References

1. Kovalev P. V., Laykov A. N., Gritsenko S. N. *Vestnik SibGAU.* 2009, no. 1(22) in 2 series. Series 2, p. 55–60.
2. Kovalev P. V. *Uspehi sovremennogo estestvoznaniya*. 2009, no. 9, p. 161–164.
3. Dorrer M. G., Ziryanov A. A. *Informatsiya I svyaz.* 2012, no. 7, p. 124–127.
4. Kovalev I. V. *Sistemi upravleniya I informatzionnie technologii.* 2005, no. 3 (20), p. 58–62.
5. Degterev A. S., Pisyman D. M. *Fundamentalynie issledovaniya*. 2005, no. 4, p. 79–80.
6. Fillips D., Garsia-Dias A. *Metodi analiza sete* (Methods for analyzing networks). Moscow, Mir, 1984.

УДК 004.056.55

РЕАЛИЗАЦИЯ НА ПЛИС ШИФРА ЗАКРЕВСКОГО НА ОСНОВЕ ПЕРЕСТРАИВАЕМОГО АВТОМАТА

Д. С. Ковалев

ОАО «Информационные спутниковые системы» имени академика М. Ф. Решетнёва»
Российская Федерация, 662972, г. Железногорск Красноярского края, ул. Ленина, 52
E-mail: dmisk@hotmail.com

Рассматривается задача проектирования быстродействующего компактного криптопроцессора. Предлагается решение данной задачи на базе конечно-автоматной модели. В качестве представителя класса автоматных шифров выбран шифр Закревского на основе перестраиваемого автомата. Представлена аппаратная реализация на ПЛИС Xilinx Spartan-3 данного шифра. Приведены значения ресурсоёмкости и производительности данной реализации. Произведено сравнение реализаций на ПЛИС шифра Закревского на основе перестраиваемого автомата, блочного шифра AES и поточных шифров – финалистов конкурса eSTREAM, рекомендованных для аппаратной реализации. Сделано заключение о возможности использования шифра Закревского на основе перестраиваемого автомата на практике.

Ключевые слова: криптопроцессор, ПЛИС, конечно-автоматная шифрсистема, шифр Закревского, перестраиваемый автомат.

FPGA IMPLEMENTATION OF THE ZAKREVSKIJ'S CIPHER BASED ON RECONFIGURABLE FSM

D. S. Kovalev

JSC “Information satellite system” named after academician M. F. Reshetnev”
52, Lenin str., Zheleznogorsk, Krasnoyarsk region, 662972, Russian Federation
E-mail: dmisk@hotmail.com

The problem of the compact high-throughput cryptoprocessor design is considered. This problem solution based on the Finite State Machine model is offered. Zakrevskij's Cipher Based on Reconfigurable FSM is chosen as a representative of the finite automata ciphers class. FPGA Xilinx Spartan-3 hardware implementation of this cipher is presented. Values of the hardware resource using and throughput of this implementation are given. The FPGA implementation comparison of Zakrevskij's Cipher Based on Reconfigurable FSM, block cipher AES and hardware-oriented stream ciphers became eSTREAM competition finalists was made. The conclusion about Zakrevskij's Cipher Based on Reconfigurable FSM practice using possibility is made.

Keywords: cryptoprocessor, FPGA, finite automata cryptosystem, Zakrevskij’s cipher, reconfigurable finite state machine.

В настоящее время существует высокая потребность в создании быстродействующих компактных криптопроцессоров, которые используются для снижения вычислительной нагрузки основного процессора, в средствах автоматического регулирования и управления техпроцессами, в телекоммуникационном оборудовании, так же как аппаратные модули доверенной загрузки операционной системы и пр.

Криптопроцессоры, как правило, являются устройствами, в которых реализованы криптографические алгоритмы различного назначения (симметричное/ асимметричное шифрование, электронная цифровая

подпись, хэширование). Часто разнородность криптоалгоритмов не позволяет использовать единый объединяющий все алгоритмы подход при проектировании криптопроцессора, что может дать существенный выигрыш по быстродействию, энергопотреблению, компактности и др. Как вариант объединяющего подхода предлагается использование автоматной модели при задании криптоалгоритмов.

Конечно-автоматные шифрсистемы давно известны криптографам [1], но мало изучены. В частности, в литературе не встречаются исследования на пригодность их к практическому использованию. В данной работе в качестве представителя класса автоматных шифров выбран шифр Закревского на основе перестраиваемого автомата [2]. Исследуются характеристики данного шифра при реализации его на базе программируемой логической интегральной схемы (ПЛИС).

Необходимые определения.

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.

