УДК 004.491.22

М.Е. Бурлаков, А.А. Петросян

Самарский национальный исследовательский университет

ПРИМЕНИМОСТЬ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ К КРИПТОАНАЛИЗУ ШИФРА DES

В статье рассматривается вопрос применимости адаптивных алгоритмов (генетические алгоритмы) к возможности оптимизации дифференциальных и линейных атак на криптоалгоритм DES.

Ключевые слова: генетический алгоритм, криптоанализ, дифференциальный криптоанализ, линейный криптоанализ, криптоаглоритм DES

Введение

В настоящее время существует большое количество криптографических алгоритмов (КА), обеспечивающих защиту всевозможных информационных систем. Каждый КА имеет свои не только сильные, но и слабые стороны, позволяющие злоумышленнику осуществить процесс криптоанализа с последующим раскрытием исходного шифртекста.

Существует множество техник, позволяющих проверить (протестировать) устойчивость КА к криптоанализу. К таковым можно отнести: дифференциальный анализ, линейный анализ и т.д.[1][2]. Зачастую, процесс криптоанализа требует больших затрат вычислительных ресурсов, что приводит к усложнению проверки стойкости КА к криптоанализу.

Одной из наиболее перспективных техник оптимизации криптоанализа является применение адаптивных алгоритмов – нейронных сетей, генетических алгоритмов, искусственных иммунных систем и т.д. [3].

1. Криптоалгоритм DES. Правильные пары

Шифр *DES* – алгоритм блочного шифрования, в основе которого лежит сеть Фейстеля с 16-ю циклами. Размеры блока и ключа равны 64 бит. Алгоритм использует комбинацию нелинейных (*S*-блоки) и линейных (перестановки *E, IP, IP*$^{-1}$) преобразований.

Дифференциальный криптоанализ представляет собой атаку на основе подобранного открытого текста, где подбираются пары открытых текстов с опре-

деленной *XOR*-разницей и анализируется вероятность появления различных пар шифр текстов (также по *XOR*-разнице). Эти вероятности могут быть использованы для того, чтобы найти вероятности возможных ключей и найти наиболее вероятные биты. Этот тип атаки основан на n-раундовых характеристиках, которые позволяют хранить информацию о промежуточных *XOR*-разницах после как можно большего количества раундов. Каждый раунд имеет определенную разницу открытых текстов ΩP, определенную разницу промежуточных результатов на n-том раунде ΩT и вероятность P того, что пара открытых текстов в результате шифрования имеет промежуточные различия, совпадающие с указанными в характеристике промежуточными результатами.

Под правильной парой понимается любая пара, значение открытого текста которой равно ΩP, а значение шифртекста после n раундов преобразования равно ΩT, в противном случае пара называются неправильной [1].

Отношением сигнала(S)/шума(N) (1) определяется отношение между числом правильных пар и средним количеством неправильных под-ключей [1]:

$$S/N = \frac{m \cdot P}{m \cdot \frac{\alpha \cdot \beta}{2^k}} = \frac{2^k \cdot p}{\alpha \cdot \beta} \qquad (1)$$

где m – число созданных пар, P – вероятность характеристики, α – среднее число предложенных ключей к каждой паре, m, β – число проанализированных пар среди всех пар, k – количество посчитанных бит ключа и 2^k – количество возможных ключей. Соотношение S/N используется для определения соотношения вероятности появления правильного ключа к вероятности появления случайного ключа.

Перед рассмотрением использования ГА в криптоанализе необходимо обозначить ряд понятий и определений.

2. Применение генетического алгоритма к криптоанализу алгоритма DES

Генетический алгоритм –это эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых решений [4]. Хромосома в ГА – вектор значений, определяющих некоторое решение поставленной задачи [4]. Приспособленность – значение, определяющее, насколько хорошо закодированное в хромосоме решение справляется с поставленной задачей [4]. Популяция – конечное множество хромосом. Для создания новой популяции из текущей в ГА выделяют функции скрещивания и мутации.

Изначально некоторым образом создается начальная популяция. Каждая хромосома популяции оценивается с помощью функции приспособленности. При помощи функций скрещивания и мутации образуется новая популяция решений. Хромосомы с наибольшим значением приспособленности имеют больший шанс участия в скрещивании. Для хромосом новой популяции также вычисляется значение приспособленности, и затем производится отбор лучших решений в следующее поколение.

Этот набор действий повторяется итеративно, пока не будет выполнен критерий остановки алгоритма. Таким критерием может быть:

1) нахождение глобального, либо локального решения;

2) исчерпание числа поколений, отпущенных на эволюцию;

3) исчерпание времени, отпущенного на эволюцию и т.д.

В рамках криптоанализа шифра *DES* хромосома будет кодировать некоторый ключ. Соответственно, необходимо определить функцию приспособленности.

Для проведения дифференциального криптоанализа с применением ГА в работах [5], [6] предлагается использовать следующую функцию приспособленности:

$$C_r = \frac{n_{sr}}{n_p}, \qquad (2)$$

где C_r – корректность хромосомы, n_{sr} – число правильных пар, сгенерированных хромосомой и n_p – общее число правильных пар. Значение C_r прямо пропорционально значению $n_{sr,}$ так как n_p фиксировано. $C_r < 1$, за исключением случая, когда $n_{sr} = n_p$.

Для демонстрации техники применения ГА в дифференциальном анализе, работа алгоритма *DES* рассматривается в реализации с 6 раундами с использованием 3х-раундовых характеристиках с ΩP = 40800000 04000000*x* с конечной целью выделения не менее 30 бит ключа. Рассмотрим хромосому длиной 30 бит, содержащую 5 под-ключей для *S*-блоков, каждый из которых состоит из 6 бит. Начальная и конечная перестановки будут опущены, так как они не имеют никакой криптографической значимости.

