НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н. Э. БАУМАНА
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408
электронный научно-технический журнал

Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах

 # 10, октябрь 2013
DOI:

Ключарёв П. Г.

УДК 004.056.55

Россия, МГТУ им. Н.Э. Баумана
pk.iu8@yandex.ru

Введение

В настоящее время активно развивается так называемая легковесная криптография (light-weight cryptography). Под этим термином подразумевается раздел криптографии, занимающийся криптографическими алгоритмами, которые могут быть эффективно реализованы на вычислительных устройствах с ограниченными ресурсами. Легковесной криптографии посвящено большое количество литературы, обзоры которой можно найти в работах [18, 28, 33].

В работе [1] автором было предложено использовать обобщенные клеточные автоматы и графы Рамануджана для синтеза поточных шифров. В дальнейшем теоретические основы этого были разработаны в статьях [1, 2, 4, 5] и была высказана гипотеза о том, что такие шифры могут быть эффективно реализованы аппаратно. Цель настоящей статьи состоит в подтверждении этой гипотезы. В настоящей статье мы приводим результаты измерения быстродействия и эффективности аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах (мы будем называть семейство таких шифров GRACE-S). В качестве платформы для реализации используются ПЛИС фирмы Altera. Производится также сравнение быстродействия и эффективности реализации этих шифров с аналогами.

Полученные результаты показывают, что семейство GRACE-S имеет производительность значительно (до 60 раз) превышающую производительность лучших аналогов.

1. Термины и определения

В этом разделе мы введем основные определения теории обобщенных клеточных автоматов, являющейся основой для рассматриваемых поточных шифров.

Назовем *обобщенным клеточным автоматом* ориентированный мультиграф $A = (V, E)$ (здесь $V = \{v_1, \ldots, v_N\}$ — множество вершин, E — мультимножество ребер). С каждой его

вершиной v_i ассоциированы: булева переменная m_i, называемая *ячейкой*, и булева функция $f_i(x_1, \ldots, x_{d_i})$, называемая локальной функцией связи i-й вершины. При этом для каждой вершины v_i входящие в нее ребра пронумерованы числами $1, \ldots, d_i$.

Обобщенный клеточный автомат работает следующим образом. В начальный момент времени каждая ячейка памяти m_i, $i = 1, \ldots, N$, имеет некоторое начальное значение $m_i(0)$. Далее автомат работает по шагам. На шаге с номером t посредством локальной функции связи вычисляются новые значения ячеек:

$$m_i(t) = f_i(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \ldots, m_{\eta(i,d_i)}(t-1)), \tag{1}$$

где $\eta(i, j)$ — номер вершины, из которой исходит ребро, входящее в вершину i и имеющее номер j. *Заполнением* клеточного автомата $M(t)$ на шаге t будем называть набор значений ячеек $(m_1(t), m_2(t), \ldots, m_N(t))$.

Назовем *однородным обобщенным клеточным автоматом* обобщенный клеточный автомат, у которого локальная функция связи для всех ячеек одинакова и равна f, т.е. для любого $i \in \{1, \ldots, N\}$ выполняется $f_i = f$. Степени захода вершин такого клеточного автомата, очевидно, одинаковы: $d_1 = d_2 = \ldots = d_N = d$.

Назовем обобщенный клеточный автомат *неориентированным*, если для любого ребра (u, v) в его графе существует и ребро (v, u). Граф такого автомата можно рассматривать как неориентированный регулярный граф, если заменить каждую пару ребер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$. Далее мы будем использовать только неориентированные однородные обобщенные клеточные автоматы, для краткости называя их просто обобщенными клеточными автоматами.

Пусть задана двоичная последовательность $\{\xi_t\}$. Назовем *обобщенным клеточным автоматом с задающей последовательностью* обобщенный клеточный автомат, у которого для вычисления одной из ячеек m_r (будем ее называть задающей ячейкой), вместо формулы (1) используется формула

$$m_r(t) = f_r\big(m_{\eta(r,1)}(t-1), m_{\eta(r,2)}(t-1), \ldots, m_{\eta(r,d_r)}(t-1)\big) \oplus \xi_t.$$

Некоторый набор ячеек клеточного автомата будем называть *выходом*. Число ячеек в этом наборе будем называть *длиной выхода* или *длиной выходного слова*. Ячейки, не входящие в выход назовем *скрытыми*. *Выходной последовательностью* клеточного автомата назовем функцию, аргументом которой является номер шага, а значением — значение выхода на этом шаге.

Для криптостойкости шифра большое значение имеет выбор графа обобщенного клеточного автомата. Согласно работе [6], хорошим выбором являются графы Рамануджана [15, 24, 26]. В данной работе используются так называемые графы Любоцкого — Филипса — Сарнака семейства $Y^{p,q}$. Обсуждение этих графов выходит далеко за рамки настоящей работы. Их подробное описание можно найти, например в работах [25, 26, 30]. Автором они рассматриваются в статьях [1, 2, 3, 6].

Кроме того, весьма важным является правильный выбор локальной функции связи обобщенного клеточного автомата. В работах [4, 5] сформулированы основные принципы выбора таких функций и построено семейство функций, отвечающее этим требованиям. В частности, локальная функция связи должна быть равновесной, шефферовой, а ее нелинейность (т.е. расстояние от этой функции до множества аффинных булевых функций) — как можно более высокой.