Автомат A при фиксированном состоянии s реализует отображение $f_s : X^* \to Y^*$, для которого $f_s(\alpha) = \beta$, где $\beta \in Y^*$ – реакция автомата A на входное слово $\alpha \in X^*$.

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

Определение 4. Шифром Закревского называется автоматный шифр, в котором множества открытых и шифрованных сообщений являются множествами слов в некоторых алфавитах, алгоритмы шифрования и расшифрования задаются взаимно обратными сильносвязными инициальными автоматами A и A^{-1} с биективными в каждом состоянии функциями выходов.

Для практического использования шифра Закревского требуется задать процедуру генерации автоматов A и A^{-1} по ключу. В работе [2] предлагается использовать для этих целей так называемый перестраиваемый автомат, т. е. автомат, функция переходов которого строится «на лету» с помощью блока управления.

Структура перестраиваемого автомата. Структура перестраиваемого автомата представлена на рисунке. Компонента Key управляет работой мультиплексора MUX, который из двух состояний $s_1 = \psi_1(s,x)$ и $s_2 = \psi_2(s,x)$ выбирает одно. Компонента Reg (регистр памяти) предназначена для хранения текущего состояния автомата. Компонента Key реализует булеву функцию, вектор значений которой является секретом (ключом) и «загружается» (вместе с начальным состоянием) в шифрсистему при инициализации. Таким образом, схема на рисунке задает шифрующий автомат $A = (X, S, Y, \psi, \varphi)$, в котором для любой пары (x,s) из $X \times S$ выполняется, что $\psi(x,s) = \psi_1(s,x)$, когда $\mathrm{Key}(x,s) = 0$, либо $\psi(x,s) = \psi_2(s,x)$, когда $\mathrm{Key}(x,s) = 1$.

Чтобы шифрующий автомат A был сильносвязным, одна из функций $\psi_1(s,x)$ или $\psi_2(s,x)$ (пусть ψ_1) задаёт сильносвязный граф переходов. Пусть $S = \{s_i: I = 1, \ldots, m\}$. Тогда существует x из X такой, что $\psi_1(s_i,x) = s_{i+1}$, когда $i<m$ и $\psi_1(s_m,x) = s_1$, причём $\mathrm{Key}(x,s) = 0$ для любого s из S.

Для расшифрования в схеме на рисунке вместо функции выходов $\varphi(s,x)$ нужно использовать функцию $\varphi'(s,y) = x$ такую, что для любого s из S выполняется $\varphi'_s(y) = \varphi^{-1}{}_s(y)$. Также значение функции $\varphi'(s,y)$ должно подаваться на вход компонентам Key, $\psi_1(s,x)$ и $\psi_2(s,x)$.

Реализация на ПЛИС. В настоящей работе исследуется перестраиваемый автомат, у которого $|X| = |Y| = 16$ (4 бита при кодировании), $|S| = 8$ (3 бита при кодировании). Таким образом, длина ключа равна $16 \cdot 8 – 8 + 3 = 128 – 8 + 3 = 123$ бита (128 бит – вектор состояний булевой функции Key, 8-бит – для реализации сильносвязности, 3 бита – начальное состояние). Таблицы переходов $\psi_1(s,x)$ и $\psi_2(s,x)$ и таблица выходов $\varphi(s,x)$ задавались случайным образом, но с обеспечением требуемых свойств (сильносвязность и биективность в каждом состоянии соответственно).

Исследуемая автоматная шифрсистема была описана на языке VHDL и промоделирована в САПР Xilinx Webpack ISE 14.1 при реализации на ПЛИС Spartan-3 XC3S50, при этом состояния автомата кодировались разными методами, что не влияло на конечные результаты.

