2010 Математические методы криптографии №3(9)

DOI 10.17223/20710410/9/6

УДК 519.713; 004.056.55

РЕАЛИЗАЦИЯ ШИФРА ЗАКРЕВСКОГО НА ОСНОВЕ ПЕРЕСТРАИВАЕМОГО АВТОМАТА[1]

В. Н. Тренькаев

Томский государственный университет, г. Томск, Россия

E-mail: tvnik@sibmail.com

Предлагается реализация шифра Закревского на основе перестраиваемого автомата, настройка которого вместе с начальным состоянием является ключом шифра. Показано, что множество шифрующих автоматов, получаемых в результате всех возможных настроек перестраиваемого автомата, обладает достаточной мощностью, чтобы противостоять атаке грубой силы. Вместе с тем предложенная реализация имеет практически приемлемую длину ключа. Также показано, что данная реализация не стойка к атаке на основе выбранного открытого текста, когда криптоаналитик знает начальное состояние и имеет несколько экземпляров шифратора.

Ключевые слова: *шифр Закревского, обратимый автомат, автомат с биективной функцией выходов, перестраиваемый автомат, кратные безусловные эксперименты по идентификации автомата.*

Введение

Известно [1, 2], что модель конечного автомата активно применяется в криптографии. Однако существует не так много используемых на практике шифров, в которых алгоритм шифрования (расшифрования) задается конечным автоматом. К числу прочих академических автоматных шифров можно отнести и шифр Закревского [3], в котором не указана процедура порождения шифрующих автоматов с требуемыми свойствами. При этом шифр Закревского можно также отнести к классу так называемых недетерминированных шифров (по терминологии [4]), т. е. шифров, у которых алгоритм шифрования формируется (выбирается) на этапе предвычислений в зависимости от секретного ключа.

Шифр с выбираемым криптоалгоритмом можно рассматривать как перестраиваемый автомат [5 – 7], т. е. автомат с возможностью настройки на требуемый алгоритм функционирования. Обычно перестраиваемый автомат имеет зафиксированную структуру логической схемы, его реализующей, и настройка автомата заключается в изменении связей между функциональными элементами схемы (структурная настройка) или их функциональности (функциональная настройка). При этом результатом каждой настройки перестраиваемого автомата является некоторый автомат из заданного класса.

В данной работе предлагается реализация шифра Закревского с использованием перестраиваемого автомата с функциональной настройкой. Каждая настройка перестраиваемого автомата порождает приведенный сильносвязный автомат с биективной функцией выходов, который задает алгоритм шифрования. Логическая сеть перестраиваемого автомата такова, что при любой настройке реализуется некоторая фиксиро-

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

ванная функция выходов, в то время как функция переходов «составляется» из функций переходов двух известных базовых автоматов. Таким образом, при аппаратной реализации перестраиваемого автомата мы имеем избыточность на уровне дублирования функциональных узлов, отвечающих за реализацию функции переходов.

1. Основные определения и обозначения

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

Четверку $s - x/y \to s'$, где $s' = \psi(x, s)$ и $y = \varphi(x, s)$, называют *переходом* автомата A и говорят, что автомат A из состояния s (обозначается A/s) под действием входного символа x переходит в состояние s' с выдачей выходного символа y.

Говорят, что входное слово $x_1x_2 \dots x_l \in X^*$ *переводит* автомат A/s в состояние s' с выдачей выходного слова (*реакции*) $y_1y_2 \dots y_l \in Y^*$, если существует (или говорят, что *реализуется* под действием $x_1x_2 \dots x_l$) последовательность переходов $s = s_1 - x_1/y_1 \to s_2$, $s_2 - x_2/y_2 \to s_3$, …, $s_l - x_l/y_l \to s_{l+1} = s'$.

Автомат A при фиксированном состоянии s реализует отображение (далее *словарный оператор*) $f_s : X^* \to Y^*$, для которого $f_s(x_1x_2 \dots x_l) = y_1y_2 \dots y_l$.

Определение 2. Автомат A называется *сильносвязным*, если для любых состояний s и s' существует входное слово, которое переводит автомат из состояния s в состояние s'.

