УДК 004.056.55

РЕАЛИЗАЦИЯ НА ПЛИС ШИФРА ЗАКРЕВСКОГО НА ОСНОВЕ ПЕРЕСТРАИВАЕМОГО АВТОМАТА, ЗАДАННОГО ФОРМУЛАМИ

Д. С. Ковалев, В. Н. Тренькаев

Рассмотрена реализация на ПЛИС шифра Закревского на основе перестраиваемого автомата, заданного формулами, когда функции переходов и выходов вычисляются с помощью часто используемой в симметричных шифрах операции сложения по модулю целого числа (обычно степени двойки). Установлено, что формульный (аналитический) способ представления автомата по сравнению с табличным приводит к улучшению эффективности ПЛИС-реализации шифра, в частности наблюдается рост производительности на 17–36 %.

Ключевые слова: *шифр Закревского, перестраиваемый автомат, табличный способ задания автомата, формульный способ задания автомата, производительность, ресурсоёмкость, ПЛИС, VHDL.*

Работа продолжает начатые в [1] исследования шифра Закревского на основе перестраиваемого автомата на пригодность к практическому использованию в различных вычислительных системах. Критерием оценки пригодности шифра к использованию на практике является эффективность его реализации на базе ПЛИС (программируемая логическая интегральная схема).

Шифр Закревского [2] является автоматным шифром, в котором алгоритмы шифрования и расшифрования задаются взаимно обратными сильносвязными автоматами, ключом являются начальное состояние и функции переходов и выходов обоих автоматов. В работе [3] предложено построение шифра Закревского на основе перестраиваемого автомата, функция переходов $\psi(x, s)$ которого вычисляется следующим образом. Для любой пары (x, s), где x — символ открытого текста, а s — текущее состояние перестраиваемого автомата, верно: если предикат $key(x, s) = 0$, то $\psi(x, s) = \psi_0(x, s)$, иначе $\psi(x, s) = \psi_1(x, s)$. Таким образом, следующее состояние задаётся как одно из состояний, полученных с помощью двух различных функций переходов ψ_0 и ψ_1. При шифровании символ шифртекста $y = \varphi(x, s)$ вычисляется с помощью «открытой» функции выходов φ, биективной в каждом состоянии. При расшифровании символ открытого текста вычисляется с помощью функции, обратной к φ.

В данной работе предлагается от табличной формы задания перестраиваемого автомата перейти к формульной, тем самым зафиксировать некоторые элементы структурного синтеза автомата. Далее x и s — целые положительные числа, сопоставленные символу открытого текста и состоянию соответственно, либо их двоичные представления (в зависимости от операции).

Для любой пары (x, s) верно: для $x \neq s$ если $key(x, s) = 0$, то $\psi(x, s) = x \oplus s$, иначе $\psi(x, s) = x \oplus \overline{s}$ (используются побитовые операции); если $x = s$, то $\psi(s, x) = (s + 1) \bmod n$, где n — количество символов алфавита открытых текстов (шифртекстов), которое равно числу состояний m. При вычислении функции выходов предлагается использовать обратимую операцию сложения целых чисел, а именно: $\varphi(x, s) = (x + s) \bmod n$. Таким образом, шифр Закревского на основе перестраиваемого автомата задаётся с помощью наиболее часто используемой в симметричных шифрах операции сложения по модулю.

Предложенная реализация перестраиваемого автомата описана на языке VHDL и промоделирована в САПР Xilinx WebPack ISE 14.1 на ПЛИС Spartan-3 XC3S50.

Результаты приведены в таблице (строки ШЗ-Ф), где представлены также результаты ПЛИС-реализации процедур шифрования и расшифрования шифра Закревского на основе перестраиваемого автомата, заданного таблицами переходов и выходов (строки ШЗ-Т), взятые из [1], и результаты реализации шифра AES [4]. Стоит отметить, что в работе [1] исследуется перестраиваемый автомат, у которого $n = 16$, $m = 8$, а длина ключа 123 бита. В данной работе $n = m = 16$ и длина ключа увеличена до 244 бит.

Сравнение ПЛИС-реализаций шифра Закревского на основе перестраиваемого автомата при табличном и формульном задании

Шифр	Ресурсоёмкость, Slices (S)	Производительность, Мбит/с (T)	Коэффициент эффективности T/S
ШЗ-Т (шифрование)	370	298	0,805
ШЗ-Т (расшифрование)	365	269	0,737
ШЗ-Ф (шифрование)	397	349	0,879
ШЗ-Ф (расшифрование)	398	366	0,920
AES	163	208	1,276

Из таблицы видно, что несмотря на некоторое усложнение конструкции (большее число состояний, большая длина ключа), производительность шифра Закревского на основе перестраиваемого автомата возросла на 17–36 %, при этом ресурсоёмкость увеличилась незначительно. Коэффициент эффективности реализации также увеличился, хотя и не достиг значения этой величины для AES. Однако AES опережает шифр Закревского на основе перестраиваемого автомата только за счёт меньшей ресурсоёмкости, что является существенным только для ПЛИС с небольшой логической ёмкостью (количеством вентилей).

В целом, проведённые исследования показывают, что аппаратная реализация шифра Закревского на основе перестраиваемого автомата, заданного формулами, пригодна к использованию на практике.

ЛИТЕРАТУРА

1. *Ковалев Д. С.* Реализация на ПЛИС шифра Закревского на основе перестраиваемого автомата // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнёва. 2014. № 1 С. 16–18.
2. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
3. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.
4. *Rouvroy G., Standaert F. X., Quisquater J. J., and 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. V. 2. P. 583–587.

УДК 519.7

ПРИМЕНЕНИЕ КОНЕЧНОГО АВТОМАТА ДЛЯ ОДНОВРЕМЕННОГО ПОИСКА НЕСКОЛЬКИХ ДВОИЧНЫХ ШАБЛОНОВ В ПОТОКЕ ДАННЫХ

И. В. Панкратов

Рассматривается задача поиска булевых векторов в потоке данных. Предлагается метод построения конечного автомата, который ищет одновременно несколько векторов, совершая только две простые операции на каждый бит или группу