2. *Wang X., Lai X., Feng D., et al.* Cryptanalysis of the hash functions MD4 and RIPEMD // EUROCRYPT-2005. LNCS. 2005. V. 3494. P. 1–18.
3. *Ермолаева Е. З., Карпунин Г. А.* Оценки сложности поиска коллизий для хэш-функции RIPEMD // Прикладная дискретная математика. Приложение. 2012. № 5. С. 43–44.

УДК 519.713

ОБ ОБРАТИМОСТИ КОНЕЧНЫХ АВТОМАТОВ С КОНЕЧНОЙ ЗАДЕРЖКОЙ

Д. А. Катеринский

Построены экспериментальные оценки доли обратимых, слабо обратимых и сильно обратимых конечных автоматов с конечной задержкой, из которых следует, что эта доля мала (до 3 %) для автоматов с близкими мощностями их алфавитов состояний и выходных символов и велика (более 80 %) для автоматов, у которых выходной алфавит в 4 раза мощнее входного и в 2 раза — внутреннего.

Ключевые слова: *конечные автоматы, слабая обратимость, обратимость, анализ обратимости, синтез обратных автоматов, доля обратимых автоматов.*

Рассмотрены автоматы, обратимые с нулевой задержкой, и автоматы, слабо или сильно обратимые с конечной задержкой. В первых функция выходов инъективна в каждом состоянии, во вторых входная последовательность восстанавливается с задержкой по выходной последовательности и начальному состоянию, а в третьих — только по выходной последовательности. Для каждого типа обратимости известны тест обратимости и алгоритм построения обратного автомата [1, 2].

В работе сообщается о программной реализации этих тестов и алгоритмов и об экспериментальных оценках доли обратимых автоматов всех типов. Полученные оценки приведены на рис. 1, где на оси абсцисс отмечена доля обратимых автоматов, на оси ординат — значения параметров автоматов, для которых проводилось исследование: m, n и k — мощности соответственно входного, внутреннего и выходного алфавитов автомата. В каждой точке оценки построены усреднением результатов вычислений для 10^4 примеров случайных автоматов. Результаты для доли обратимых автоматов с нулевой задержкой совпадают с теоретическими, вычисленными по формуле

$$d = \frac{(C_k^m \cdot m!)^n}{k^{mn}}.$$

Из рис. 1 видно, что:

1) доля обратимых автоматов мала (менее 3 %), если мощности входного, внутреннего и выходного алфавитов близки друг к другу или мощности внутреннего и выходного алфавитов меньше мощности входного алфавита;

2) доля обратимых автоматов высока (более 80 %), если мощность выходного алфавита много больше (более чем в 4 раза) мощности входного алфавита и больше (хотя бы в 2 раза) мощности внутреннего алфавита.

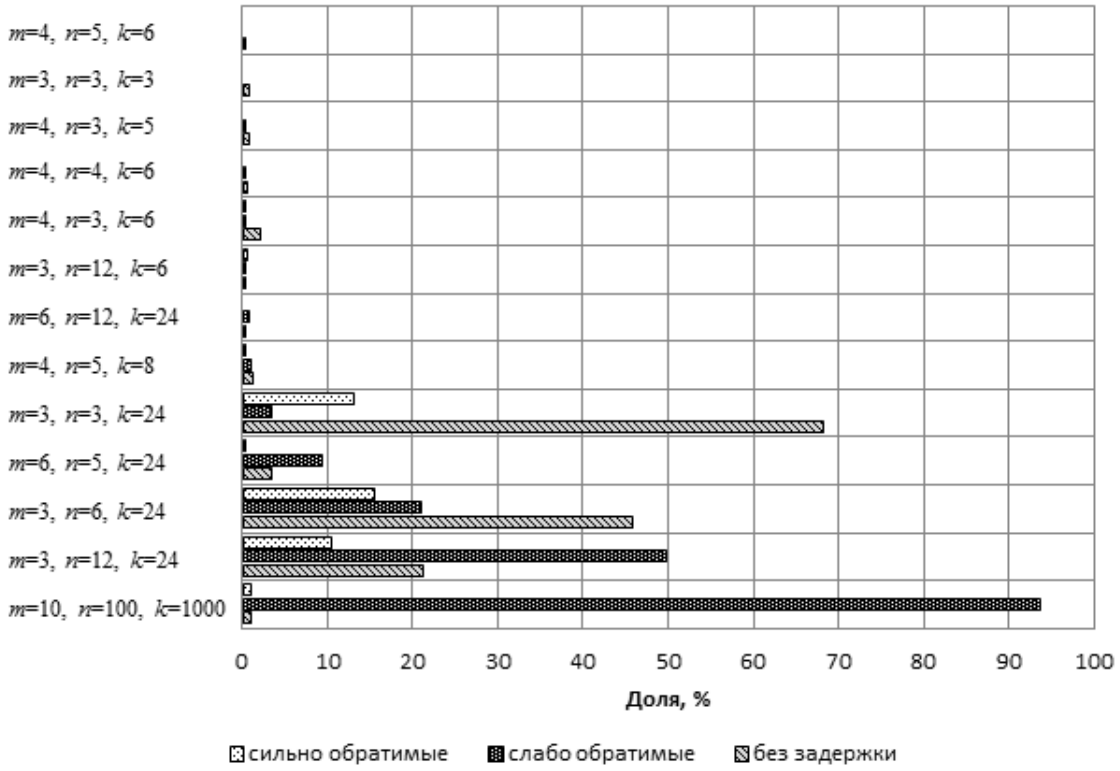

Рис. 1. Доля обратимых автоматов

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).