Определение 3. Автомат A называется *приведенным*, если для любого состояния s не существует состояния s', такого, что $s \neq s'$ и $f_s = f_{s'}$.

Определение 4. Автомат A *обратим*, если при любом состоянии s для отображения f_s существует обратное отображение f_s^{-1}.

Определение 5. Автомат $A^{-1} = (Y, S, X, \psi', \varphi')$ называется *обратным* к автомату $A = (X, S, Y, \psi, \varphi)$, реализующему $\{f_s : s \in S\}$, если A^{-1} реализует $\{f_s^{-1} : s \in S\}$.

Несложно показать, что при $|X| = |Y|$ автомат A обратим, если и только если для любого $s \in S$ функция $\varphi_s(x) = \varphi(x, s)$ является биекцией из X в Y.

Определение 6. Автомат A называется *автоматом с биективной функцией выходов*, если для любого $s \in S$ функция $\varphi_s(x)$ является биекцией.

Таким образом, автомат с биективной функцией выходов (и только он при $|X| = |Y|$) является обратимым и для него существует обратный автомат. В этом случае A^{-1} может быть получен по A следующим образом: для каждого перехода $s - x/y \to s'$ автомата A строится соответствующий переход $s - y/x \to s'$ автомата A^{-1}.

2. Шифр Закревского

Шифр Закревского является симметричным шифром, в котором множества открытых и шифрованных сообщений являются множествами слов в некоторых алфавитах, алгоритмы шифрования и расшифрования задаются взаимно обратными сильносвязными автоматами с биективными функциями выходов, и ключом шифра являются начальное состояние и функции переходов и выходов обоих автоматов.

Пусть X и Y — алфавиты соответственно открытых и шифрованных сообщений, причем далее везде $|X| = |Y|$. Тогда шифрование по Закревскому заключается в преобразовании открытого сообщения $\alpha \in X^*$ в шифрованное сообщение $\beta \in Y^*$ с помощью автомата $A = (X, S, Y, \psi, \varphi)$ (с необходимыми свойствами) при фиксированном

начальном состоянии s, т. е. мы имеем $f_s(\alpha) = \beta$. Чтобы расшифровать β, требуется построить обратный автомат $A^{-1} = (Y, S, X, \psi', \varphi')$ и подать на него β, поскольку $f_s^{-1}(\beta) = \alpha$.

Пусть мы имеем два разных ключа k_A и k_B, т. е. автомат $A = (X, S, Y, \psi_A, \varphi_A)$ с начальным состоянием q и автомат $B = (X, S, Y, \psi_B, \varphi_B)$ с начальным состоянием p. Ключи k_A и k_B называются *эквивалентными*, если автоматы A/q и B/p реализуют один и тот же словарный оператор.

Показано [1], что число всех попарно неэквивалентных ключей шифра Закревского не меньше m^n, где $|X| = |Y| = m$, $|S| = n$, то есть атака на шифр, основанная на методе полного (тотального) опробования ключей, практически не осуществима при $m, n > 20$. Кроме того, в рамках автоматной модели криптоанализ шифра Закревского сводится к решению задачи восстановления (идентификации) автомата с помощью проведения эксперимента с ним, которая в общем случае считается труднорешаемой. Однако к недостаткам шифра Закревского можно отнести большой размер ключа.

Действительно, пусть $r =]\log_2|S|[$, т. е. r есть наименьшее целое, такое, что $2^r \geqslant |S|$, и $v =]\log_2|Y|[$. Тогда для задания ключа потребуется не менее $mn(r + v) + r$ бит. При $r = v = 5$ и $m = n = 20$ мы имеем 4005 бит, что на порядок больше используемых на практике размеров в 128/256 бит.

Кроме того, существует проблема генерирования ключей, так как ключевое множество шифра Закревского задано описанием свойств его элементов, но для практического использования требуется задаться порождающей процедурой, допускающей простую программную и/или аппаратную реализацию. Иными словами, необходим алгоритм генерирования сильносвязных автоматов с биективной функцией выходов и с низкой вероятностью повтора, чтобы ключ выбирался случайно и равновероятно. При этом порождающая процедура может зависеть от некоторого параметра. Тогда автомат с заданными свойствами будет строиться под управлением некоторого ключа инициализации приемлемого размера, например пароля пользователя. Для решения данной задачи предлагается использовать перестраиваемый автомат.