Семейство функций, удовлетворяющих всем необходимым требованиям построено в работе [5]. В частности, в случае четного числа переменных используется функция

$$\begin{aligned} g_2(v,u,x_1,y_1,\ldots,x_k,y_k) = \\ = (1\oplus v)(\beta_1(x_1,y_1,\ldots,x_k,y_k)\oplus u)\oplus v(\beta_3(x_1,y_1,\ldots,x_k,y_k)\oplus u) = \\ = \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1,\ldots,x_k)\oplus v(s_1(x_1,\ldots,x_k)\oplus s_3(x_1,\ldots,x_k))\oplus u, \end{aligned} \quad (2)$$

где $s_1(x_1,\ldots,x_k)$ и $s_3(x_1,\ldots,x_k)$ — произвольные булевы функции, причем $k+t_3 = 1 \pmod 2$, где t_3 — число ненулевых коэффициентов в алгебраической нормальной форме функции s_3, и свободный член АНФ функции s_1 равен 1.

В данной работе используются локальные функции связи от шести переменных. Следует отметить, что такая функция от шести переменных, имеющая вид (2), может быть представлена в виде суперпозиции двух четырехместных булевых функций. Более подробно это показано ниже.

2. Конструкция поточного шифра

Опишем здесь рассматриваемое семейство поточных шифров GRACE-S (ему также посвящены другие работы автора, например, [1, 2, 4, 5]). Семейство основано на обобщенных клеточных автоматах. Использованию клеточных автоматов в криптографии посвящен ряд работ, в том числе [1, 8].

Поточный шифр представляет собой генератор гаммы и состоит (рис. 1) из двух обобщенных клеточных автоматов с задающей последовательностью CA_1 и CA_2 и линейного регистра сдвига с обратной связью (LFSR). Автоматы имеют разный размер и различные локальные функции связи: f_1 и f_2. Задающей ячейкой является одна из скрытых ячеек каждого из этих автоматов, а задающей последовательностью является выходная последовательность регистра сдвига. При этом число выходных ячеек обоих автоматов должно быть одинаковым. Генератор работает пошагово. На каждом шаге выходом генератора гаммы является поразрядная сумма по модулю два выходов автоматов. При этом на выходе генератора гаммы на каждом шаге формируется слово (будем называть его *выходным словом*), длина которого равна длине выхода каждого автомата. Гамма является конкатенацией выходных слов на каждом шаге.

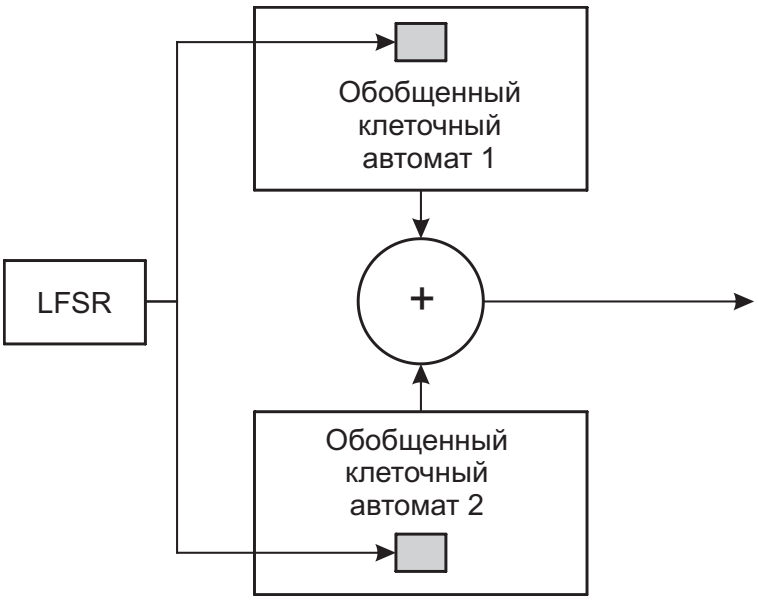

Рис. 1. Структура генератора гаммы

Криптографический ключ может иметь любую длину, меньшую числа ячеек каждого клеточного автомата не менее, чем в полтора раза. При этом, длина LFSR должна быть равна длине ключа, а характеристический многочлен LFSR должен быть неприводимым.

Начальным заполнением каждого клеточного автомата является ключ, конкатенированный с некоторой константой, дополняющей ключ до размера автомата (т.е. числа ячеек). Эта константа должна иметь приблизительно одинаковое количество единиц и нулей. Ключ является также начальным заполнением регистра сдвига.

Шифрование, производится путем поразрядного сложения открытого текста с гаммой по модулю два. Расшифрование производится аналогично.

Обозначим заполнение клеточного автомата CA на шаге t как $CA(t, M_0, \xi)$, где M_0 — начальное заполнение, а ξ — задающая последовательность. Выход клеточного автомата обозначим $pr_m(CA(t, M_0, \xi))$, где m — длина выхода, а pr_r — функция, возвращающая некоторые r разрядов аргумента (имеющие наперед заданные номера).

Обозначим через $LFSR(L_0)$ последовательность, порождаемую линейным регистром сдвига, здесь L_0 — его начальное заполнение.

Таким образом, выход генератора гаммы на шаге t вычисляется по формуле

$$y(t, key) = CA_1(t, key||c_1, LFSR(key)) \oplus CA_2(t, key||c_2, LFSR(key)),$$

где CA_1 и CA_2 — два обобщенных клеточных автомата с задающей последовательностью; $\oplus$ — поразрядное сложение по модулю два; c_1 и c_2 — константы, дополняющие ключ до размера клеточного автомата. Вес этих констант должен быть близок к половине длины; $||$ — операция конкатенации двоичных векторов.

