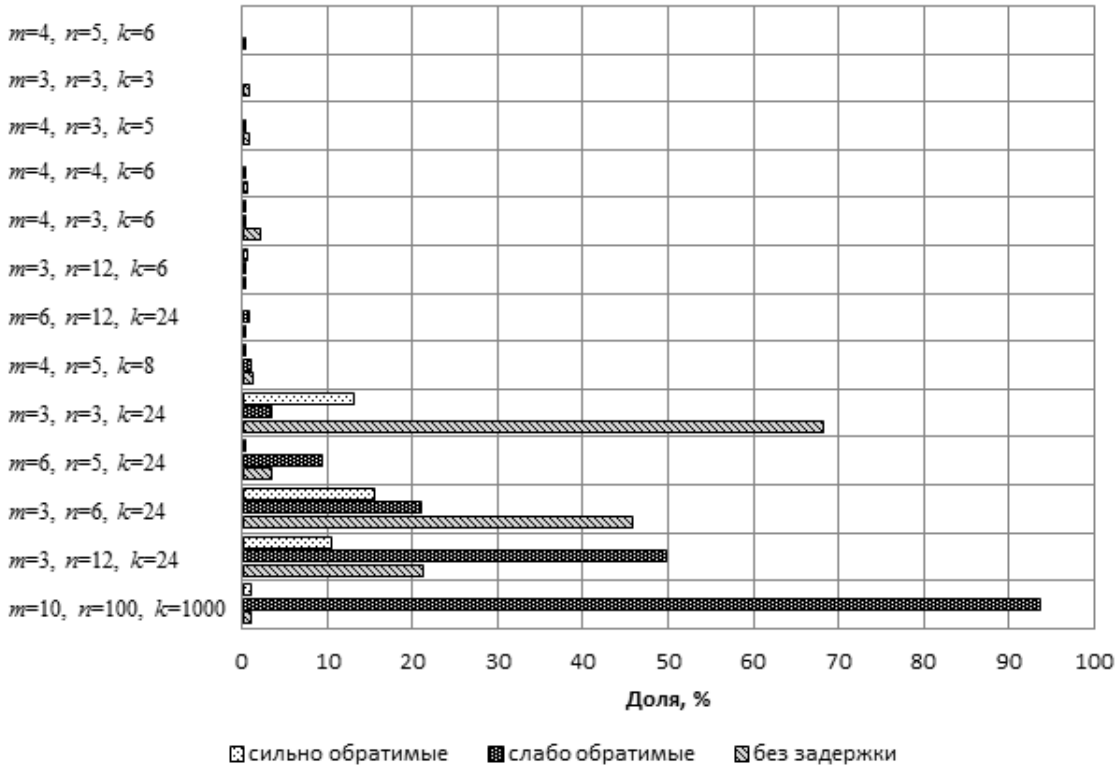

Рис. 1. Доля обратимых автоматов

ЛИТЕРАТУРА

1. *Богаченко Н. Ф.* Применение теоретико-автоматных моделей в криптографии // Математические структуры и моделирование. 2007. Вып. 17. С. 112–120.
2. *Tao R. J.* Finite automata and application to cryptography. Tsinghua: Springer, 2008.

УДК 004.056.55

РЕАЛИЗАЦИЯ НА ПЛИС СИММЕТРИЧНОГО АНАЛОГА FAPKC

Д. С. Ковалев

Рассмотрена реализация на ПЛИС симметричного аналога конечно-автоматной шифрсистемы с открытым ключом (FAPKC). Проведено сравнение ресурсоёмкости и производительности аппаратных реализаций симметричного аналога FAPKC с другими автоматными шифрсистемами. Представлены результаты сравнения ПЛИС-реализаций симметричного аналога FAPKC, AES и других современных блочных шифров.

Ключевые слова: *нелинейный автомат, обратимый с задержкой автомат, конечно-автоматная криптосистема, FAPKC, FASKC, ПЛИС, FPGA, VHDL.*

Данная работа продолжает начатые в [1, 2] исследования конечно-автоматных шифрсистем на пригодность к практическому использованию. Предметом текущего исследования является симметричный аналог конечно-автоматной шифрсистемы с открытым ключом (FAPKC). Критерием оценки пригодности шифра к использованию на пратике в данной работе является эффективность его реализации на базе ПЛИС (программируемая логическая интегральная схема).

Идея построения симметричной криптосистемы на основе нелинейных обратимых с задержкой автоматов [3] была предложена в [4]. В симметричном аналоге FAPKC (далее предлагается использовать аббревиатуру FASKC — Finite Automata Single Key Cryptosystem) используются обратимые с задержкой автоматы, т. е. такие автоматы, у которых входное слово восстанавливается по выходному с задержкой на несколько тактов работы, а также автоматы с конечной памятью, значение выходного символа для которых зависит от значений конечного количества входных и выходных символов в предыдущие такты работы. Ключ шифрования состоит из двух обратимых нелинейных автоматов A и B (с небольшой задержкой τ_1 и τ_2 соответственно), обратные к которым могут быть построены с полиномиальной сложностью.

