УДК 519.713 DOI 10.17223/2226308X/12/53

ПЕРЕСТРАИВАЕМЫЕ АВТОМАТЫ НА ПОДСТАНОВКАХ

В. Н. Тренькаев

Предлагается структура перестраиваемого автомата, поведение которого определяется набором базовых подстановок. Настройка автомата заключается в «сборке» функции переходов и функции выходов из базовых подстановок. Вариант «сборки» фиксируется заданием трёх изменяемых подстановок: для входного алфавита, для функции выходов, для функции переходов. Показано, что любая настройка перестраиваемого автомата соответствует приведённому сильносвязному обратимому автомату, а следовательно, предлагаемый перестраиваемый автомат может быть использован при реализации автоматных шифров, в частности шифра Закревского.

Ключевые слова: *перестраиваемый автомат, обратимый автомат, автоматный шифр.*

Перестраиваемые автоматы — цифровые автоматы, имеющие возможность внесения изменений в алгоритм функционирования, что реализуется с помощью настройки. Существует много вариантов архитектур перестраиваемых автоматов [1, 2], ориентированных на разные прикладные области (сети, встраиваемые системы, обработка сигналов и пр.), использующих разные способы настройки (на базе ПЗУ, ОЗУ, ПЛИС и пр.).

В данной работе рассматривается архитектура с функциональной настройкой, когда не изменяются связи между элементами автомата, но изменяется их функциональность. Областью приложения является криптография, а именно автоматные шифры [3, 4], в которых алгоритм шифрования (расшифрования) задаётся конечным автоматом. В случае автоматного шифрования каждой настройке перестраиваемого автомата, читай ключу, должен соответствовать некоторый обратимый автомат из заданного класса. Для дальнейшего изложения введём некоторые определения из [4].

Определение 1. *Конечным автоматом* A называется пятёрка (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. Далее считаем, что $X = Y = S$.

Четвёрку $s - x/y \to s'$, где $s' = \psi(x, s)$ и $y = \varphi(x, s)$, называют *переходом* автомата A. Говорят, что входное слово $x_1x_2 \dots x_n \in X^*$ *переводит* автомат A из состояния s в состояние s' с выдачей выходного слова $y_1y_2 \dots y_n \in Y^*$, если существует последовательность переходов $s = s_1 - x_1/y_1 \to s_2$, $s_2 - x_2/y_2 \to s_3$, $\dots$, $s_n - x_n/y_n \to s_{n+1} = s'$.

Автомат A при фиксированном состоянии s реализует алфавитное отображение $f_s : X^* \to Y^*$, для которого $f_s(x_1x_2 \dots x_n) = y_1y_2 \dots y_n$.

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 *приведённым*, если для любого состояния s не существует другого 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}.

Структура перестраиваемого автомата на подстановках представлена на рис. 1, где $SubX$, $SubY$, $SubS$ реализуют отображения $SubX : X \times K_X \to X$, $SubY : S \times K_Y \to S$, $SubS : S \times K_S \to S$ соответственно. Базовые компоненты $Sub1$, $Sub2$, …, $SubN$, а также настраиваемые компоненты $SubX$, $SubY$, $SubS$ при фиксированных ключах из K_X, K_Y, K_S соответственно реализуют подстановки. Все базовые подстановки различны. Количество базовых подстановок совпадает с количеством состояний. Мультиплексоры $M1$ и $M2$ в зависимости от управляющего символа «пропускают» далее значение одной из базовых подстановок. $M1$ отвечает за «сборку» функции выходов, а $M2$ — функции переходов. Компонента Reg в каждый момент автоматного времени хранит текущее состояние. Таким образом, перестраиваемый автомат имеет большую жёсткую логику — N базовых компонент, малую программируемую логику — три компоненты $SubX$, $SubY$, $SubS$ и два мультиплексора для управления процессом «сборки». Жёсткая логика дает высокое быстродействие, а программируемая логика — гибкость.

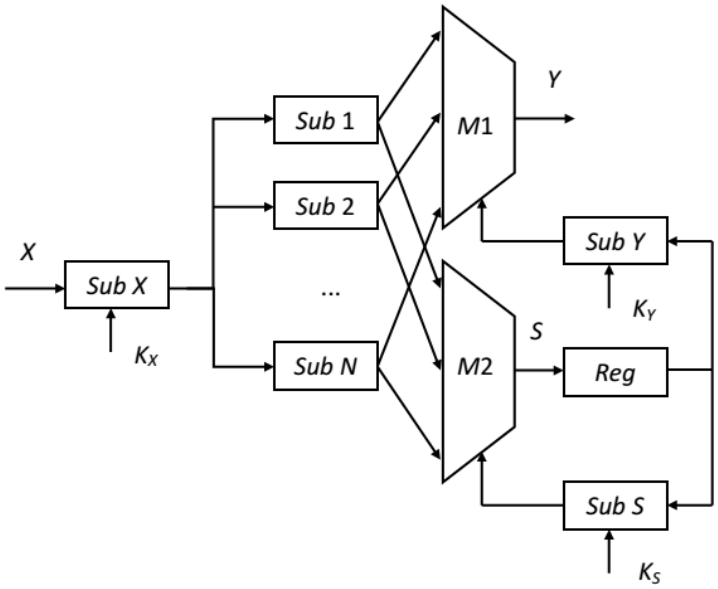

Рис. 1. Структура перестраиваемого автомата на подстановках

Утверждение 1. Перестраиваемый автомат на подстановках при фиксированных ключах из K_X, K_Y, K_S есть приведённый сильносвязный обратимый автомат.

ЛИТЕРАТУРА

1. *Das N. and Priya P. A.* FPGA implementation of reconfigurable Finite State Machine with input multiplexing architecture using Hungarian method // Intern. J. Reconfigurable Computing. 2018. Article ID 6831901. 15 p.
2. *Teich J. and Koster M.* (Self-)reconfigurable Finite State Machines: Theory and Implementation // Proc. DATE'02. 2002. P. 559–566.
3. *Агибалов Г. П.* Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.
4. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.