Вырабатываемая генератором гамма представляет собой конкатенацию выходов, причем после начала работы автомата делается несколько холостых шагов:

$$\gamma = y(\tau + 1, key)||y(\tau + 2, key)|| \ldots,$$

где τ — число холостых шагов.

Эксперименты показали, что число холостых шагов должно быть пропорционально диаметру. Поэтому в случае использования графов Рамануджана $\tau = \Omega(\log n)$, где n — размер большего клеточного автомата. Экспериментально показано, что на практике число холостых шагов должно быть не менее чем $2D$, где D — диаметр графа.

3. Реализация на ПЛИС и производительность

Программируемая логическая интегральная схема (ПЛИС) реализует набор однотипных реконфигурируемых ячеек. В процессе программирования ПЛИС определяется конфигурация каждой такой ячейки, а также связи между ними. С помощью ПЛИС можно реализовать практически любую цифровую схему. Описание цифровых схем осуществляется посредством специальных языков, наиболее известными из которых являются VHDL и Verilog. В настоящей работе в качестве платформы были выбраны ПЛИС фирмы Altera, а в качестве языка описания — язык VHDL.

Поскольку требовалось провести тестирование производительности шифров из семейства GRACE-S при различных параметрах, был разработан комплекс программ, позволяющий генерировать VHDL-файл, реализующий шифр из семейства GRACE-S, заданный входными параметрами, такими как графы клеточных автоматов, локальные функции связи, количество выходных ячеек и др. Комплекс программ был реализован на языке C#. Параметры задавались с помощью XML-файла. Для компиляции VHDL-файла и моделирования использовались САПР Altera Quartus II 12.0 и САПР Altera ModelSim Starter Edition 10.0d.

Основой архитектуры ПЛИС Altera являются модули адаптивной логики (Adaptive Logic Module, ALM). ПЛИС состоит из большого количества таких модулей. Каждый ALM состоит из элемента комбинаторной логики, двух регистров и двух сумматоров. С помощью элемента комбинаторной логики можно реализовать булеву функцию. Причем, младшие модели ПЛИС (семейство Cyclone) позволяют реализовать в каждом ALM произвольную булеву функцию от четырех переменных, в то время как старшие модели (семейства Arria и Stratix) — произвольную булеву функцию от шести переменных. Поэтому для обеспечения высокой эффективности, локальная функция связи обобщенных клеточных автоматов должна зависеть не более чем от шести переменных и должна допускать возможность реализации с помощью наименьшего числа функций, зависящих от четырех переменных. Выбранное семейство функций удовлетворяет этим требованиям.

Действительно, функцию (2) можно представить в виде суперпозиции следующих двух функций зависящих от меньшего числа переменных:

$$g_{21}(u, x_1, y_1, \ldots, x_{k-\rho}, y_{k-\rho}, t) = \bigoplus_{i=1}^{k-\rho} x_i y_i \oplus u \oplus t;$$

$$g_{22}(v, x_1, \ldots, x_k, y_{k-\rho+1}, \ldots, y_k) =$$

$$= \bigoplus_{i=k-\rho+1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus v(s_1(x_1, \ldots, x_k) \oplus s_3(x_1, \ldots, x_k)).$$

Указанная суперпозиция вводится следующим образом:

$$g_2(v, u, x_1, y_1, \ldots, x_k, y_k) = g_{21}(u, x_1, y_1, \ldots, x_{k-\rho}, y_{k-\rho}, g_{22}(v, x_1, \ldots, x_k, y_{k-\rho+1}, \ldots, y_k)).$$

Всего функция g_2 имеет $d = 2k + 2$ аргументов. Функция g_{21} имеет $2(k - \rho)$ аргументов, а функция g_{22} имеет $k + \rho + 1$ аргумент. При ρ близком к $(k + 1)/3 = n/6$ у функций g_{21} и g_{22} будет приблизительно поровну аргументов. В частности, при $d = 6$ и $\rho = 1$ эти две функции имеют по четыре аргумента, т.е. шестиместная локальная функция связи данного вида может быть представлена в виде суперпозиции двух четырехместных функций.

Было проведено исследование производительности при различных значениях параметров (табл. 1) на различных ПЛИС фирмы Altera (Cyclone II, Cyclone V, Arria II GX, Arria V, Stratix III, Stratix V). Для ПЛИС Cyclone II и Stratix V была проверена работа на физической ПЛИС, с помощью соответствующих отладочных плат с внешним тактовым генератором.

Таблица 1

Параметры протестированных шифров из семейства GRACE-S

No п/п	Кол-во ячеек клеточного автомата № 1	Кол-во ячеек клеточного автомата № 2	Кол-во выходных ячеек	Длина ключа
1	230	242	128	128
2	390	402	256	128
3	770	810	512	128
4	1182	1202	768	128
5	1550	1602	1024	128
6	2310	2342	1536	128
7	3090	3110	2048	128
8	4622	4650	3072	128
9	230	242	128	256
10	390	402	256	256
11	770	810	512	256
12	1182	1202	768	256
13	1550	1602	1024	256
14	2310	2342	1536	256
15	3090	3110	2048	256
16	4622	4650	3072	256

Данные по быстродействию, максимальной тактовой частоте и эффективности реализации приведены на рис. 2, 3, 4. Здесь под эффективностью аппаратной реализации понимается отношению быстродействия к количеству аппаратных ресурсов. Для рассматриваемых ПЛИС единицей аппаратных ресурсов является логический элемент — LE.