3. Перестраиваемый автомат

С любым автоматом можно связать логическую сеть, моделирующую его поведение. Будем считать, что логические сети (совокупности элементов, связанных между собой путем отождествления некоторых их полюсов) могут включать в себя многофункциональные настраиваемые элементы, т. е. элементы, поведение которых зависит от $k \in K$, где K — конечное множество настроек.

Автомат, реализуемый такой логической сетью, будем называть *перестраиваемым*, полагая, что его функции переходов и выходов зависят не только от $(x, s) \in X \times S$, но и от $k \in K$, т. е. перестраиваемый автомат — это шестерка $(X, S, Y, K, \psi, \varphi)$, где $\psi : X \times S \times K \to S$ и $\varphi : X \times S \times K \to Y$. Будем говорить, что, фиксируя некоторое k из K, мы *настраиваем* автомат.

Таким образом, перестраиваемый автомат задает множество J автоматов $A_k = (X, S, Y, \psi_k, \varphi_k)$, где $\psi_k(x, s) = \psi(x, s, k)$ и $\varphi_k(x, s) = \varphi(x, s, k)$ для $k \in K$.

Пусть I, O и K — конечные множества, $C = \{0, 1\}$ и заданы функции $\delta_0 : I \to O$, $\delta_1 : I \to O$, $\pi : I \times K \to C$, а также функция $\rho : O \times O \times C \to O$, такая, что $\rho(d_0, d_1, c) = d_c$ для всех d_0, d_1 в O и $c \in C$. Таким образом, ρ работает как мультиплексор, который в зависимости от управляющего символа $c \in C$ «пропускает со входов на выход» либо d_0, либо d_1.

Определим функцию $\lambda : I \times K \to O$ так, что $\lambda(i,k) = \lambda_k(i) = \rho(\delta_0(i), \delta_1(i), \pi_k(i))$ для любых $i \in I$ и $k \in K$, и будем называть её *настраиваемой композицией* (с управлением π, зависящим от входа в I и настройки в K). При фиксированной настройке k она показана схематически на рис. 1.

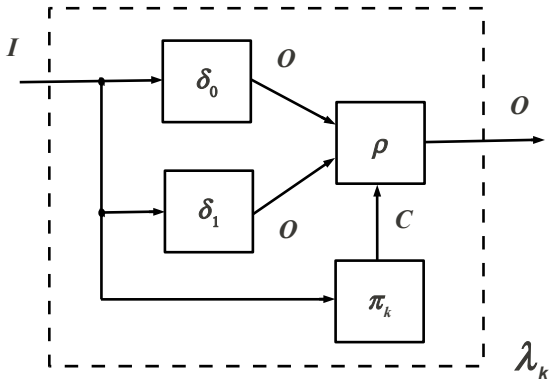

Рис. 1. Настраиваемая композиция λ с настройкой k

Построим перестраиваемый автомат $R = (X, S, Y, K, \psi, \varphi)$ следующим образом. Функция выходов φ зависит от $k \in K$ фиктивно, т. е. является фактически отображением $\varphi : X \times S \to Y$, и $\{\varphi_s(x) : s \in S\}$ есть множество различных биекций. Функция переходов ψ является настраиваемой композицией λ, в которой $I = X \times S$ и $O = S$, т. е. для любой пары $(x, s) \in X \times S$ верно $\psi_k(x, s) = \lambda_k(x, s)$. Логическая сеть, реализующая автомат R, изображена на рис. 2. Она состоит из компонент *State*, *Out* и *Reg*. Компонента *State* реализует настраиваемую функцию переходов $\psi_k(x, s)$, компонента *Out* — фиксированную функцию выходов $\varphi(x, s)$, компонента *Reg* — память автомата. Последняя компонента состояние, поступающее ей на вход, выдает на выход в следующий такт работы. Данная сеть является каноническим предствлением автомата схемой, состоящей из комбинационной части (компоненты *State* и *Out*) и элементов памяти (компонента *Reg*).

