УДК 681.3.06:519.248.681

# МЕТОД НЕДЕТЕРМИНИРОВАННОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ КОМБИНИРОВАНИЯ РАЗНОТИПНЫХ ЦИКЛОВЫХ ФУНКЦИЙ

С.А. Сидченко
(Харьковский университет Воздушных Сил им. И. Кожедуба)

*В статье предложен программно-ориентированный метод недетерминированного преобразования на основе комбинирования нескольких разнотипных цикловых функций с возможностью построения большого количества модификаций преобразования.*

***недетерминированное преобразование, комбинирование, разнотипные цикловые функции***

**Постановка проблемы.** Настоящий момент времени характеризуется ускоренными темпами создания и развития информационных систем. Информация, циркулирующая в этих системах, все чаще рассматривается, как стратегический ресурс государства (предприятия, банка и т.п.). По этому поводу существует высказывание “кто владеет информацией, тот владеет ситуацией”. Наряду с ростом значимости информации растет и число преступлений, связанных с ее хищением. В связи с этим все более остро встают вопросы информационной безопасности государства.

Одним из важных приоритетов в обеспечении информационной безопасности является “створення засобів захисту від несанкціонованого доступу до інформаційних ресурсів та від порушення нормального функціонування комп’ютерно-телекомунікаційних мереж” [1]. Большинство этих средств строится на основе специальных (криптографических) методов преобразования информации.

**Анализ литературы.** По мнению К. Шеннона [2], в практических шифрах (специальных преобразованиях информации) необходимо использовать два общих принципа: рассеивание и перемешивание.

Рассеивание представляет собой распространение влияния одного знака открытого текста на множество знаков преобразованного текста, что позволяет скрыть статистические свойства открытого текста.

Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текстов.

Шеннон выдвинул идею создания составного шифра, удовлетворя-

ющего принципам рассеивания и перемешивания, т.е. шифра, который может быть реализован в виде некоторой последовательности простых шифров, который вносит небольшой вклад в значительное суммарное рассеивание и перемешивание.

На основе этого принципа создано большое количество криптографических преобразований информации. Например, алгоритмы, представленные на конкурсы AES (http://www.nist.gov/aes) и NESIE (http://www.cryptonessie.com), алгоритм ГОСТ 28147-89 и др. Но большей частью эти преобразования являются детерминированными с заранее известной структурой (по правилу Керкгоффса).

В [3, 4 и др.] авторы предложили использовать управляемые операции (примитивы) для создания стойких недетерминированных криптографических преобразований.

**Цель статьи.** Предложить метод создания недетерминированного преобразования информации на основе комбинирования нескольких разнотипных цикловых функций.

**Изложение основного материала.** Пусть имеются две системы преобразования информации T и R (криптографические системы). В них, как правило, область определений (пространство сообщений) совпадает с областью значений (пространство криптограмм). Как отмечено в [2], для получения новой системы S их можно комбинировать двумя способами.

Первый способ состоит в образовании своего рода “взвешенной суммы”

$$S = pT + qR, \qquad (1)$$

где $p + q = 1$.

Эта операция состоит, во-первых, из предварительного выбора систем T или R с вероятностями p и q. Этот выбор является частью ключа S. После того как этот выбор сделан, системы T или R применяются в соответствии с их определениями. Полный ключ системы S должен указывать, какая из систем T или R выбрана и с каким ключом используется выбранная система

$$K_S = K_p \,||\, K_T \,||\, K_R,$$

где $K_S$ – ключ системы S; $K_p$ – ключ выбора системы T или R; $K_T$ – ключ системы T; $K_R$ – ключ системы R.

На практике для систем T и R, как правило, может использоваться один и тот же ключ преобразования.

Второй способ комбинирования двух секретных систем заключается в образовании “произведения”, т.е. сначала применяется система T к исходной информации, а затем система R к результату этой операции, что дает результирующую операцию S, которую запишем в виде произведения

$$S = TR. \qquad (2)$$

Умножение двух систем некоммутативно (т.е. не всегда $TR = RT$), хотя в частных случаях (подстановка и перестановка) коммутативность имеет место.

Ключ системы S состоит как из ключа системы T, так и из ключа системы R, причем предполагается, что эти ключи выбираются соответственно их первоначальным вероятностям и независимо.

$$K_S = K_T \,||\, K_R .$$

Однако на практике может быть и третий способ получения системы S, заключающийся в комбинировании способов (1) и (2):

$$S = pT + qR + kTR, \tag{3}$$

где $p + q + k = 1$.