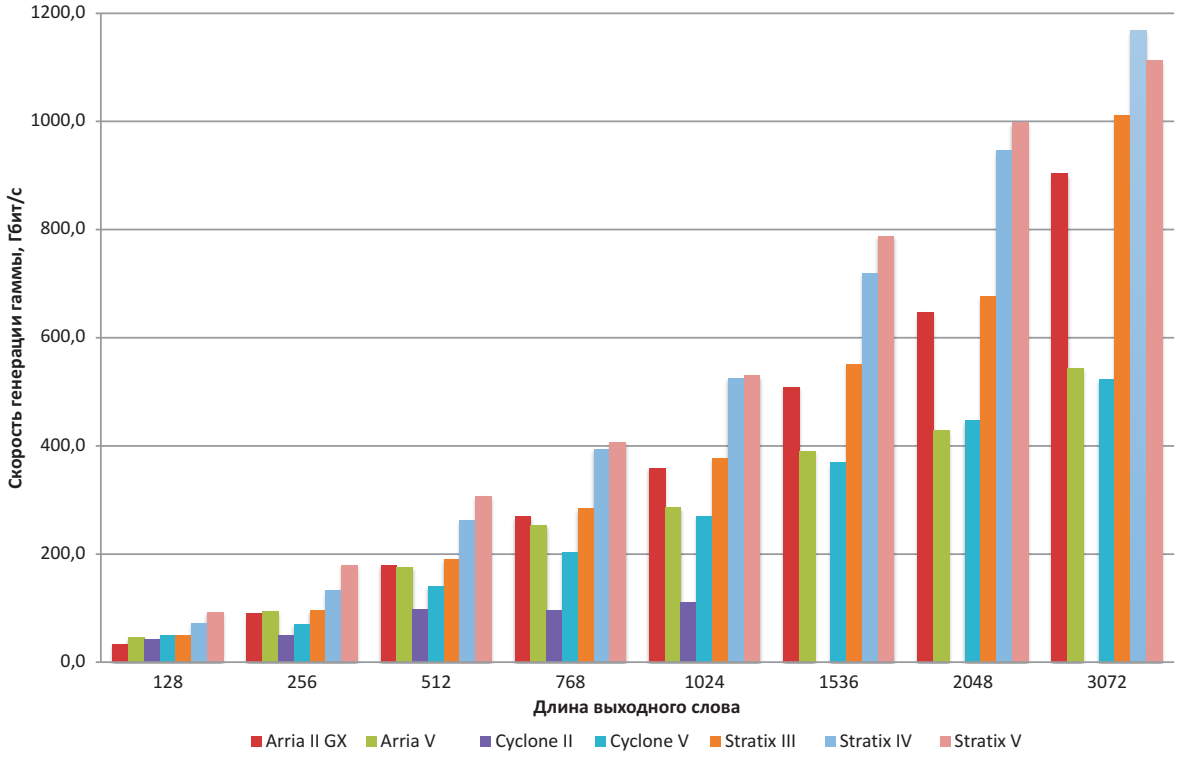

Рис. 2. Скорость генерации гаммы

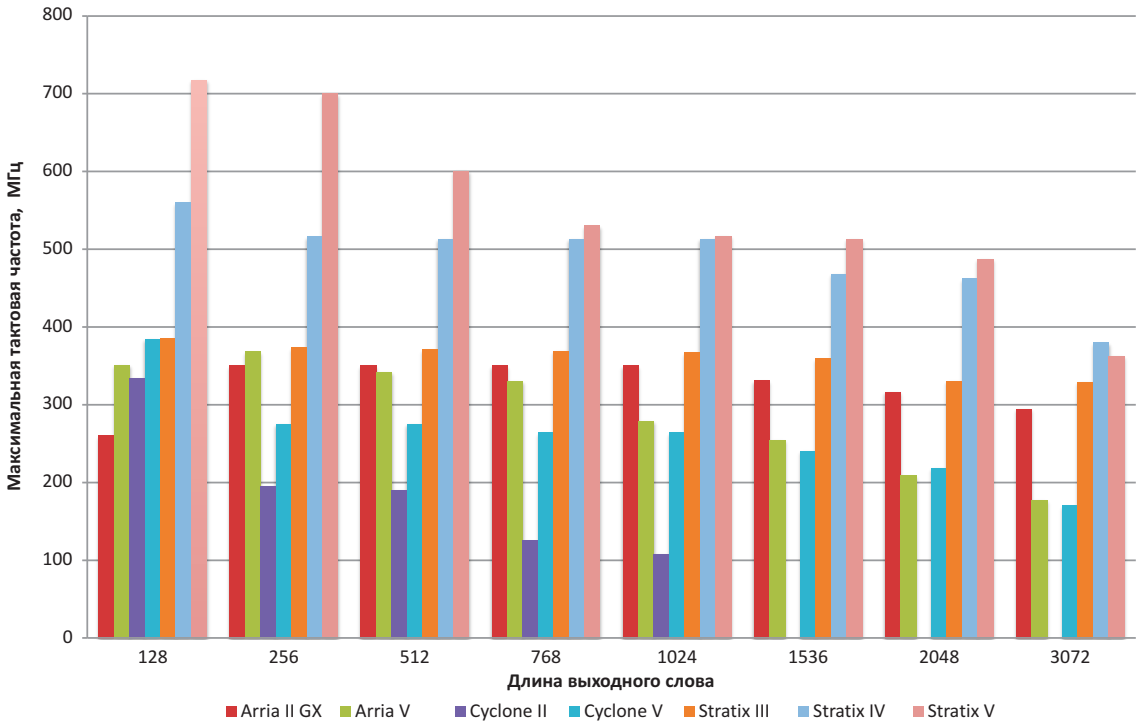

Рис. 3. Максимальная тактовая частота

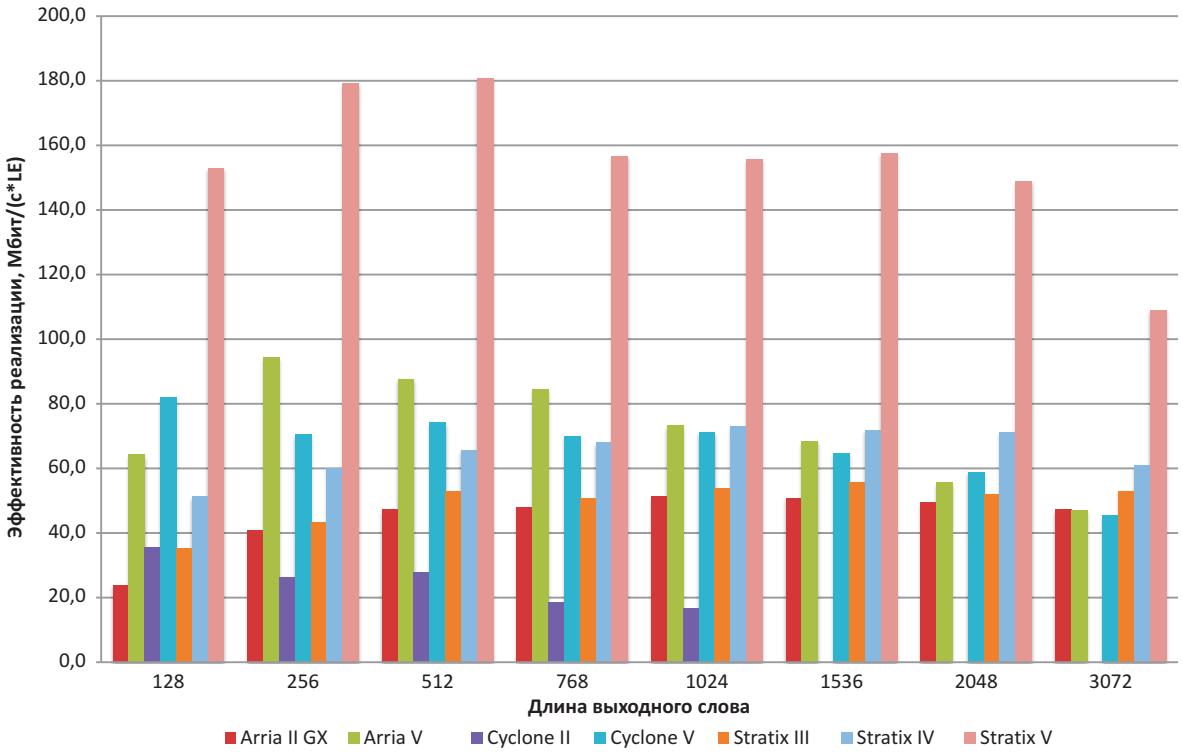

Рис. 4. Эффективность реализации

4. Сравнение параметров эффективности и быстродействия семейства криптоалгоритмов GRACE-S с существующими аналогами при аппаратной реализации

Сравнение проводилось с поточными криптоалгоритмами, представленными на европейский конкурс eSTREAM, проводившийся в 2005–2008 гг., который был направлен на поиск криптостойких поточных шифров. Данные о быстродействии реализаций алгоритмов получены из работы [22]. Методика сравнения аналогична используемой в статье [7].

Сравнение быстродействия (т.е. скорости выработки гаммы) проводилось по двум показателям: быстродействие на максимальной тактовой частоте и быстродействие на тактовой частоте 100 МГц. Сравнение производилась с криптоалгоритмами AES (в режиме OFB) [14], Achterbahn [19, 20], Grain [21, 23, 32], MICKEY [9, 10, 11, 12], MOSQUITO [13], SFINKS+ [31], Trivium [16, 17], VEST [27], ZK-Crypt [34].

Данные приведены в табл. 2. Отражены данные для семейства GRACE-S с различной длиной выходного слова (256, 1024, 3072) и при реализации на наиболее характерных ПЛИС фирмы Altera: Stratix V, как наиболее быстродействующей, и Cyclone II, как наиболее дешевой. Из табл. 2 видно, что быстродействие при реализации на Stratix V в 60 раз превышает быстродействие криптоалгоритма Trivium, имеющего максимальное быстродействие среди алгоритмов, представленных на конкурс eStream.

Сопоставление эффективности аппаратной реализации приведено в табл. 3. Данные по криптоалгоритмам AES, Trivium, MICKEY и Grain приведены в соответствии со статьей [29].

