В. А. Орлов, В. А. Конявский

ОБЩЕАВТОМАТНОЕ ШИФРОВАНИЕ

В настоящее время криптографическую защиту информации осуществляют в основном с использованием ЭВМ. Как известно, на большинстве ЭВМ преобразования входной информации в выходную являются конечно-автоматными отображениями, которые более подробно описаны ниже. Отметим, что теория автоматов — достаточно развитый раздел дискретной математики.

Вырожденным классом конечных автоматов являются автоматы с *одним* состоянием. Эти автоматы реализуют так называемые *стационарные* отображения слов в конечных алфавитах (в каждый момент времени значение выходной буквы зависит только от значения входной буквы в тот же момент времени). Шифр простой замены является примером использования стационарных отображений. Отметим, что широко распространенная криптосистема с открытым ключом RSA также реализует стационарные отображения.

По данным известных авторам источников [1—6] в современной криптографии используется небольшое число классов конечных автоматов специального вида. При этом либо описание класса автоматов общедоступно (криптосистема DES и т. п.), либо конечные автоматы являются автономными (линейные и нелинейные регистры сдвига и др.), т. е. применяются для построения псевдослучайных последовательностей.

Задача о выявлении обратимости конечных автоматов известна давно. Например, в [7] отмечено, что задача обратимости клеточных автоматов не решена.

В работе получены необходимые и достаточные условия, при которых автоматную функцию можно использовать в качестве криптографического преобразования. При этом доступной информацией является *класс* криптоалгоритмов (конечно-автоматные функции); описание автоматной функции является секретным.

Конечный автомат — это имеющее вход и выход устройство, которое в каждый момент времени находится в одном из своих состояний. Конечный автомат осуществляет преобразование информации в дискретные моменты времени 0, 1, 2, …, t, … На вход автомата поступает последовательность символов входного алфавита $X = \{x_1, x_2, \ldots, x_n\}$; эту последовательность называют входным словом. Функционирование конечного автомата осуществляется в соответствии с системой из ns команд, где s — мощность алфавита состояний $Q = \{q_1, q_2, \ldots, q_s\}$. В каждый момент времени значением выхода автомата является элемент выходного алфавита $Y = \{y_1, y_2, \ldots, y_m\}$. Каждая команда имеет вид

$$x_i q_j \to y_k q_r\ ,$$

где x_i — входная буква, q_j — текущее состояние, y_k — выходная буква и q_r — состояние в следующий за текущим момент времени (следующее состояние).

Функционирование конечного автомата задают также кортежем

$$<X, X, Q, V, \rho>,$$

где $V\colon X \times Q \to Y$ (функция выхода),

$\rho\colon X \times Q \to$ (функция переходов).

Конечный автомат с определенным состоянием в начальный момент времени называется *инициальным автоматом*. В соответствии со своей системой команд инициальный автомат реализует автоматную функцию, которая произвольное входное слово в алфавите X преобразует в выходное слово в алфавите Y той же длины. Осуществляемое инициальным автоматом преобразование слов проиллюстрируем следующей таблицей:

время	0	1	2	3	…………	n	$n+1$
входная буква	$x^{(0)}$	$x^{(1)}$	$x^{(2)}$		…………	$x^{(n)}$	

состояние	$q^{(0)}$	$q^{(1)}$	$q^{(2)}$	$q^{(3)}$	....	$q^{(n)}$	$q^{(n+1)}$
выходная буква	$y^{(0)}$	$y^{(1)}$	$y^{(2)}$		....	$y^{(n)}$	

Здесь и далее через $x^{(j)}$ ($y^{(j)}$) обозначаем j-ю букву входного (выходного) слова, а через $q^{(j)}$ — состояние автомата в момент времени j (при заданном входном слове).

По букве входного слова и состоянию, используя функции выхода и переходов, находим букву выходного слова в тот же момент времени и состояние в следующий момент.

Если функции выхода и переходов задать двумерными массивами, то описанное преобразование легко реализовать очень простым устройством, основная сложность которого заключается в организации хранения и выборки информации об этих функциях. Кроме того, преобразование осуществляется с максимальным быстродействием.

