейки таблицы заполняются в соответствии с формулой (2). В результате такого заполнения мы получаем значения вероятности равенства значения Q из формулы (1) нулю. Важно заметить, что в большинстве случаев на вход блока замены поступает значение сообщения, сложенное со значением ключа K, поэтому для ключа K используется также единичный вектор α. Опираясь на это, можно сформулировать алгоритм анализа блока замены для линейного криптоанализа, аналогично тому, как это было сделано для дифференциального криптоанализа блоков замены:

1. Берется очередной блок замены, на вход которого поступает n бит.
2. В таблице анализа для данного блока замены все исходные значения полагаются равными 0.
3. Определяется первое возможное значение единичного вектора β.
4. Определяется значение первого единичного вектора α.
5. Определяется первое возможное значение входа X в S-блок замены.
6. Для входа X в соответствии с принципом работы S-блока определяется выход Y.
7. Вычисляется значение Q в соответствии с формулой (2).
8. Если Q=0, то в таблице анализа увеличивается на 1 значение, стоящее на пересечении строки с номером единичного вектора β и столбца с номером единичного вектора α.
9. Значение X увеличивается на 1.
10. Если X<2n, то происходит переход к пункту 5.
11. Берется следующее возможное значение единичного вектора α.
12. Если все возможные значения единичного вектора α проанализированы, то происходит переход к пункту 13, иначе переход к пункту 6.
13. Берется следующее возможное значение единичного вектора β.
14. Если все возможные значения единичного вектора β проанализированы, то происходит переход к пункту 15, иначе переход к пункту 4.
15. Если не все блоки замены проанализированы, то происходит переход к пункту 1, иначе алгоритм завершает свою работу.

Как и в случае с дифференциальным криптоанализом алгоритма шифрования ГОСТ 28147-89, для линейного криптоанализа также остается открытым вопрос о том, существуют ли такие блоки замены, которые могут значительно ослабить стойкость алгоритма и позволить вычислить ключ с использованием метода линейного криптоанализа. На этот вопрос мы также постараемся дать ответ в ходе работы над данным дипломным проектом. Для этого, как и в предыдущем случае,

нам необходимо выделить критерии, на основе которых на начальном этапе анализа мы будем проводить отбор блоков замены, разделяя их на три класса:

– стойкие блоки замены;
– нестойкие блоки замены;
– блоки замены средней стойкости.

Известно, что для линейного криптоанализа необходимо построить эффективные линейные аналоги. Эффективность линейного аналога определяется значением отклонения $\Delta(Q_{(i)}) = |1\text{-}2p|$ (необходимо различать использование знака Δ для обозначения разности (дифференциала) при дифференциальном криптоанализе и для обозначения отклонения при линейном криптоанализе). Чем больше отклонение (что возможно как при малом значении вероятности p, так и при большом), тем эффективнее аналог. Если отклонение равно 0, что возможно при значении вероятности p = ½, то аналог неэффективен и не может быть использован для дальнейшего анализа. В связи с этим, те блоки, для которых будет наблюдаться равномерное распределение (а это значит, что в таблице все значения вероятностей будут равны ½, или близки к этому значению) будем относить к классу стойких. А те блоки замены, для которых в таблице анализа будут присутствовать значения вероятностей, близкие к 1 или к 0, будем относить к классу нестойких. Все остальные блоки замены мы будем относить к классу блоков замены средней стойкости.

Ранее мы отмечали, что для криптоанализа требуются достаточно большие вычисления. При решении нашей задачи нам необходимо будет проанализировать все возможные варианты для используемых блоков замены. Так как в качестве объекта анализа нами выбран алгоритм шифрования ГОСТ 28147-89, то мы будем ориентироваться на структуру блоков, используемых в этом алгоритме. На вход этих блоков замены поступают 4-х битовые значения, которые преобразуются в 4-х битовые выходные значения. Таким образом, на вход блока замены может поступить значение в диапазоне от 0 до 15 (всего 16 значений), а это значит, что есть 16! = 20922789888000 возможных значений для заполнения блока замены. Естественно, что для обработки всех вариантов с помощью одной вычислительной станции потребуется достаточно большое количество времени. Поэтому целесообразно использовать распределенные многопроцессорные вычисления. В качестве средства для разработки параллельных программ нами был выбран стандарт MPI. Большим достоинством при этом является возможность осуществлять вычисления как на кластерных системах, так и с использованием незадействованных ресурсов вычислительных систем, объединенных в одну сеть.