Таблица 2

Быстродействие аппаратных реализаций шифров семейства GRACE-S в сравнении с аналогичными существующими шифрами

Генератор	Макс. тактовая частота, МГц	Быстродействие при макс. тактовой частоте, Гбит/с	Быстродействие при тактовой частоте 100 МГц, Гбит/с
GRACE-S — 256, Cyclone II	195	49	25
GRACE-S — 1024, Cyclone II	108	110	102
GRACE-S — 256, Strarix V	700	179	25
GRACE-S — 1024, Strarix V	517	529	102
GRACE-S — 3072, Strarix V	362	1112	307
AES (OFB)	182	0,52	0,29
Achterbahn	250	0,46	0,18
Grain	300	4,47	1,49
MICKEY	308	0,28	0,93
MOSQUITO	265	0,73	0,27
SFINKS+	167	1,24	0,74
Trivium	312	18,5	5,95
VEST	286	4,25	1,48
ZK-Crypt	203	6,05	2,98

Таблица 3

Эффективность аппаратных реализаций шифров семейства GRACE-S в сравнении с аналогичными существующими шифрами

Генератор	Быстродействие, Мбит/с	Аппаратные ресурсы, тыс. LE	Эффективность, Гбит/(с · LE)
AES	0,61	5	0,12
Grain	3,44	0,5	6,77
MICKEY	0,22	0,5	0,41
Trivium	16,3	0,7	23,3
GRACE-S — 256, Cyclone II	49	1,9	26
GRACE-S — 1024, Cyclone II	110	6,7	16
GRACE-S — 256, Strarix V	179	1	179
GRACE-S — 1024, Strarix V	529	3,4	155
GRACE-S — 3072, Strarix V	1112	10,2	109

Из табл. 3 видно, что эффективность аппаратной реализации алгоритмов GRACE–S в несколько раз превышает эффективность аппаратной реализации лучшего из алгоритмов, представленных на конкурсе eStream.

Заключение

В статье показано, что семейство поточных шифров, основанных на обобщенных клеточных автоматах GRACE-S, допускает высокоэффективную аппаратную реализацию, показывающую скорость, которая в 60 и более раз превышает скорость известных поточных шифров, и эффективность реализации, которая в 7 и более раз превышает эффективность

реализации известных поточных шифров. Кроме того, аппаратные ресурсы, необходимые для реализации шифров из этого семейства, весьма невелики, что позволяет отнести их к легковесным (lightweight) криптоалгоритмам.

Автор благодарит А.В. Дудина за помощь в подготовке материалов для этой статьи.

Работа выполнена при финансовой поддержке РФФИ (грант № 12-07-31012).

Список литературы

1. Ключарёв П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. Электронное научно-техническое издание. 2011. № 10.
2. Ключарёв П.Г. Криптографические свойства клеточных автоматов, основанных на графах Любоцкого — Филипса — Сарнака// Безопасные информационные технологии. Сборник трудов Второй всероссийской научно-технической конференции. М.: НИИ радиоэлектроники и лазерной техники, 2011. С. 163–173.
3. Ключарёв П.Г. Блочные шифры, основанные на обобщенных клеточных автоматах // Наука и образование. Электронное научно-техническое издание. 2012. № 12.
4. Ключарёв П.Г. О периоде обобщенных клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 2.
5. Ключарёв П.Г. Обеспечение криптографических свойств обобщенных клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 3.
6. Ключарёв П.Г. Построение псевдослучайных функций на основе обобщеклеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2012. № 10.
7. Сухинин Б. М. Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование. Электронное научно-техническое издание. 2010. № 9.
8. Сухинин Б.М. О некоторых свойствах клеточных автоматов и их применении в структуре генераторов псевдослучайных последовательностей // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2011. № 2. С. 68–76.
9. Babbage S., Dodd M. The stream cipher mickey (version 1) // ECRYPT Stream Cipher Project Report. 2005. Vol. 15. P. 2005.
10. Babbage S., Dodd M. The stream cipher mickey-128 2.0 // Article for eSTREAM Project. 2006. Avairable at http://www.ecrypt.eu.org/stream/p2ciphers/mickey128/mickey128_p2.pdf.
11. Babbage S., Dodd M. The stream cipher mickey 2.0 // ECRYPT Stream Cipher. 2006. Available at http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3.pdf.
12. Babbage S., Dodd M. The mickey stream ciphers // New Stream Cipher Designs. Springer, 2008. P. 191–209.