В соответствии с 3-х-раундовой характеристикой (Рисунок 2), если добавить четвертый раунд, имеющий соотношение вида ‘d =’b $\oplus$ ‘C с входным параметром 40800000x, то результирующим значением в 5-ти S-блочной структуре (S2,S5…S8) по выполнении операции XOR получим нулевое значение. Шестой раунд рассчитывается из следующего соотношения ′F = ′c $\oplus$

′D ⊕ ′l. Ожидаемая вероятность правильной пары равна 1/16 относительно характеристик по результатам работы 3 раундов.

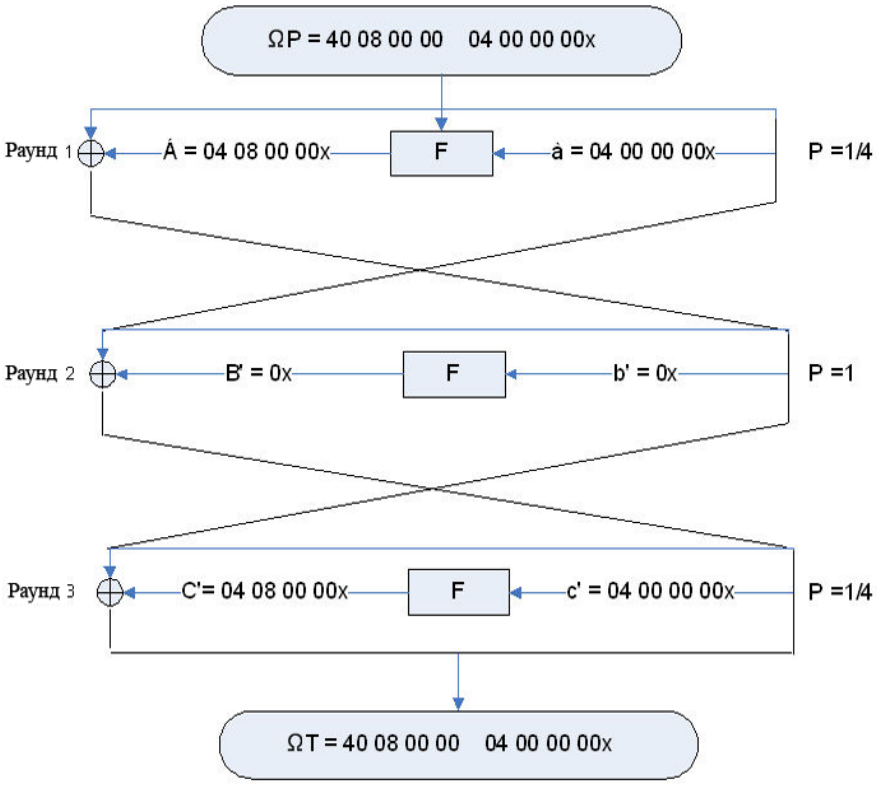

Рисунок 1 – 3-х-раундовая характеристика алгоритма *DES*

2.1. Порядок применения генетического алгоритма в дифференциальном анализе

Изначально генерируется заданное количество случайных пар с фиксированной разницей *ΩP*=40800000 04000000*x* с последующим их 67нновационем. Из полученных пар выбираются правильные. С помощью ГА находится наилучшая хромосома, кодирующая 5 под-ключей 6-ти *S*-блоков (*S*2, *S*5, …, *S*8). Если полученная хромосома имеет приспособленность не меньше нужной, то результат выполнения алгоритма успешный. Полученные 30 бит 67нноча размещаются в нужные позиции и грубым перебором вычисляются остальные 26 бит.

Замечание: вышеописанный алгоритм может быть использован с различными 3-х раундовыми характеристиками (00200008 00000400*x*) , чтобы получить дополнительно 12 бит ключа (для *S*1 и *S*4), чтобы уменьшить перебор с 26 бит до 14.

2.2. Реализация применения генетического алгоритма в дифференциальном анализе

Дифференциальный криптоанализ с применением ГА был реализован авторами с использованием языка программирования *Java*, а также открытой библиотеки *The Watchmaker Framework*.

При помощи описанного ранее алгоритма удалось взломать 6-ти раундовую версию *DES* и извлечь под-ключи *S*-блоков *S*2, *S*5, *S*6, *S*7 и *S*8, имея 100 правильных пар с определенной *XOR*-разницей.

В дальнейшем, авторы видят следующие пути улучшения качества работы алгоритма:

1) использование линейного криптоанализа с применением ГА для первоначального определения некоторого количества бит;

2) определение влияния определённых операций (преобразований) шифрования на значение вектора хромосомы.

Также рассматривается возможность применения ГА в криптоанализе не только усложненной версии шифра *DES*, но и в других КА и хэш-функциях.

Литература

1. Biham E. Differential Cryptanalysis of DES-like Cryptosystems / Eli Biham, Adi Shamir // The Weizmann Institute of Science Department of Applied Mathematics, 1990.

2. Matsui M. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology-EUROCRYPT’93, 1994.

3. Бурлаков М.Е. О некоторых моделях оптимизации искусственной нейронной сети генетическими алгоритмами // Перспективные информационные технологии (ПИТ-2014): труды Международной научно-технической конференции. – Самара: Издательство Самарского научного центра РАН, 2014. – 99-105 с.

4. Генетический алгоритм [Электронный ресурс], − Режим доступа: https://ru.wikipedia.org/.

5. Bahaa-Eldin A.M. Intelligent Systems for Information Security // Ph.D. Thesis, Ain Shams University, 2004. – P. 82.

6. Hassan M.H. A Genetic Algorithm for Cryptanalysis with Application to DES-like Systems // International Journal of Network Security, Vol.8, 2009. – P.177-186.