Обобщая, можно представить систему S в виде комбинации нескольких m систем. Тогда (3) можно записать в виде

$$S = p_1 T + p_2 R + \ldots + p_{m-1} V + p_m M + p_{m+1} TR + \ldots + p_{m+\frac{m!}{2!(m-2)!}} VM + \ldots + \\ + p_{\sum\limits_{n=1}^{m} \frac{m!}{n!(m-n)!}} TR \ldots VM, \tag{4}$$

где $\sum\limits_{n=1}^{m} \frac{m!}{n!(m-n)!}$ $\sum\limits_{i=1} p_i = 1$ – вероятность выбора систем или их комбинаций; m – количество систем, из которых строится система S; T, R, …, V, M – исходные системы.

Для построения системы S в качестве “строительных блоков” можно использовать симметричные блочные преобразования и операции:

– операции командного процессора компьютера (поразрядное суммирование по модулю 2, суммирование и/или вычитание по модулю $2^{32}$ или $2^{64}$, поразрядного логического умножения и/или сложения, подстановки, циклического сдвига на фиксированное число двоичных разрядов или разрядов, зависящих от ключа или преобразуемых данных, и др.);

– операции перестановок (фиксированных и зависящих от ключа или преобразуемых данных);

– специальные преобразования информации и цикловые функции известных криптограических преобразований (алгоритмы, представленные на конкурсы AES и NESIE, алгоритм ГОСТ 28147-89 и многие другие).

Стоит отметить, что для реализации (4) необходимо выбрать одну из архитектур сети Фейстеля и учесть одним из показателей стойкости криптографического преобразования, которым является лавинный эффект – число циклов шифрования, начиная с которого обеспечивается влияние любого входного бита на каждый выходной бит.

В качестве примера рассмотрим распространение лавинного эффекта в цикловой функции преобразования ГОСТ 28147-89 (рис. 1). Предположим, что во входном 64-битном блоке изменен первый бит. Первой операцией шифрования является сложение по модулю $2^{32}$ (перенос из старших разрядов в младшие), что приведет к изменению не более 5 битов суммы [5]. После выполнения замены в 4-битовых группах изменение распространится на 8 бит (две смежные 4-битовые группы). Циклический сдвиг влево на 11 бит не изменяет биты, а изменяет их положение в блоке. Это приводит к распределению 8 бит (измененных) по трем смежным 4-битовым группам. На рисунке каждый прямоугольник соответствует 4-битовой группе, затронутые изменением биты выделены серым цветом.

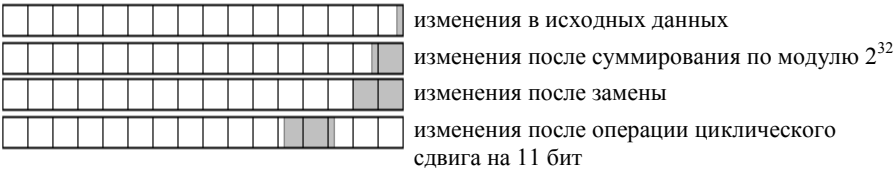


Рис. 1. Лавинный эффект в исходных данных через операции цикловой функции преобразования ГОСТ 28147-89

Из примера видно, что изменение одного бита исходного блока распространится на один байт преобразованного блока информации. Поэтому для организации лавинного эффекта после каждой цикловой функции или в ее окончании необходимо учесть использование управляемых или неуправляемых операций перестановки или циклического сдвига. В цикловой функции преобразования ГОСТ 28147-89 это функция циклического сдвига на 11 бит влево.

В силу того, что современные компьютеры начинают строиться на 64-битной архитектуре и для повышения стойкости к атаке “по подобранному преобразованному тексту” необходимо использовать цикловые функции с размером блока преобразования 128 бит (размер полублока равен 64 битам).

Исходя из (4) и приведенных выше предположений можно предложить следующую схему недетерминированного преобразования информации на основе комбинирования разнотипных цикловых функций, представленную на рис. 2.

На схеме используются следующие обозначения: k (256 бит) – ключ инициализации алгоритма преобразования и формирования раундовых ключей K; K (1024 бит) – ключ преобразования, состоящий из раундовых ключей: K = K1||K2||…||K16; F1, F2,…, F8 – цикловые функции одного раунда преобразования; P – операция перестановки бит; TV – тестовый вектор; E – функция преобразования информации.