13. Daemen J., Kitsos P. The self-synchronizing stream cipher moustique // New Stream Cipher Designs. Springer, 2008. P. 210–223.
14. Daemen J., Rijmen V. The design of Rijndael: AES-the advanced encryption standard. Springer, 2002.
15. Davidoff G., Sarnak P., Valette A. Elementary number theory, group theory and Ramanujan graphs. Cambridge University Press, 2003. Vol. 55.
16. De Canniere C. Trivium: A stream cipher construction inspired by block cipher design principles // Information Security. Springer, 2006. P. 171–186.
17. De Canniere C., Preneel B. Trivium // New Stream Cipher Designs. Springer, 2008. P. 244–266.
18. Eisenbarth T., Kumar S. A survey of lightweight-cryptography implementations // Design & Test of Computers, IEEE. 2007. Vol. 24, no. 6. P. 522–533.
19. Gammel B., Göttfert R., Kniffler O. The achterbahn stream cipher. estream, ecrypt stream cipher project, report 2005/002, 2005.
20. Gammel B., Göttfert R., Kniffler O. Achterbahn-128/80: Design and analysis // ECRYPT Network of Excellence-SASC Workshop Record. 2007. P. 152–165.
21. Hell M., Johansson Th., Maximov A., Meier W. The grain family of stream ciphers // New Stream Cipher Designs. Springer, 2008. P. 179–190.
22. Gurkaynak F., Luethi P., Bernold N. et al. Hardware evaluation of eSTREAM candidates: Achterbahn, Grain, MICKEY, MOSQUITO, SFINKS, Trivium, VEST, zk-crypt. 2006. Available at: http://www.ecrypt.eu.org/stream/papersdir/2006/015.pdf.
23. Hell M., Johansson T., Meier W. Grain: a stream cipher for constrained environments // Int. J. of Wireless and Mobile Computing. 2007. Vol. 2, no. 1. P. 86–93. Available at: http://inderscience.metapress.com/index/j463lh7251257262.pdf.
24. Hoory S., Linial N., Wigderson A. Expander graphs and their applications // Bulletin of the American Mathematical Society. 2006. Vol. 43, no. 4. P. 439–562.
25. Lubotzky A., Phillips R., Sarnak P. Explicit expanders and the ramanujan conjectures // Proceedings of the eighteenth annual ACM symposium on Theory of computing / ACM. 1986. P. 240–246.
26. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs // Combinatorica. 1988. Vol. 8, no. 3. P. 261–277.
27. O'Neil S., Gittins B., Landman H. A. Vest hardware-dedicated stream ciphers // IACR Cryptology ePrint Archive. 2005. Vol. 2005. P. 413. Available at: https://eprint.iacr.org/2005/413.
28. Poschmann A. Y. Lightweight cryptography: Cryptographic engineering for a pervasive world // PH. D. THESIS / Citeseer. 2009. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.1450.

29. Rogawski M. Hardware evaluation of eSTREAM candidates: Grain, Lex, Mickey128, Salsa20 and Trivium. 2007. Available at: http://www.ecrypt.eu.org/stream/papersdir/2007/025.pdf.
30. Sarnak P. Some applications of modular forms. Cambridge University Press, 1990. Vol. 99.
31. Braeken A., Lano J., Mentens N. et al. Sfinks: A synchronous stream cipher for restricted hardware environments // SKEW-Symmetric Key Encryption Workshop. 2005.
32. Hell M., Johansson Th., Maximov A., Meier W. A stream cipher proposal: Grain-128 // Information Theory, 2006 IEEE International Symposium on IEEE. 2006. P. 1614–1618.
33. Yalla P., Kaps J.-P. Lightweight cryptography for fpgas // Reconfigurable Computing and FPGAs, 2009. ReConFig'09. International Conference on IEEE. 2009. P. 225–230.
34. Hecht A., Bard G., Dunkelman O. et al. The zk-crypt algorithm specification. 2007.

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU

SCIENCE and EDUCATION

EL № FS77 - 48211. №0421200025. ISSN 1994-0408

electronic scientific and technical journal

Performance and effectiveness of hardware realization of stream ciphers based on generalized cellular automata

 # 10, October 2013

DOI:

Klyucharev P. G.

Bauman Moscow State Technical University
105005, Moscow, Russian Federation
pk.iu8@yandex.ru

In this article data on performance and effectiveness of the GRACE-S family of stream ciphers based on generalised cellular automata and expander graphs were discussed. Altera FPGA was used as a platform for hardware implementation. The performance of GRACE-S stream ciphers was compared with the performance of stream ciphers that had won the eSTREAM competition. According to the performed tests, the performance of the GRACE-S family of stream ciphers significantly (up to 60 times) exceeds the performance of the best-known stream ciphers.

References

1. Klyucharev P.G. Kletochnye avtomaty, osnovannye na grafakh Ramanudzhana, v zadachakh generatsii psevdosluchaynykh posledovatel'nostey [Cellular automations based on Ramanujan graphs in the field of the generation of pseudorandom sequences]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2011, no. 10. Avilable at: http://technomag.edu.ru/doc/241308.html, accessed 01.09.2013.
2. Klyucharev P.G. Kriptograficheskie svoystva kletochnykh avtomatov, osnovannykh na grafakh Lyubotskogo — Filipsa — Sarnaka [Cryptographic properties of cellular automata based on LPS-graphs]. *Bezopasnye informatsionnye tekhnologii: sb. trudov Vtoroy vserossiyskoy nauchno-tekhnicheskoy konferentsii* [Proc. of the 2nd All-Rus. sci.-tech. conf. "Secure information technologies"]. Moscow, Publication of Research Institute of Radioelectronics and Laser Technology, 2011, pp. 163–173.
3. Klyucharev P.G. Blochnye shifry, osnovannye na obobshchennykh kletochnykh avtomatakh [Construction of pseudo-random functions based on generalized cellular automata]. *Nauka i*

obrazovanie MGTU im. N.E. Baumana [Science and Education of the Bauman MSTU], 2012, no. 12. DOI: 10.7463/0113.0517543.