При шифровании к открытому тексту добавляются произвольные $\tau_1 + \tau_2$ символов. После этого находится реакция α автомата A в выбранном начальном состоянии на «расширенный» открытый текст. Шифртекст есть реакция автомата B в выбранном начальном состоянии на входное слово α. Таким образом, длина шифртекста, по сравнению с открытым текстом, увеличивается на $\tau_1 + \tau_2$ символов. При расшифровании сначала находится реакция β автомата, обратного к B, в его начальном состоянии на зашифрованное слово. Исходный открытый текст получается как реакция автомата, обратного к A, в его начальном состоянии на входное слово β, при этом начальные $\tau_1 + \tau_2$ символов отбрасываются. Таким образом, процедуры расшифрования FAPKC и FASKC совпадают.

Криптосистема FASKC описана на языке VHDL и промоделирована в САПР Xilinx WebPack ISE 14.1 на ПЛИС семейств Spartan-3 и Virtex-2. В табл. 1 представлены результаты реализации на Spartan-3 XC3S1000 процедур шифрования и расшифрования криптосистем FAPKC и FASKC. Видно, что процедура шифрования FASKC несколько уступает процедуре шифрования FAPKC как в плане ресурсоёмкости, так и в плане скорости преобразования открытого текста в шифртекст. При этом общая для этих криптосистем процедура расшифрования хотя и использует большее число ресурсов, имеет более высокую производительность.

Таблица 1

Сравнение ПЛИС-реализаций FAPKC и FASKC

Процедура	Ресурсоёмкость, Slices (S)	Производительность, Мбит/с (T)	T/S
Шифрование (FAPKC)	3968	294	0,07
Шифрование (FASKC)	4074	252	0,06
Расшифрование	5549	309	0,05

В табл. 2 представлены результаты реализации FASKC на Spartan-3 XA3S1000 и автоматной шифрсистемы Закревского [5] на Spartan-3 XAS400 [6]; производительность FASKC сравнима с производительностью шифра Закревского, в то время как последний имеет в несколько раз меньшую ресурсоёмкость.

Одним из методов изучения эффективности реализации шифрсистем является сравнение исследуемого шифра с криптоалгоритмами, используемыми на практике. В табл. 3 сравниваются реализации FASKC и AES на ПЛИС Spartan-3 и Virtex-2. Результаты реализации AES взяты из работы [7].

Из табл. 3 следует, что хотя FASKC и имеет более высокую производительность, чем AES, ресурсоёмкость последнего меньше в десятки раз. К аналогичным выводам можно прийти, сравнивая FASKC с другими современными блочными шифрами

Таблица 2

Сравнение ПЛИС-реализаций FASKC и шифра Закревского

Шифр	Ресурсоёмкость, Slices (S)	Производительность, Мбит/с (T)	T/S
FASKC (E)	4074	252	0,06
FASKC (D)	5549	309	0,05
Шифр Закревского	1715	290	0,16

Таблица 3

Сравнение ПЛИС-реализаций FASKC и AES

Шифр	ПЛИС	Ресурсоёмкость, Slices (S)	Производительность, Мбит/с (T)	T/S
FASKC (E)	XC3S1000-4	4074	252	0,06
FASKC (D)	XC3S1000-4	5549	309	0,05
AES	XC3S50-4	163	208	1,28
FASKC (E)	XC2V1000-6	4082	368	0,09
FASKC (D)	XC2V1000-6	5549	546	0,10
AES	XC2V40-6	146	358	2,45

(3DES, IDEA, CAST), реализованными в [8]. В целом, проведённые исследования показывают, что использование аппаратной реализации симметричного аналога FAPKC на практике допустимо, однако возможно не на всех ПЛИС в силу высокой ресурсоёмкости шифрсистемы.

ЛИТЕРАТУРА

1. *Ковалев Д. С., Тренькаев В. Н.* Реализация на ПЛИС шифра FAPKC // Прикладная дискретная математика. Приложение. 2011. № 4. С. 33–34.
2. *Ковалев Д. С.* Реализация на ПЛИС шифра FAPKC-4 // Прикладная дискретная математика. Приложение. 2012. № 5. С. 44–46.
3. *Tao R. J.* Finite automata and application to cryptography. Tsinghua University Press and Springer, 2008.
4. *Abubaker S.* Lightweight and secure cryptosystems based on finite automata. Электронные данные. Режим доступа: `http://webdocs.cs.ualberta.ca/~vogt/networks/3-2-Abubaker.pdf`, свободный.
5. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
6. *Милошенко А. В.* Аппаратная реализация шифрсистемы, основанной на автомате Закревского // Прикладная дискретная математика. Приложение. 2010. № 3. С. 23–24.
7. *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.
8. *Kitsos P., Sklavos N., Galanis M. D., and Koufopavlou O.* 64-bit Block ciphers: hardware implementations and comparison analysis // Comput. Electric. Eng. 2004. No. 30. P. 593–604.