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).

тор $x = (x_1, \ldots, x_n)$, составленный из состояний регистров, где $n = \sum_{i=1}^{k} l_i$, l_i — длина i-го регистра. *Функцией управления сдвигом* назовем векторную булеву функцию $c : \mathbb{Z}_2^n \to \mathbb{Z}_2^k$, $c(x) = (y_1, ..., y_k)$, такую, что при следующем такте i-й регистр сдвигается тогда и только тогда, когда $y_i = 1$. *Функцией следующего состояния* называется векторная булева функция $next : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, которая в соответствии с функцией управления сдвигом и функциями обратной связи регистров определяет следующее состояние: $next(x) = x'$. *Вырожденным состоянием* назовем такое состояние, у которого как минимум в одном регистре все значения одинаковы. Будем говорить, что функция управления сдвигом *обратима*, если по любому невырожденному состоянию $next(x)$ можно восстановить вектор $c(x)$ однозначно. Доказан следующий факт.

Теорема 1. Пусть функции обратной связи всех регистров генератора обратимы по последней переменной. Тогда функция следующего состояния обратима тогда и только тогда, когда обратима функция управления сдвигом.

A5/1 [1] — это поточный алгоритм шифрования, используемый для обеспечения конфиденциальности передаваемых данных между телефоном и базовой станцией в европейской системе мобильной цифровой связи GSM (Group Special Mobile).

Утверждение 1. Функция управления сдвигом в генераторе A5/1 необратима.

Из утверждения 1 и теоремы 1 следует, что функция $next$ в A5/1 необратима, а значит, существуют состояния, в которые нельзя перейти. *t-Простым* состоянием назовем такое состояние, которое получено совершением t тактов, начиная с состояния без предшественника, причем такое t минимально. Количество t-простых состояний обозначим N_t.

Теорема 2. Количества t-простых состояний в A5/1 для $t = 0, 1, 2, 3$ равны $3 \cdot 2^{61}$, $13 \cdot 2^{58}$, $334 \cdot 2^{53}$ и $2792 \cdot 2^{49}$ соответственно.

Заметим, что сумма чисел N_0, N_1, N_2, N_3 составляет довольно большую долю в количестве всех состояний ключевого пространства шифра A5/1 — больше девяти десятых. Наглядней этот результат можно увидеть в таблице ниже (первая строка — число сделанных тактов, вторая — доля оставшегося числа состояний в ключевом пространстве).

Число тактов	0	1	2	3	4
Ключевое пространство, %	100	62,5	42,2	25,9	15

Полученные результаты можно использовать следующим образом. Пусть есть некое состояние, с которого мы начинаем перехват генерируемой гаммы. Можно пропустить T битов гаммы для того, чтобы отсечь большую долю состояний, которые не могли получиться в процессе тактирования. Таким образом, при совершении T тактов можно отбросить все 0, 1, ..., $(T-1)$-простые состояния. Нахождение такого T, при котором откинутое число знаков гаммы будет как можно меньше, а отброшенная доля ключевого пространства достаточно большой, уменьшит трудоемкость криптоанализа.

Стоит отметить, что наблюдается экспоненциальное сокращение ключевого пространства с каждым пропущенным битом гаммы, т. е. при каждом отбрасывании бита гаммы ключевое пространство сокращается почти в 2 раза.

К сожалению, с каждым следующим тактом значительно увеличивается сложность подсчета числа t-простых состояний, и уже для 3-простых состояний подсчет их доли занял около 100 мин работы суперкомпьютера SMP16x256 (использовалось 4 ядра).

ЛИТЕРАТУРА

1. *Biryukov A., Shamir A.* Real Time Cryptanalysis of the Alleged A5/1 on a PC // Preproc. FSE' 7. 2000. P. 1–18.

УДК 004.056.55

АППАРАТНАЯ РЕАЛИЗАЦИЯ ШИФРСИСТЕМЫ, ОСНОВАННОЙ НА АВТОМАТЕ ЗАКРЕВСКОГО[1]

А. В. Милошенко

На сегодняшний день встречается мало примеров использования конечных автоматов в качестве аппаратных шифраторов. Разработан прототип шифрсистемы, построенной на базе автомата Закревского [1] с заданными свойствами, в виде программно-аппаратного комплекса. Программная часть комплекса включает в себя генератор шифрующих автоматов и генератор ключей (подмножество переходов автомата), а также транслятор с табличного задания абстрактного автомата на язык описания аппаратуры VHDL. Аппаратную часть комплекса составляет ПЛИС (программируемая логическая интегральная схема), программирование которой осуществляется с помощью САПР Xilinx ISE. В ходе экспериментов выявлен оптимальный способ кодирования состояний автомата.

Для описания автоматной шифрсистемы потребуются следующие определения.

Определение 1. Конечным автоматом A называется пятерка (S, X, Y, ψ, φ), где S — конечное непустое множество состояний; X и Y — конечные входной и выходной алфавиты соответственно, причем далее считается, что $|X| = |Y|$; $\psi : S \times X \to S$ и $\varphi : S \times X \to Y$ — функции переходов и выходов соответственно.

Определение 2. Автомат A является автоматом с биективной функцией выходов, если для любого $s \in S$ функция $\varphi_s(x) = \varphi(s, x)$ определяет взаимно однозначное отображение X на Y. Автоматом Закревского будем называть сильносвязный конечный автомат с биективной функцией выходов.

Если функции ψ и φ определены для всех пар $(s, x) \in S \times X$, то автомат A называется полностью определенным, иначе частичным. Таким образом, полностью определенный автомат A при фиксированном состоянии s реализует отображение f_s множества входных слов X^* на множество выходных слов Y^*. Известно [2], что для полностью определенного автомата A, реализующего $\{f_s : s \in S\}$, существует обратный автомат A^{-1}, который реализует $\{f_s^{-1} : s \in S\}$, если A есть автомат Закревского (АЗ).

Определение 3. Шифрсистема на базе АЗ — шифрсистема, в которой АЗ A используется для шифрования, а обратный автомат A^{-1} — для расшифрования. Считается, что у АЗ A функция переходов ψ является частичной. Произвольное доопределение функции ψ вместе с начальным состоянием являются ключом шифрсистемы.

Ясно, что количество возможных ключей шифрсистемы на базе АЗ равно $|S| \cdot |S|^n$, где n — количество пар (s, x), на которых функция ψ не определена.

Очевидно, что не все АЗ следует использовать в качестве шифратора. Определим требуемые свойства шифрующего автомата Закревского:

1) случайность — равномерное и случайное распределение значений функций ψ и φ;

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).