Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 004.056.55

РАЗРАБОТКА МЕТОДИКИ ОЦЕНКИ ЗАВИСИМОСТИ КРИПТОСТОЙКОСТИ АЛГОРИТМА ГОСТ 28147-89 ОТ ВЫБРАННОЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

В. Ю. Золотухин, Т. А. Чалкин

Каждая операция преобразования n бит в рамках процедуры шифрования может быть представлена в виде набора из n булевых функций от n переменных. Анализируя характеристики этих функций, можно судить об особенностях процесса шифрования при данных конкретных значениях ключевой информации, так как вид функций будет меняться в зависимости от ключа (и таблицы замен — в случае шифра ГОСТ 28147-89).

На сегодняшний день наиболее эффективными и хорошо изученными методами криптоанализа являются линейный и дифференциальный криптоанализ. Линейный метод заключается в построении линейной аппроксимации преобразования бит, выполняемого в ходе шифрования. Дифференциальный криптоанализ состоит в изучении процесса изменения различий для пары открытых текстов, имеющих определенные исходные различия в нескольких битах, в процессе прохождения через раунды процесса шифрования.

Для достижения высокого уровня стойкости шифра к линейному и дифференциальному криптоанализу необходимо, чтобы булевы функции, составляющие преобразование бит, соответствующее процедуре шифрования, обладали высокими показателями нелинейности (то есть были далеки в смысле расстояния Хэмминга от множества аффинных булевых функций) и лавинного эффекта (для любого изменения значений входных переменных функции выходное значение должно меняться с вероятностью 1/2, причем «непредсказуемым» образом, если рассматривать функцию как «черный ящик»). Количественными характеристиками, отражающими устойчивость шифрования к линейному и дифференциальному методам криптоанализа, являются нелинейность и динамическое расстояние [1, 2].

При рассмотрении раунда шифрования алгоритма ГОСТ 28147-89 видно, что нелинейность и лавинный эффект обеспечиваются операциями сложения полублока данных с подключом раунда и замены бит по таблице, поскольку операции циклического сдвига и побитового сложения с левым полублоком являются линейными и не несут лавинного эффекта. В работе [3] описан алгоритм построения узлов замен алгоритма ГОСТ 28147-89, отвечающих требованиям устойчивости к линейному и дифференциальному криптоанализу, определяемой по значениям количественных характеристик нелинейности и динамического расстояния для отдельных узлов.

Но так как криптостойкость шифрования (в смысле потенциальной устойчивости к линейному и дифференциальному методам криптоанализа) обеспечивается еще и характеристиками ключа, то возникает задача нахождения оценки влияния выбранного ключа на нелинейность преобразования бит. Если анализировать раунд шифрования

в целом, то нелинейность раунда можно оценивать как нелинейность композиции преобразований сложения с подключом раунда и замены бит по таблице.

В ходе работы по данному направлению путем эмпирических исследований были получены результаты, свидетельствующие о том, что в зависимости от выбранного ключа в рамках одного раунда шифрования показатели нелинейности и динамического расстояния преобразования бит по таблице замен могут как увеличиваться, так и уменьшаться.

В настоящее время при построении криптосистем на основе шифра ГОСТ 28147-89 практикуется независимый выбор ключа и таблицы замен. Так как исследования взаимного влияния характеристик криптостойкости ключа и таблицы замен показали как возможное усиление параметров криптостойкости, так и их ослабление (в рамках раунда), то можно сделать вывод о том, что для каждой таблицы замен существуют непересекающиеся множества подключей, которые:

1) улучшают показатели криптостойкости (нелинейность и динамическое расстояние) в рамках раунда;
2) ухудшают параметры криптостойкости;
3) не изменяют параметры криптостойкости.

В силу того, что в алгоритме ГОСТ 28147-89 подключи раундов используются независимо, а таблица замен в каждом раунде используется одна и та же, результаты, полученные для отдельного раунда, легко переносятся на весь процесс шифрования в целом, если известны закономерности соотношения между нелинейностью и динамическим расстоянием двух преобразований бит и аналогичными параметрами их композиции.

Для повышения криптостойкости шифрования по алгоритму ГОСТ 28147-89 предлагаемая методика предполагает формирование ключевой информации для шифрования таким образом, чтобы таблица замен и ключ шифрования максимально усиливали влияние друг друга на криптостойкость шифрования в большинстве раундов.

ЛИТЕРАТУРА

1. *Столлингс В.* Криптография и защита сетей: принципы и практика М.: Издательский дом «Вильямс», 2001.
2. *Mister S., Adams C.* Practical S-box design // Proc. Workshop in selected areas in cryptography. Queen's University, Kingston, Ontario, 1996.
3. *Чалкин Т. А., Волощук К. М.* Алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147-89 // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнева. 2009. Вып. 1(22). Ч. 2. С. 46–50.

УДК 519.7

О СОКРАЩЕНИИ КЛЮЧЕВОГО ПРОСТРАНСТВА ПОТОЧНОГО ШИФРА A5/1 ПРИ ТАКТИРОВАНИИ[1]

С. А. Киселев

Рассмотрим генератор псевдослучайной последовательности (гаммы), состоящий из k регистров с обратной связью. *Состоянием генератора* будем называть булев век-

[1]Исследование выполнено при поддержке гранта Президента РФ для молодых российских ученых (грант МК № 1250.2009.1).