Как известно, применяемые при шифровании и расшифровывании преобразования должны быть взаимно однозначными.

Конечный автомат M назовем обратимым (ОК-автоматом), если существует конечный автомат M_1, такой, что по описанию автомата M, его начальному состоянию и произвольному выходному слову автомата M автомат M_1 однозначно определяет входное слово. В этом случае автомат M_1 будем обозначать через M^{-1}. Таким образом, в качестве криптографических преобразований можно использовать только автоматные функции, соответствующие ОК-автоматам.

Для простоты изложения будем рассматривать конечные автоматы, у которых входной и выходной алфавиты совпадают. Такие автоматы, у которых мощность входного алфавита (алфавита состояний) равна n (равна s), будем называть $(n,\ s)$-автоматами.

Пусть $V_j(x)$, $1 \le j \le s$, — функция $V(x,\ q_j)$. Нетрудно проверить, что необходимым условием того, что автомат M — это ОК-автомат, является инъективность функций $V_j(x)$ для любого j. Функция $f(x)$ инъективна, если из неравенства $x_i \ne x_j$ следует неравенство $f(x_i) \ne f(x_j)$. В нашем случае (совпадение входного и выходного алфавитов) утверждение об инъективности функции $V_j(x)$ эквивалентно утверждению о том, что она является перестановкой.

Справедливо следующее утверждение.

Теорема. *Автомат $M=\langle X,\ Y,\ Q,\ V,\ P\rangle$ является обратимым тогда и только тогда, когда для любого j функция $V_j(x)$ инъективна.*

Известно, что число $(n,\ s)$-автоматов не превосходит n^{ns}. Нетрудно проверить, что число $(n,\ s)$-автоматов, являющихся ОК-автоматами, имеет оценку $(n!)^s$. Отметим, что имеет место следующая (асимптотическая) формула Стирлинга

$$n! \ \sim\ \sqrt{2\pi n}\,\frac{n^n}{e^n}.$$

Таким образом, доля ОК-автоматов стремится к 0 при увеличении значений параметров автомата n и s. Однако ОК-автоматы образуют достаточно мощный класс.

При использовании ОК-автоматов в криптографии ключи шифрования определяют описания (таблицы) функций $V(x,\ q)$ и $P(x,\ q)$.

Получение описаний функций $V^{-1}(x,\ q)$ и $P^{-1}(x,\ q)$ обратного автомата по описаниям функций $V(x,\ q)$ и $P(x,\ q)$ является эффективной процедурой. Следовательно, общеавтоматное шифрование является симметричным.

Задача криптоанализа общеавтоматного шифрования — восстановление описания конечного автомата (нахождение функций $V(x,\ q)$ и $P(x,\ q)$) по наблюдению входных и выходных слов. Такие работы велись давно (см., например: [8]). Из них следует, что при надлежащем выборе ключей общеавтоматное шифрование обладает достаточной криптостойкостью.

В заключение предлагаем использовать ОК-автоматы в качестве стандарта поточного шифрования.

СПИСОК ЛИТЕРАТУРЫ:

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии: Учебное пособие. М.: Гелиос АРВ, 2005.
2. Введение в криптографию / Под общ. ред. В. В. Ященко. М.: МЦНМО, «ЧеРо», 1998. — 272 с.
3. *Саймон Сингх.* Книга кодов. М.: АСТ: Астрель, 2007. — 447 с.
4. *Смарт Н.* Криптография. М.: Техносфера, 2005. — 528 с.
5. *Коблиц Н.* Курс теории чисел и криптографии. М.: ТВП, 2001. — 254 с.
6. *Фергюсон Н., Шнайер Б.* Практическая криптография. М.: Вильямс, 2005. — 424 с.
7. *Евсютин О. О., Росошек С. К.* Шифр на основе обратимых клеточных автоматов на разбиении // Безопасность информационных технологий. 2007. № 4. С. 27–31.
8. *Трахтенброт Б. А., Барздинь Я. М.* Конечные автоматы (поведение и синтез). М.: Наука, 1970.