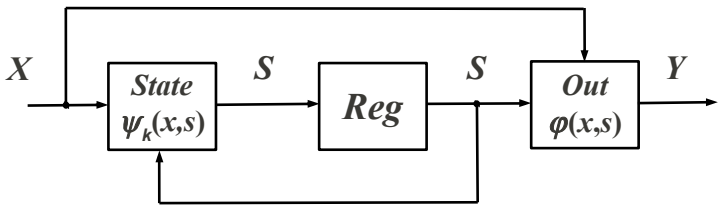

Рис. 2. Перестраиваемый автомат R

Нетрудно заметить, что поведение перестраиваемого автомата R формируется в результате совместной работы двух автоматов $B_0 = (X, S, Y, \delta_0, \varphi)$ и $B_1 = (X, S, Y, \delta_1, \varphi)$. Причем состояние, в которое переходит автомат R из текущего, формирует как δ_0,

так и δ_1, но в память «закладывается» только одно из двух возможных значений, т. е. память является общей для автоматов B_0 и B_1.

Далее предполагается, что функции δ_0 и δ_1 в настраиваемой композиции λ автомата R таковы, что существует входное слово α длины n, которое переводит автомат B_0 и автомат B_1 из некоторого состояния t в то же состояние t, посещая при этом (проводя автомат через) все другие состояния из S, и, кроме того, в автоматах B_0/t и B_1/t под действием α реализуется одинаковая последовательность переходов. Тогда при любой настройке k автомата R для любой пары состояний в полученном автомате $A_k \in J$ существует входное слово, которое переводит A_k из первого из этих состояний во второе. Таким образом, по построению автомата R справедливо следующее утверждение.

Утверждение 1. Перестраиваемый автомат $R = (X, S, Y, K, \psi, \varphi)$ при каждой настройке $k \in K$ является приведенным сильносвязным автоматом $A_k = (X, S, Y, \psi_k, \varphi)$ с биективной функцией выходов, причем для любой пары (x, s) из $X \times S$ верно: если $\pi_k(x, s) = 0$, то $\psi_k(x, s) = \delta_0(x, s)$, иначе $\psi_k(x, s) = \delta_1(x, s)$.

4. Реализация шифра Закревского на основе перестраиваемого автомата

Ввиду утверждения 1 любая настройка автомата R задает (порождает) шифрующий автомат для шифра Закревского. При этом (в случае $X = Y$) для шифрования и расшифрования используется логическая сеть (рис. 2), где при расшифровании компонента Out реализует функцию $\eta(x, s)$, такую, что $\eta_s(x) = \varphi_s^{-1}(x)$ при любом $s \in S$. Именно эта сеть и предлагается в качестве *реализации шифра Закревского*. В ней ключом выступает настройка автомата R вместе с некоторым начальным состоянием. Таким образом, ключевое множество Ω в реализации шифра Закревского на основе перестраиваемого автомата является множеством $\{A_k/s : A_k \in J, s \in S\}$. Оно, естественно, много меньше множества всех ключей в шифре Закревского с теми же параметрами автомата. Вместе с тем, при надлежащем выборе последних, его можно сделать достаточно большим, чтобы противостоять атаке грубой силы.

Теорема 1. Ключевое множество Ω не содержит попарно эквивалентных ключей, и его мощность равна $n2^{n(m-1)}$.

Доказательство. По построению существует входное слово α длины n, под действием которого в автоматах B_0 и B_1, а значит, и в любом $A_k \in J$ реализуется одинаковая последовательность переходов. Следовательно, для n пар (x, s) значения функции $\pi_k(x, s)$ не зависят от k, и число всех таких функций, сопоставляемых разным значениям k, равно 2^{nm-n}. Таким образом, $|\Omega| \leqslant n2^{n(m-1)}$.

Покажем, что ключевое множество Ω не содержит попарно эквивалентных ключей и, следовательно, $|\Omega| = n2^{n(m-1)}$. Пусть мы имеем два произвольных разных ключа, т. е. автомат $A = (X, S, Y, \psi_A, \varphi) \in J$ с начальным состоянием q и автомат $B = (X, S, Y, \psi_B, \varphi) \in J$ с начальным состоянием p. Если q и p — разные состояния, то поскольку по построению $\{\varphi_s(x) : s \in S\}$ — множество различных биекций, существует хотя бы один входной символ x, такой, что $\varphi_q(x) \neq \varphi_p(x)$. Следовательно, автоматы A/q и B/p реализуют разные словарные операторы.

