ЛИТЕРАТУРА

1. *Biryukov A., Shamir A.* Real Time Cryptanalysis of the Alleged A5/1 on a PC // Preproc. FSE' 7. 2000. P. 1–18.

УДК 004.056.55

АППАРАТНАЯ РЕАЛИЗАЦИЯ ШИФРСИСТЕМЫ, ОСНОВАННОЙ НА АВТОМАТЕ ЗАКРЕВСКОГО[1]

А. В. Милошенко

На сегодняшний день встречается мало примеров использования конечных автоматов в качестве аппаратных шифраторов. Разработан прототип шифрсистемы, построенной на базе автомата Закревского [1] с заданными свойствами, в виде программно-аппаратного комплекса. Программная часть комплекса включает в себя генератор шифрующих автоматов и генератор ключей (подмножество переходов автомата), а также транслятор с табличного задания абстрактного автомата на язык описания аппаратуры VHDL. Аппаратную часть комплекса составляет ПЛИС (программируемая логическая интегральная схема), программирование которой осуществляется с помощью САПР Xilinx ISE. В ходе экспериментов выявлен оптимальный способ кодирования состояний автомата.

Для описания автоматной шифрсистемы потребуются следующие определения.

Определение 1. Конечным автоматом A называется пятерка (S, X, Y, ψ, φ), где S — конечное непустое множество состояний; X и Y — конечные входной и выходной алфавиты соответственно, причем далее считается, что $|X| = |Y|$; $\psi : S \times X \to S$ и $\varphi : S \times X \to Y$ — функции переходов и выходов соответственно.

Определение 2. Автомат A является автоматом с биективной функцией выходов, если для любого $s \in S$ функция $\varphi_s(x) = \varphi(s, x)$ определяет взаимно однозначное отображение X на Y. Автоматом Закревского будем называть сильносвязный конечный автомат с биективной функцией выходов.

Если функции ψ и φ определены для всех пар $(s, x) \in S \times X$, то автомат A называется полностью определенным, иначе частичным. Таким образом, полностью определенный автомат A при фиксированном состоянии s реализует отображение f_s множества входных слов X^* на множество выходных слов Y^*. Известно [2], что для полностью определенного автомата A, реализующего $\{f_s : s \in S\}$, существует обратный автомат A^{-1}, который реализует $\{f_s^{-1} : s \in S\}$, если A есть автомат Закревского (АЗ).

Определение 3. Шифрсистема на базе АЗ — шифрсистема, в которой АЗ A используется для шифрования, а обратный автомат A^{-1} — для расшифрования. Считается, что у АЗ A функция переходов ψ является частичной. Произвольное доопределение функции ψ вместе с начальным состоянием являются ключом шифрсистемы.

Ясно, что количество возможных ключей шифрсистемы на базе АЗ равно $|S| \cdot |S|^n$, где n — количество пар (s, x), на которых функция ψ не определена.

Очевидно, что не все АЗ следует использовать в качестве шифратора. Определим требуемые свойства шифрующего автомата Закревского:

1) случайность — равномерное и случайное распределение значений функций ψ и φ;

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

2) минимальность — не существует автомата с меньшим числом состояний, эквивалентного исходному.

Реализация автоматной шифрсистемы на базе ПЛИС проходит в несколько этапов (рис. 1).

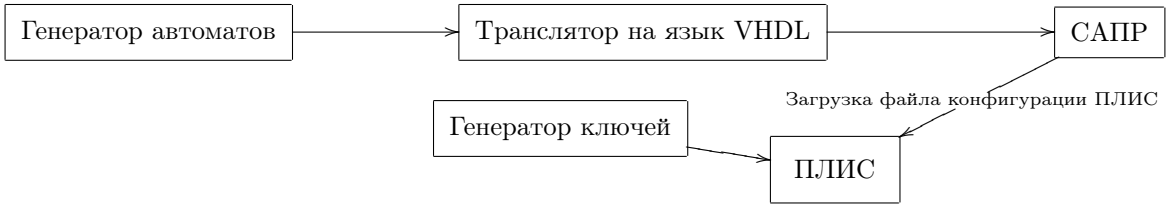

Рис. 1. Этапы реализации автоматной шифрсистемы на базе ПЛИС

Генераторы автоматов и ключей, а также транслятор с табличного описания автомата на язык VHDL реализованы программно. Генератор автоматов строит таблицу переходов и выходов (ТПВ) частичного автомата Закревского с заданным n. При этом сильносвязность достигается построением случайного цикла по всем состояниям в графе переходов автомата, минимальность — генерированием разных столбцов в таблице выходов автомата, случайность — использованием генератора псевдослучайных чисел на основе простых чисел Мерсенна.

Транслятор по ТПВ частичного автомата генерирует VHDL-код шифратора. Далее на основе полученного VHDL-кода с помощью САПР Xilinx ISE программируется ПЛИС. Также с помощью генератора ключей можно получить псевдослучайный ключ. При этом передача ключа осуществляется через входную шину данных ПЛИС, после чего ключ хранится в памяти шифратора на протяжении всего сеанса шифрования.

Проведены эксперименты по реализации АЗ на ПЛИС Spartan3 XA3S400 с различным количеством входных (выходных) символов и состояний, а также при разных встроенных в САПР Xilinx ISE способах кодирования состояний. Оказалось, что лучшим способом кодирования (с точки зрения утилизации ресурсов микросхемы и быстродействия) для данной задачи является метод One-Hot, когда каждое состояние кодируется булевым вектором длины $|S|$, в котором только одна компонента равна единице. В частности, для автомата Закревского с $|X| = |Y| = 32$ и $|S| = 100$ количество используемых Slice составило 1715 (или 429 CLB), т. е. 47 % от возможного. При этом максимально возможная частота работы ПЛИС равна 58 МГц, т. е. максимальная скорость работы достигает 290 Мбит/с. Таким образом, наши результаты сравнимы с результатами из [3] по реализации на ПЛИС известных блочных шифров (TripleDES, IDEA и др.).

ЛИТЕРАТУРА

1. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.
2. *Тренькаев В. Н., Колесников Р. Г.* Автоматный подход к атакам на симметричные шифры // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 130–135.
3. *Kitsos P., Sklavos N., Galanis M. D., Koufopavlou O.* 64-bit Block ciphers: hardware implementations and comparison analysis // Computers and Electrical Engineering. 2004. No. 30. P. 593–604.