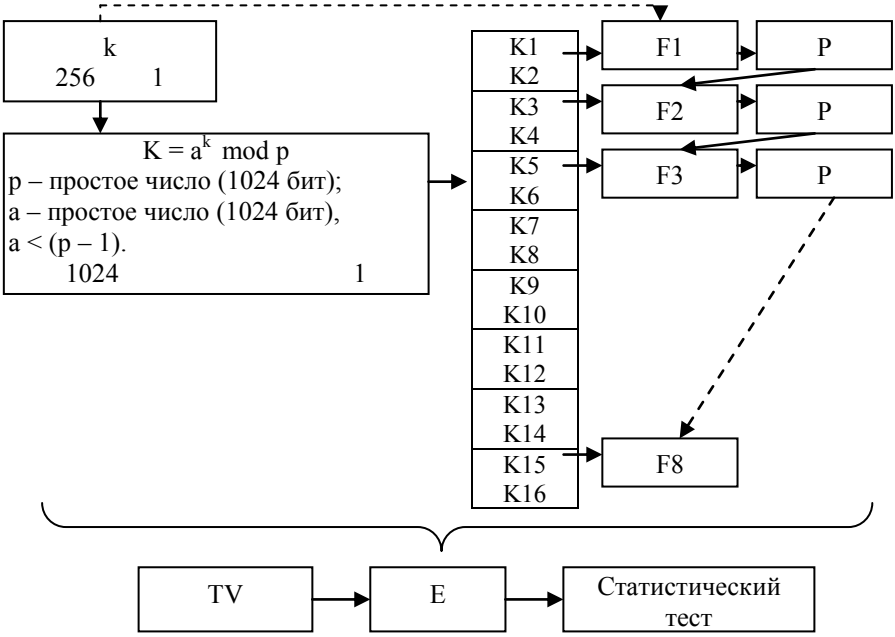


Рис. 2. Схема недетерминированного преобразования информации на основе комбинирования разнотипных цикловых функций

Схема преобразования состоит из двух частей. Первая заключается в формировании алгоритма преобразования на основе секретного ключа k для инициализации алгоритма преобразования. Цикловые функции выбираются по формуле

$$F_r = k_r \bmod m,$$

где $k = k_1 || k_2 || ... || k_8$; m – количество базовых цикловых функций, участвующих в формировании алгоритма; r – номер раунда преобразования.

Всего схема предусматривает следующее количество возможных реализаций: m! – при использовании всех цикловых функций в преобразовании; $m(m-1)...(n-m)$ – при использовании в преобразовании $n\ (n < m)$ цикловых функций из m.

На первом этапе формируется также и ключ преобразования K из ключа инициализации k по формуле

$$K = a^k \bmod p,$$

где p – простое число (1024 бит); a – простое число (1024 бит), a < (p – 1).

На втором этапе производится непосредственно преобразование

информации. Открытые данные подлежащие преобразованию, разбивают на 128-разрядные блоки и подаются на преобразование через все раунды. В схеме предлагается 8 раундов, это связано с использованием 1024 битов ключа. Хотя количество раундов может быть увеличено за счет применения другой схемы формирования или использования ключа (например, расширенный ключ K применяется по ключевому расписанию ГОСТ 28147-89, что приведет к увеличению количества раундов до 32). Каждый раунд состоит из двух подраундов, на которых 128-и битный блок преобразуется по 64 бита на каждом из подраундов.

После прохода через цикловую функцию блок подается на операцию перестановки. В качестве этой операции может выступать операция циклического сдвига влево на число бит, зависящих от преобразуемых данных.

Для проверки статистических характеристик алгоритма преобразования может проводиться тестовый прогон с использованием тестового вектора TV.

Обратное преобразование проводится в обратном порядке.

**Выводы.** Предложен программно-ориентированный недетерминированный метод преобразования информации на основе комбинирования нескольких разнотипных цикловых функций, в котором используется подсистема настройки для каждого пользователя, в зависимости от ключа доступа (ключа преобразования). Он обладает возможностью построения большого количества модификаций преобразования и обладает практически абсолютной стойкостью к известным атакам.

## ЛИТЕРАТУРА


1. *Толубко В.Б., Жук С.Я., Косевцов В.О. Концептуальні основи інформаційної безпеки України // Наука і оборона – 2004. – №2. – С. 19-25.*
2. *Шеннон К.Э. Теория связи в секретных системах // В кн. Шеннон К.Э. Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – С. 333-402.*
3. *Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 496 с.*
4. *Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004. – 448 с.*
5. *Винокуров А., Применко Э. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США. «Системы безопасности». – М.: «Гротэк», 2001. – №№ 1, 2.*



*Поступила 20.06.2006*

**Рецензент:** доктор технических наук, профессор И.Д. Горбенко,
Харьковский национальный университет радиоэлектроники.