При разработке параллельных алгоритмов самым главным является правильная организация межпроцессорных взаимодействий. Однако при рассмотрении решаемой нами задачи, мы пришли к выводу, что все процессы могут выполнять анализ отведенных им блоков замены независимо друг от друга. В этом случае важной задачей остается правильное (равномерное) распределение данных для осуществления анализа. Проблема заключается в том, что нам необходимо осуществить перебор всех возможных заполнений S-блоков замены, то есть все возможные сочетания из 16 элементов (от 0 до 15). Вопрос заключается в том, как грамотно задать тому или иному процессу, какие заполнения S-блока необходимо проанализировать. Обзор существующей литературы позволил найти алгоритм, позволяющий получить из сочетания чисел некоторое десятичное число. Этот алгоритм приведен в [8]. Опираясь на этот алгоритм, мы получили обратный ему, позволяющий получать из десятичного числа уникальную последовательность. Таким образом, задача распределения данных свелась к равномерному распреде-

лению диапазона анализа (от 0 до 16!-1) между процессами, участвующими в вычислениях. Для решения этой задачи мы использовали алгоритм, разработанный и опробованный в работе [6].

Параллельный алгоритм, разработанный для оценки стойкости блоков, прошел тестовые испытания с использованием вычислительного кластера HP(20 процессорных ядер IntelXeon 1,77 МГц; 10 Гб ОЗУ; Gigabit Ethernet). Показано линейное сокращение времени вычислений при увеличении числа задействованных процессоров. В ходе эксперимента получены некоторые (но не все) блоки замены и их таблицы анализа для алгоритма шифрования ГОСТ 28147-89 как для линейного, так и для дифференциального криптоанализа. Показано, что полный анализ всех вариантов блоков замены для алгоритма ГОСТ 28147-89 займет примерно 20 – 23 суток. Дальнейшее исследование полученных блоков замены заключается в поиске дифференциалов, обладающих максимальной вероятностью, и оценке вычислительной сложности алгоритма ГОСТ 28147-89 с их использованием. Алгоритм поиска дифференциалов разработан в работе [6]. С его использованием планируется получить теоретические оценки, которые в дальнейшем будут проверены на практике.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *E. Biham, A. Shamir*: “Differential Cryptanalysis of the Full 16-round DES”, Crypto'92, Springer-Velgar, 1998. P. 487.

2. *E. Biham, A. Shamir*: “Differential Cryptanalysis of DES-like Cryptosystems”, Extended Abstract, Crypto'90, Springer-Velgar, 1998. P. 2.

3. *M. Matsui*: “Linear Cryptanalysis Method for DES Cipher”, Advances in Cryptology – EUROCRYPT’93, Springer-Verlag, 1998. P. 386.

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

5. *Чмора А.Л.* Современная прикладная криптография. 2-е изд. – М.: Гелиос АРВ, 2002.

6. *Е.А. Ищукова*. Разработка и исследование алгоритмов анализа стойкости блочных шифров методом дифференциального криптоанализа [Текст] / Е.А. Ищукова // Научная работа депонированная в ВИНИТИ.

7. *Бабенко Л.К., Ищукова Е.А.* Современные алгоритмы блочного шифрования и методы их анализа – М.: Гелиос АРВ, 2006.

8. *Кнут Д.Э.* Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е изд.: Пер. с англ.: Уч. пос. – М. : Издательский дом «Вильямс», 2000. – 832 с.