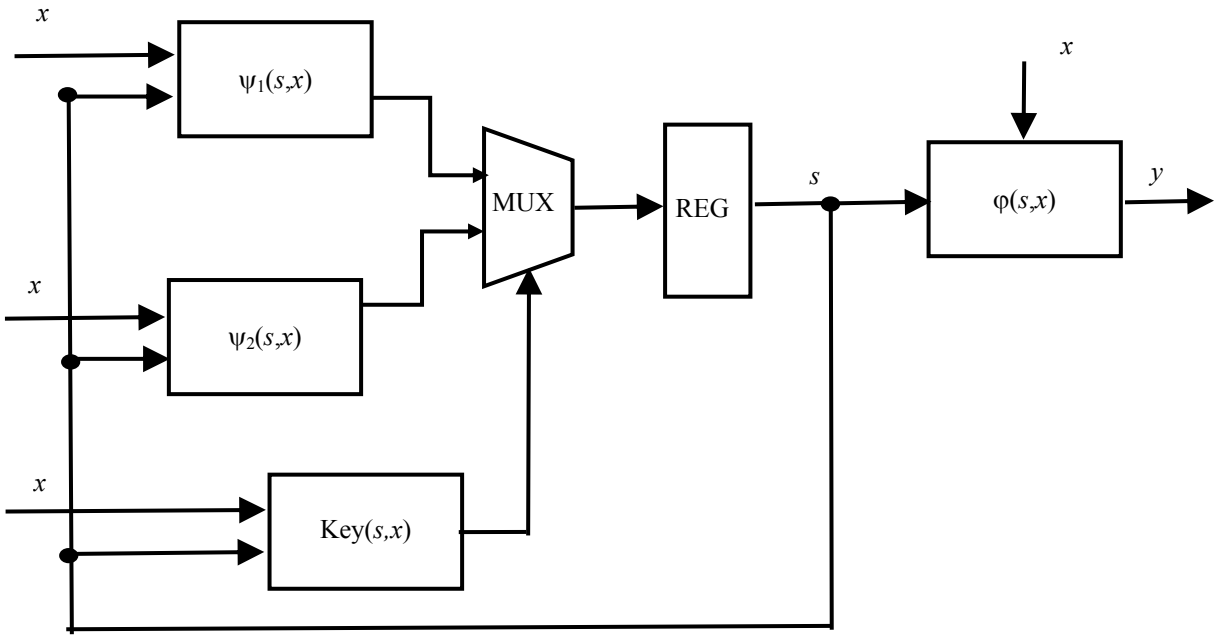
Оказалось, что процедура расшифрования имеет несколько более низкую производительность, чем процедура шифрования, но при этом также требует несколько меньшего числа ресурсов микросхемы.

Критерием оценки практической пригодности криптосистемы является эффективность её ПЛИС-реализации в сравнении с реализациями современных блочных и поточных шифров на ПЛИС того же типа.

В таблице сравниваются результаты реализации шифра Закревского на основе перестраиваемого автомата и современных блочных (представленных шифром AES) и поточных (представленных шифрами – финалистами конкурса eSTREAM, рекомендованными для аппаратной реализации: Grain, MICKEY и Trivium) шифров. Результаты реализации AES взяты из работы [3], шифров – финалистов eSTREAM – из работы [4].

Сравнение ПЛИС-реализаций шифра Закревского на основе перестраиваемого автомата и современных блочных и поточных шифров

Шифр	Ресурсоёмкость (S), Slices	Производительность (T), Мбит/с	T/S
Закревского (шифрование)	370	298	0,805
Закревского (расшифрование)	365	269	0,737
AES	163	208	1,276
Grain	50	196	3,920
MICKEY	115	233	2,026
Trivium	50	240	4,800



Структура перестраиваемого автомата

Таким образом, шифр Закревского на основе перестраиваемого автомата имеет более высокую производительность, чем блочный шифр AES и аппаратно-ориентированные поточные шифры – финалисты eSTREAM, однако уступает им в ресурсоёмкости.

В данной работе предлагается решать задачу проектирования криптопроцессора с набором различного вида криптоалгоритмов на базе автоматной модели. Проводятся исследования шифра Закревского на основе перестраиваемого автомата как представителя симметричных автоматных шифров. Указанный шифр реализован на ПЛИС Spartan-3, проведено сравнение ПЛИС-реализаций шифра Закревского на основе перестраиваемого автомата, шифров AES, Grain, MICKEY, Trivium. Проведённые исследования показывают, что автоматное симметричное шифрование пригодно к использованию на практике.

Библиографические ссылки

1. Агибалов Г. П. Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.

2. Тренькаев В. Н. Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.

3. Rouvroy G., Standaert F. X., Quisquater J. J., Legat J. D. Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications // Proc. Intern. Conf. Inform. Technology: Coding and Computing. 2004, vol. 2, p. 583–587.

4. Hwang D., Chaney M., Karanam S., Ton N., Gaj K. Comparison of FPGA-targeted hardware implementations of eSTREAM stream cipher candidates // SASC 2008 Workshop Record. eSTREAM Project, 2008, p. 151–162.

References

1. Agibalov G. P. *Prikladnaya diskretnaya matematika*. *Prilozhenie.* 2009, no 2, p. 43–73.

2. Tren'kaev V. N. *Prikladnaya diskretnaya matematika*. 2010, no 3, p. 69–77.

3. Rouvroy G., Standaert F. X., Quisquater J. J., Legat J. D. Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications. *Proc. Intern. Conf. Inform. Technology: Coding and Computing*. 2004, vol. 2, p. 583–587.

4. Hwang D., Chaney M., Karanam S., Ton N., Gaj K. Comparison of FPGA-targeted hardware implementations of eSTREAM stream cipher candidates. *SASC 2008 Workshop Record*. eSTREAM Project, 2008, p. 151–162.