Рассмотрим случай, когда q и p — одинаковые состояния. Так как A/q и B/p — разные ключи, то A и B — разные автоматы и, следовательно, существует хотя бы одна пара $(x, s) \in X \times S$, такая, что $\psi_A(x, s) \neq \psi_B(x, s)$. Также по построению при любом $k \in K$ в автомате $A_k \in J$ существует последовательность переходов $t = s_{i_1} - x_1/y_1 \to s_{i_2}, s_{i_2} - x_2/y_2 \to s_{i_3}, \ldots, s_{i_n} - x_n/y_n \to s_{i_{n+1}} = t$. Причем $x_1x_2 \ldots x_n$ переводит автомат A_k из состояния t в состояние t, посещая при этом все другие

состояния из S. Следовательно, используя данную последовательность переходов, всегда можно построить входное слово β, которое переводит A/q и B/p (при условии, что q и p — одинаковые состояния, а это так по предположению) в состояние s. Пусть $\psi_A(x,s)=s'$ и $\psi_B(x,s)=s''$. Так как s' и s'' — разные состояния, то существует хотя бы один входной символ z, такой, что $\varphi_{s'}(z)\neq\varphi_{s''}(z)$. Таким образом, существует входное слово βxz, в ответ на которое автоматы A/q и B/p выдают разные выходные слова, т. е. A/q и B/p реализуют разные словарные операторы. ■

Каждой настройке $k\in K$ автомата R во взаимно-однозначное соответствие ставится вектор значений функции $\pi_k(x,s)$, в котором n компонент предопределены заранее. Он является некоторым булевым вектором h длины $|X\times S|$, поэтому длина ключа предложенной реализации шифра Закревского не превышает числа $mn+r$. Например, при $m=n=20$ и $r=5$ это число равно 405 (а не 4005 — длине ключа в шифре Закревского при тех же значениях m, n и r). Однако, ввиду теоремы 1, достаточно взять $m=n=10$ и $r=4$, чтобы достичь в реализации приемлемого числа $(2^{90}\cdot 10)$ всех возможных ключей и приемлемой длины ключа (104 бита). Также можно отметить, что булев вектор h может быть получен на основе некоторого генератора псевдослучайных последовательностей, который, в свою очередь, может инициализироваться булевым вектором меньшей длины, чем h, но достаточной для обеспечения его (булева вектора h) случайности. Таким образом, предложенная реализация шифра Закревского имеет малую длину ключа при достаточно большой мощности ключевого множества.

5. Криптоанализ реализации шифра Закревского на основе перестраиваемого автомата

Рассмотрим способность реализации шифра Закревского противостоять криптоаналитической атаке с использованием выбранного открытого текста. В рамках автоматной модели имеем задачу восстановления (идентификации) автомата с помощью проведения с ним эксперимента [8]. Здесь ограничимся применением кратных безусловных экспериментов, т. е. будем предполагать, что у криптоаналитика имеется в наличии несколько экземпляров (копий) неизвестного автомата, находящихся перед экспериментом в одном и том же начальном состоянии (их число называется кратностью эксперимента), и прикладываемые к ним входные слова определяются заранее, а не по ходу эксперимента. Задача заключается в том, чтобы по реакциям экземпляров автомата определить сам автомат.

В нашем случае для эксперимента предъявлены экземпляры некоторого автомата E из множества J, которое задается перестраиваемым автоматом R, построенным вышеописанным способом. Будем предполагать, что начальное состояние автомата E, одно то же во всех экземплярах, известно. Требуется по наблюдаемым реакциям этих экземпляров на входные слова определить функцию переходов автомата E.

Под *длиной эксперимента* понимают сумму длин всех применённых в нём входных слов, а под его кратностью — количество использованных копий автомата. Покажем, что любой автомат $E\in J$ при известном его начальном состоянии может быть восстановлен кратным безусловным экспериментом, длина и кратность которого не превышают $(n+2)mn$ и mn соответственно.

