Е. Ю. Родионов
Московский инженерно-физический институт (государственный университет)

Применение запутывающих преобразований в криптографических целях

Целью настоящей работы является систематизация знаний и результатов в области запутывающих преобразований, разработка и изучение методов запутывания криптографических конструкций, оценка алгоритмической сложности запутывающих преобразований. В данной работе рассматривается метод запутывания симметричных блочных шифров, имеющих в основе своей конструкции петлю Фейстеля, а так же попытки криптоанализа получившейся конструкции.

Защита программного обеспечения от незаконного распространения и модификации является одной из главных задач компьютерной безопасности. Для достижения поставленных целей используется множество различных методов и приёмов, включающих использование политик безопасности, сетевых фильтров, криптографических систем, специального аппаратного обеспечения, предотвращающего незаконное распространение программного обеспечения, и т.д. Но насколько бы ни были сильны такие методы они не защищают от того, что злоумышленник, получив доступ к коду программы, может понять принцип её работы, изучить используемые в ней алгоритмы и структуры данных.

Впервые задача запутывания была упомянута в работе Уитфилда Диффи и Мартина Хеллмана «Новые направления в криптографии». В ней предложено использовать для построения ассиметричной криптосистемы сложность задачи, заключающейся в анализе программ на низкоуровневом языке программирования (ассемблер, байт-код). В настоящей работе рассматривается возможность преобразования симметричных криптосистем в ассиметричные с помощью запутывающих преобразований.

Данное направление позволяет из симметричного алгоритма шифрования и применения запутывающих преобразований получить ассиметричный алгоритм шифрования. Достигается это следующим образом: берётся конкретный алгоритм шифрования и фиксируется ключ, затем к полученному алгоритму шифрования с фиксированным ключом применяются запутывающие преобразования, так чтобы извлечение ключевой информации из получившегося запутанного алгоритма было вычислительно трудно. Таким образом, получается открытый ключ, который абоненты могут использовать для связи, шифруя с помощью него сообщения. Преобразование симметричных криптографических систем, в ассиметричные позволяет получить определённые выгоды:

- маленький размер закрытого ключа,
- быстрая скорость шифрования/расшифрования.

Данное направление наиболее востребовано в электронных ключах для защиты программного обеспечения от незаконного распространения. Программное обеспечение, работающее в электронном ключе, существенно ограничено в аппаратных и временных ресурсах, исходя из небольшого количества памяти и относительно низкой скорости работы процессора (микроконтроллера).

Для того чтобы оценивать стойкость и качество запутывающих преобразований необходимо ввести формальное определение запутывания. В работе [1] впервые введено определение запутывающих преобразований в терминах машины Тьюринга. Вероятностный алгоритм O называется запутывающим машину Тьюринга M, если выполнены следующие условия:

- для любой машины Тьюринга M строка O(M) описывает ту же машину Тьюринга,
- длина строки, описывающей машину Тьюринга O(M) и её время работы полиномиально зависят от длины строки описывающей машину Тьюринга M и её времени работы соответственно,
- любой другой алгоритм, получающий на вход строку, описывающую машину Тьюринга O(M), за полиномиальное время получит информации о её работе не более, чем было бы получено информации о работе машины Тьюринга M в результате её анализа по принципу «чёрный ящик».

В этой же работе получен результат, опровергающий существование универсальных запутывающих преобразований, соответствующих вышеприведённому определению. Однако такой факт не опровергает существование запутывающих преобразований для определённого класса алгоритмов.

В работе [2], доказывается существование запутывающих преобразований для алгоритмов, вычисляющих функции типа «точка». На их примере продемонстрировано, запутывание схемы проверки пароля. Таким образом, получен класс программ, к которым применимы запутывающие преобразования.

Функция $f_\alpha(x)$ называется функцией типа «точка», если

$$f_\alpha(x) = \begin{cases} 1, \text{ если } x = \alpha, \\ 0, \text{ в противном случае} \end{cases}$$

В работах [3], [4] так же вводятся определения запутывающих преобразований, более слабые, чем в работе [1], с целью формализации оценки стойкости полученных криптографических конструкций. В частности определение запутывающих преобразований, приведённое в [3], так же не допускает существование универсальных запутывающих алгоритмов, однако не опровергается существование запутывающих преобразований для определенных классов алгоритмов: симметричные схемы шифрования.

В работе [5] приводится метод, предназначенный для запутывания симметричных блочных шифров, построенных с использованием петли Фейстеля. Достигается это путём введения перемешивающих биективных преобразований и интеграции цикловых ключей с S-боксами в соответствующем раунде.

В настоящей работе рассмотрены подходы к криптоанализу запутанного алгоритма шифрования DES. В результате приведённых атак появляется возможность извлечения из запутанного алгоритма секретного ключа и перемешивающих биективных преобразований. Данные методы криптоанализа реализуемы исходя из устройства шифра DES. Так же в данной работе рассматривается возможность применения подобных атак к запутанному алгоритму ГОСТ 28147-89.

В настоящей работе была предпринята попытка систематизации предыдущих результатов и создания ассиметричных криптосистем на базе симметричных с помощью запутывающих преобразований. Существует возможность создания действительно стойких криптосистем подобного вида. Данная тема имеет довольно перспективные направления дальнейшего развития: разработка запутывающих преобразование к симметричным шифрам другого вида (например, AES) и разработка блочных шифров специального вида, стойких к попыткам криптоанализа, приведённым в настоящей работе.

Список используемой литературы

1. On the (Im)possibility of Obfuscating Programs, B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, K. Yang
2. Positive results and techniques for obfuscation, B. Lynn, M. Prabhakaran, and A. Sahai
3. Obfuscation for Cryptographic Purposes, Dennis Hofheinz, John Malone-Lee, and Martijn Stam
4. On the Possibility of Provably Secure Obfuscating Programs, Nikolay P. Varnovsky and Vladimir A. Zakharov.
5. A White-Box DES Implementation for DRM Applications, S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot.