Математические структуры и моделирование
2008, вып. 18, с. 102–107

УДК 003.26:519.713

ШИФРЫ ЗАМЕНЫ КАК ПРИМЕРЫ ДИСКРЕТНЫХ АВТОМАТОВ

Н.Ф. Богаченко

В статье обсуждается криптографический подход к изложению основных моделей теории автоматов. Представлены шифры замены, допускающие реализацию в виде комбинационных и последовательных автоматов.

Классическая теория автоматов представляет собой математический аппарат, предназначенный, в первую очередь, для синтеза (построения логических схем) дискретных устройств. Вместе с тем автоматные модели используются и в других областях, в частности в микропрограммировании, при построении трансляторов и т.д.

Государственный образовательный стандарт высшего профессионального образования для специальности 075200 – «Компьютерная безопасность» включает в дисциплину «Дискретная математика» раздел, посвященный теории автоматов. Это обусловлено тем, что теоретико-автоматные модели находят применение и в сфере обеспечения информационной безопасности. В частности, абстрактная модель шифратора может быть представлена в терминах автоматов с памятью [2, 3], понятие детерминированного конечного автомата используется при построении моделей безопасности компьютерных систем [5]. Исходя из вышесказанного, преподавание теории автоматов при подготовке специалистов в области информационной безопасности должно включать в себя не только «инженерную» составляющую, но и «привязку» к классическим моделям криптографии. Данная статья демонстрирует пример такой интеграции.

Еще одна причина привлечения аппарата теории автоматов к построению шифров заключается в том, что большинство современных криптосистем базируется на теоретико-числовых моделях. Представляет интерес исследование других подходов к разработке и анализу алгоритмов шифрования.

1. Дискретные автоматы

Дискретный автомат – это математическая модель дискретного устройства, представленная в терминах входных, выходных и внутренних дискретных переменных. Дискретные автоматы подразделяются на два класса: автоматы без памяти (комбинационные) и автоматы с памятью (последовательные).

Омский государственный университет.
E-mail: nfbogachenko@mail.ru

Если входные сигналы обозначить $x_1, \ldots, x_n$, а выходные – $y_1, \ldots, y_m$, то функциональная модель комбинационного автомата представляется в следующем виде:

$$\begin{cases} y_1 = y_1(x_1, \ldots, x_n), \\ \vdots \\ y_m = y_m(x_1, \ldots, x_n). \end{cases} \tag{1}$$

В отличие от комбинационного, последовательный автомат наделен множеством внутренних состояний. Пусть текущее состояние последовательного автомата определяется значениями переменных $\tau_1, \ldots, \tau_k$, тогда его функциональная модель имеет вид:

$$\begin{cases} y_1 = y_1(x_1, \ldots, x_n, \tau_1, \ldots, \tau_k), \\ \vdots \\ y_m = y_m(x_1, \ldots, x_n, \tau_1, \ldots, \tau_k), \\ \varphi_1 = \varphi_1(x_1, \ldots, x_n, \tau_1, \ldots, \tau_k), \\ \vdots \\ \varphi_k = \varphi_k(x_1, \ldots, x_n, \tau_1, \ldots, \tau_k). \end{cases} \tag{2}$$

Здесь $\varphi_1, \ldots, \varphi_k$ – функции возбуждения памяти, отвечающие за смену внутреннего состояния автомата. Последовательный автомат, определенный системой (2), называется автоматом Мили [1, 4].

На рисунке 1 представлены структурные схемы комбинационного и последовательного автоматов.

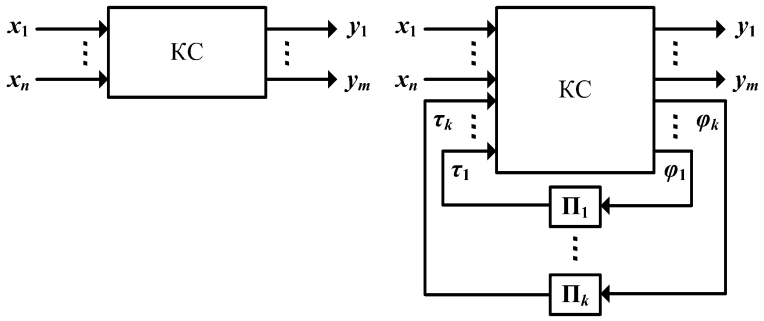

Рис. 1. Структурные схемы комбинационного (слева) и последовательного (справа) автоматов; КС – комбинационная схема (состоит из логических элементов и не имеет контуров); $\Pi_1, \ldots, \Pi_k$ – элементы памяти

В рамках поставленной перед нами задачи – установить взаимосвязь между теоретико-автоматными моделями и алгоритмами шифрования – представляется целесообразным в качестве примеров комбинационных и последовательных автоматов рассматривать аппаратную реализацию шифров простой и многозначной замены. В такой постановке задача построения криптосистемы разбивается на две части: синтез шифратора и дешифратора.

2. Блок подстановок как комбинационный автомат

Пусть необходимо продемонстрировать процесс синтеза комбинационного автомата. Представляется возможным в качестве модельной задачи рассмотреть шифр замены, а именно блок подстановок.

Для простоты будем шифровать последовательности из трех бит. Допустим, необходимо реализовать подстановку, заданную таблицей 1. Данную подстанов-

Таблица 1. Шифр замены или таблица выходов комбинационного автомата S_1

Вход	000	001	010	011	100	101	110	111
Выход	010	111	100	110	001	000	101	011

ку можно интерпретировать как таблицу выходов некоторого комбинационного автомата S_1, функциональная модель которого в этом случае будет иметь следующий вид [4]:

$$\begin{cases} y_1 = \overline{x}_1\overline{x}_2x_3 \vee \overline{x}_1x_2\overline{x}_3 \vee \overline{x}_1x_2x_3 \vee x_1x_2\overline{x}_3, \\ y_2 = \overline{x}_1\overline{x}_2\overline{x}_3 \vee \overline{x}_1\overline{x}_2x_3 \vee \overline{x}_1x_2x_3 \vee x_1x_2x_3, \\ y_3 = \overline{x}_1\overline{x}_2x_3 \vee x_1\overline{x}_2\overline{x}_3 \vee x_1x_2\overline{x}_3 \vee x_1x_2x_3. \end{cases} \tag{3}$$

После минимизации система (3) преобразуется в уравнения:

$$\begin{cases} y_1 = \overline{x}_1x_3 \vee x_2\overline{x}_3, \\ y_2 = \overline{x}_1\overline{x}_2 \vee x_2x_3, \\ y_3 = \overline{x}_1\overline{x}_2x_3 \vee x_1\overline{x}_3 \vee x_1x_2. \end{cases} \tag{4}$$

Наконец, на рисунке 2 представлена логическая схема шифратора S_1.

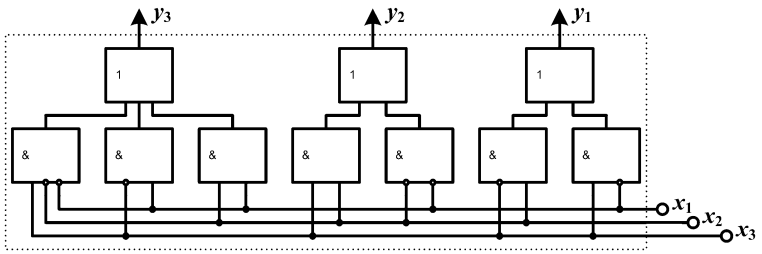

Рис. 2. Логическая схема комбинационного автомата S_1, реализующего блок подстановок

Синтез обратного автомата – дешифратора – аналогичен. Достаточно в таблице 1 строки «вход» и «выход» поменять местами и повторить приведенные выше расчеты.

3. Шифр многозначной замены как автомат Мили

Перейдем теперь к автоматам с памятью. В качестве примера вновь обратимся к шифру замены. Рассмотренная криптосистема является очень слабой: частотные характеристики открытого сообщения сохраняются и в криптотексте.

Повысить криптостойкость позволяют шифры многозначной замены, в которых каждому символу (кодовой комбинации) открытого алфавита ставится в соответствие не один, а несколько символов шифра.

Преобразуем подстановку из таблицы 1 в шифр многозначной замены (см. табл. 2).

Таблица 2. Шифр многозначной замены или таблица выходов автомата Мили S_2

	Входные сигналы							
	000	001	010	011	100	101	110	111
00	010	111	100	110	001	000	101	011
01	011	010	000	101	110	111	001	100
10	110	100	001	111	010	011	000	101
Состояния	Выходные сигналы							

Главная трудность, которая возникает при использовании шифров многозначной замены, заключается в запоминании ключа. В общем случае требуется построить функцию-распределитель, задающую порядок выбора подстановок.

Можно предложить следующий подход к решению данной проблемы. Будем интерпретировать таблицу 2 как таблицу выходов некоторого последовательного автомата, точнее, автомата Мили, S_2. В этом случае необходимо определить и таблицу переходов [4]. Так как в нашем примере замена трехвариантная, то автомат должен иметь три состояния: $a_1 = 00$, $a_2 = 01$, $a_3 = 10$. Пусть переходы автомата заданы таблицей 3. Теперь для запуска алгоритма шифрования остается определить начальное состояние, с которого стартует автомат.

Таблица 3. Таблица переходов автомата Мили S_2

	Входные сигналы							
	000	001	010	011	100	101	110	111
00	01	00	10	00	01	01	10	00
01	10	10	00	10	00	01	00	10
10	00	01	01	01	01	00	10	01
Состояния	Состояния перехода							

Функциональная модель автомата S_2 представляется системой булевых функций, зависящих от пяти переменных:

$$\begin{cases} y_1 = y_1(x_1, x_2, x_3, \tau_1, \tau_2), \\ y_2 = y_2(x_1, x_2, x_3, \tau_1, \tau_2), \\ y_3 = y_3(x_1, x_2, x_3, \tau_1, \tau_2), \\ \varphi_1 = \varphi_1(x_1, x_2, x_3, \tau_1, \tau_2), \\ \varphi_2 = \varphi_2(x_1, x_2, x_3, \tau_1, \tau_2). \end{cases} \tag{5}$$

Функции выходов и функции возбуждения памяти строятся стандартным образом согласно каноническому методу структурного синтеза [1,4]. Если в качестве

элементов памяти выбрать элементы задержки, то после минимизации каноническая система уравнений автомата S_2 примет следующий вид[1]:

$$\begin{cases} y_1 = \overline{x}_1\overline{x}_2\tau_1\overline{\tau}_2 \vee \overline{x}_1x_3\overline{\tau}_2 \vee x_1\overline{x}_2\overline{\tau}_1\tau_2 \vee x_2\overline{x}_3\overline{\tau}_1\overline{\tau}_2 \vee x_2x_3\overline{\tau}_1\tau_2 \vee x_2x_3\tau_1\overline{\tau}_2, \\ y_2 = \overline{x}_1\overline{x}_2\overline{x}_3\overline{\tau}_2 \vee \overline{x}_1\overline{x}_2\overline{\tau}_1 \vee \overline{x}_1x_2x_3\overline{\tau}_2 \vee \overline{x}_2\overline{\tau}_1\tau_2 \vee x_1\overline{x}_2\tau_1\overline{\tau}_2 \vee x_2x_3\overline{\tau}_1\overline{\tau}_2, \\ y_3 = \overline{x}_1\overline{x}_2\overline{x}_3\overline{\tau}_1\tau_2 \vee \overline{x}_1\overline{x}_2x_3\overline{\tau}_1\overline{\tau}_2 \vee \overline{x}_1x_2x_3\overline{\tau}_1\tau_2 \vee \overline{x}_1x_2\tau_1\overline{\tau}_2 \vee x_1\overline{x}_2x_3\overline{\tau}_1\tau_2 \vee \\ \qquad x_1\overline{x}_3\overline{\tau}_1\overline{\tau}_2 \vee x_1x_2\overline{x}_3\overline{\tau}_1 \vee x_1x_2\overline{\tau}_1\overline{\tau}_2 \vee x_1x_3\tau_1\overline{\tau}_2, \\ \varphi_1 = \overline{x}_1\overline{x}_2\overline{\tau}_1\tau_2 \vee x_2\overline{x}_3\overline{\tau}_1\overline{\tau}_2 \vee x_1x_2\overline{x}_3\overline{\tau}_2 \vee x_2x_3\overline{\tau}_1\tau_2, \\ \varphi_2 = \overline{x}_1x_2\tau_1\overline{\tau}_2 \vee \overline{x}_1x_3\tau_1\overline{\tau}_2 \vee \overline{x}_2\overline{x}_3\overline{\tau}_1\overline{\tau}_2 \vee x_1\overline{x}_2\overline{x}_3\overline{\tau}_2 \vee x_1\overline{x}_2x_3\overline{\tau}_1 \vee x_2x_3\tau_1\overline{\tau}_2. \end{cases} \tag{6}$$

Структурная схема автомата S_2 представлена на рисунке 3. Последний этап

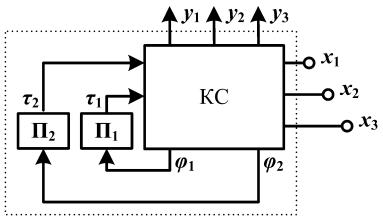

Рис. 3. Структурная схема автомата Мили S_2, реализующего шифр многозначной замены

синтеза – построение комбинационной части схемы (КС) по системе булевых функций (6) – не представляет сложности, но в силу громоздкости итоговой логической схемы будет опущен.

Отметим, что для однозначности расшифрования (для существования обратного автомата) необходимо и достаточно, чтобы в шифраторе в каждом наборе выходных сигналов, соответствующих одному состоянию, все значения были различны [3]. По таблице 2 несложно проверить, что это требование выполнено (в пределах одной строки кодовые комбинации не повторяются). Мы не будем подробно останавливаться на вопросах синтеза дешифратора. В работе [3] описан алгоритм построения таблиц обратного автомата, дальнейшие расчеты аналогичны.

Проверка правильности синтеза шифратора S и дешифратора S^{-1} сводится к последовательному применению их к некоторому открытому тексту α:

$$\alpha = S^{-1}(S(\alpha)). \tag{7}$$

4. Преимущества автоматной модели шифратора

Предложенная в работе криптографическая составляющая основных моделей теории автоматов помимо методического интереса дает инструмент для исследования алгоритмов шифрования.

[1]Для упрощения логических функций использовался программный пакет для моделирования электронных схем Electronics Workbench. В пакете реализован метод Квайна - Мак-Класски, позволяющий минимизировать булевы функции, заданные таблицей истинности или совершенной дизъюнктивной нормальной формой.

Представленный шифрующий автомат S_2 обладает всеми преимуществами шифров многозначной замены: одинаковые фрагменты входной последовательности в общем случае шифруются различными блоками. Например, кодовая комбинация «000» может быть зашифрована одним из трех способов: «010», «011» или «110», в зависимости от того, в каком состоянии находится автомат.

Пусть в качестве начального выбрано состояние $a_1 = 00$ и открытый текст представляет собой последовательность «000 000 101 010 000 000 100 000». Тогда шифротекст - это реакция автомата S_2 на данное входное слово (см. табл. 4). Как видно из примера, биграмма «000 000» шифруется по-разному: «010 011»

Таблица 4. Пример работы шифратора S_2

Открытый текст	000	000	101	010	000	000	100	000	
Состояния	00	01	10	00	10	00	01	00	01
Шифротекст	010	011	011	100	110	010	110	010	

или «110 010», а подпоследовательность «110 010» может быть шифротексом двух различных биграмм: «000 000» или «100 000».

Вопрос о более серьезном анализе шифра, построенного на основе последовательного автомата, выходит за рамки данной работы. Скорее всего, как и все шифры замены, он не сможет противостоять частотному анализу при шифровании больших сообщений на одном ключе (в нашем случае – на одном автомате). Представляется целесообразным использовать «автоматное» шифрование как одну из состовляющих какой-либо комбинированной (состоящей из нескольких процедур шифрования разных типов) криптосистемы.

Литература

1. Баранов С.И. Синтез микропрограммных автоматов. Ленинград: Энергия, 1974. 216 с.
2. Белов Е.Б., Зубов А.Ю., Погорелов Б.А., Проскурин Г.В., Черемушкин А.В., Шанкин Г.П., Шурупов А.Н. Криптографические методы защиты информации. Учебно-методическое пособие для курсов повышения квалификации преподавателей вузов учебно-методического объединения по образованию в области информационной безопасности. Часть 2. Москва. 2003.
3. Богаченко Н.Ф. Применение теоретико-автоматных моделей в криптографии // Математические структуры и моделирование. 2007. Омск: ООО «УниПак». Вып. 17. С. 112–120.
4. Богаченко Н.Ф., Файзуллин Р.Т. Синтез дискретных автоматов. Учебно-методическое пособие. Омск: Издательство Наследие. Диалог-Сибирь, 2006. 150 с.
5. Девянин П.Н. Модели безопасности компьютерных систем. М.: Издательский центр «Академия», 2005. 144 с.