По построению автомата R существует входное слово длины n, которое при любом $k\in K$ переводит автомат $A_k\in J$ из некоторого состояния в то же самое состояние, посещая при этом все другие состояния из S. Следовательно, любой автомат $E\in J$,

предъявленный для эксперимента, с известным начальным состоянием можно перевести входным словом α длины не более n в любое заданное состояние s.

Тогда задача восстановления автомата E сводится к задаче восстановления в нем произвольного перехода $s - x/y \to s'$, у которого состояние s является известным экспериментатору, x — выбираемый входной символ, y — наблюдаемый выходной символ. По утверждению 1 неизвестное состояние s' принадлежит $\{\delta_0(x,s), \delta_1(x,s)\}$. Если $\delta_0(x,s) = \delta_1(x,s) = p$, то $s' = p$. Если $\delta_0(x,s)$ и $\delta_1(x,s)$ — разные состояния, то по свойству функции выходов φ автомата R существует хотя бы один входной символ z, такой, что $\varphi(z, \delta_0(x,s)) \neq \varphi(z, \delta_1(x,s))$. Тогда по реакции автомата E из начального состояния на входное слово αxz длины не более $n+2$ можно однозначно идентифицировать состояние s'.

Так как для восстановления переходов автомата E достаточно перебрать все пары (x,s) из $X \times S$, используя для каждой пары свою копию автомата E, то длина эксперимента будет не более $(n+2)mn$, а кратность — mn. Тем самым доказана следующая теорема.

Теорема 2. Существует кратный безусловный эксперимент с длиной не более $(n+2)mn$ и кратностью не более mn, посредством которого однозначно восстанавливается любой автомат из класса J с известным начальным состоянием.

В переводе на язык криптографии это значит, что для реализации шифра Закревского на основе перестраиваемого автомата R имеет место следующее свойство: если часть ключа, представленная начальным состоянием автомата шифрования, известна, то остальная его часть полностью раскрывается простой атакой с выбором не более mn открытых текстов с общей длиной не более $(n+2)mn$ символов. О её стойкости к другим атакам с той же или иными угрозами ничего пока неизвестно.

Заключение

В данной работе предложена ориентированная на практику реализация шифра Закревского на основе автомата, перестраиваемого на разные шифрующие автоматы по параметру настройки. Показано, что: 1) каждая настройка перестраиваемого автомата порождает приведенный сильносвязный автомат с биективной функцией выходов; 2) количество настроек достаточно велико, чтобы противостоять атаке грубой силы; 3) настройка задается булевым вектором длины, приемлемой для практического использования в криптографии; 4) аппаратная реализация перестраиваемого автомата имеет избыточность на уровне дублирования функциональных узлов, отвечающих за реализацию функции переходов; 5) при известном начальном состоянии шифрующего автомата, полученного настройкой перестраиваемого автомата, задача его идентификации с помощью кратного безусловного эксперимента имеет полиномиальную сложность (от размеров автомата); 6) вопрос о стойкости данной реализации к атакам других типов требует дополнительных исследований.

ЛИТЕРАТУРА

1. *Агибалов Г. П.* Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.
2. *Бабаш А. В., Шанкин Г. Н.* Криптография. М.: СОЛОН-Р, 2002. 512 с.
3. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
4. *Молдовян А. А., Молдовян Н. А., Советов Б. Я.* Криптография. СПб.: Изд-во «Лань», 2001. 224 с.

5. *Шидловский С. В.* Автоматическое управление. Перестраиваемые структуры. Томск: Томский государственный университет, 2006. 288 с.
6. *Glaser J., Damm M., Haase J., Grimm Ch.* A dedicated reconfigurable architecture for finite state machines // LNCS. 2010. No. 5992. P. 122–133.
7. *Sklyarov V.* Reconfigurable models of finite state machines and their implementation in FPGAs // J. Systems Architecture. 2002. No. 47. P. 1047–1064.
8. *Гилл А.* Введение в теорию конечных автоматов. М.: Наука, 1966. 272 с.