4. Klyucharev P.G. O periode obobshchennykh kletochnykh avtomatov [About the period of generalized cellular automatons]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 2. Available at: http://technomag.edu.ru/doc/340943.html, accessed 01.09.2013.
5. Klyucharev P.G. Obespechenie kriptograficheskikh svoystv obobshchennykh kletochnykh avtomatov [On cryptographic properties of generalized cellular automatons]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 3. Available at: http://technomag.edu.ru/doc/358973.html, accessed 01.09.2013.
6. Klyucharev P.G. Postroenie psevdosluchaynykh funktsiy na osnove obobshchennykh kletochnykh avtomatov [Construction of pseudorandom functions based on generalized cellular automata]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2012, no. 10. DOI: 10.7463/1112.0496381.
7. Sukhinin B.M. Razrabotka generatorov psevdosluchaynykh dvoichnykh posledovatel'nostey na osnove kletochnykh avtomatov [The Development of Pseudorandom Binary Sequences Generators Based on Cellular Automata]. *Nauka i obrazovanie MGTU im. N.E. Baumana* [Science and Education of the Bauman MSTU], 2010, no. 9. Available at: http://technomag.bmstu.ru/doc/159714.html, accessed 01.09.2013.
8. Sukhinin B.M. O nekotorykh svoystvakh kletochnykh avtomatov i ikh primenenii v strukture generatorov psevdosluchaynykh posledovatel'nostey [Some properties of cellular automata and their application in the structure of pseudorandom sequences generators]. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie* [Herald of the Bauman MSTU. Ser. Instrument Engineering], 2011, no. 2, pp. 68–76.
9. Babbage S., Dodd M. *The stream cipher MICKEY (version 1)*. From: eSTREAM: the ECRYPT Stream Cipher Project. 2005/015, 2005. Available at: http://www.ecrypt.eu.org/stream/ciphers/mickey/mickey.pdf, accessed 01.09.2013.
10. Babbage S., Dodd M. *The stream cipher MICKEY-128 2.0*. From: eSTREAM: the ECRYPT Stream Cipher Project, 2006. Avaiable at: http://www.ecrypt.eu.org/stream/p2ciphers/mickey128/mickey128_p2.pdf, accessed 01.09.2013.
11. Babbage S., Dodd M. *The stream cipher MICKEY 2.0*. From: eSTREAM: the ECRYPT Stream Cipher Project, 2006. Available at: http://www.ecrypt.eu.org/stream/p3ciphers/mickey/mickey_p3.pdf, accessed 01.09.2013.
12. Babbage S., Dodd M. The MICKEY stream ciphers. In: *New Stream Cipher Designs*. Springer, 2008. P. 191–209. (Ser. *Lecture Notes in Computer Science*; vol. 4986). DOI: 10.1007/978-3-540-68351-3_15.

13. Daemen J., Kitsos P. The self-synchronizing stream cipher MOUSTIQUE. In: *New Stream Cipher Designs. Springer*, 2008. P. 210–223. (Ser. *Lecture Notes in Computer Science*; vol. 4986). DOI: 10.1007/978-3-540-68351-3_16.

14. Daemen J., Rijmen V. *The Design of Rijndael. AES — the Advanced Encryption Standard*. Springer, 2002. 238 p. (Ser. *Information Security and Cryptography*). DOI: 10.1007/978-3-662-04722-4.

15. Davidoff G., Sarnak P., Valette A. *Elementary Number Theory, Group Theory and Ramanujan Graphs*. Cambridge University Press, 2003. 156 p. (Ser. *London Mathematical Society Student Texts*; vol. 55).

16. De Canniere C. Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles. In: *Information Security*. Springer, 2006. P. 171–186. (Ser. *Lecture Notes in Computer Science*; vol. 4176). DOI: 10.1007/11836810_13.

17. De Canniere C., Preneel B. Trivium. In: *New Stream Cipher Designs*. Springer, 2008. P. 244–266. (Ser. *Lecture Notes in Computer Science*; vol. 4986). DOI: 10.1007/978-3-540-68351-3_18.

18. Eisenbarth T., Kumar S. A survey of lightweight-cryptography implementations. *Design and Test of Computers, IEEE*, 2007, vol. 24, no. 6, pp. 522–533. DOI: 10.1109/MDT.2007.178.

19. Gammel B., Göttfert R., Kniffler O. *The Achterbahn Stream Cipher*. From: eSTREAM: the ECRYPT Stream Cipher Project. 2005/002, 2005. Available at: http://www.ecrypt.eu.org/stream/ciphers/achterbahn/achterbahn.pdf, accessed 01.09.2013.

20. Gammel B., Göttfert R., Kniffler O. Achterbahn-128/80: Design and analysis. *ECRYPT Network of Excellence — Workshop Record of The State of the Art of Stream Ciphers — SASC 2007*, Ruhr University Bochum, Germany, Jan 31 – Feb 1, 2007, pp. 152–165.

21. Hell M., Johansson Th., Maximov A., Meier W. The grain family of stream ciphers. In: *New Stream Cipher Designs*. Springer, 2008. P. 179–190. (Ser. *Lecture Notes in Computer Science*; vol. 4986). DOI: 10.1007/978-3-540-68351-3_14.

22. Gurkaynak F., Luethi P., Bernold N., Blattmann R., Goode V., Marghitola M., Kaeslin H., Felber N., Fichtner W. *Hardware Evaluation of eSTREAM Candidates: Achterbahn, Grain, MICKEY, MOSQUITO, SFINKS, Trivium, VEST, ZK-Crypt*. From: eSTREAM: the ECRYPT Stream Cipher Project. 2006/015, 2006. Available at: http://www.ecrypt.eu.org/stream/papersdir/2006/015.pdf, accessed 01.09.2013.

23. Hell M., Johansson T., Meier W. Grain: a stream cipher for constrained environments. *International Journal of Wireless and Mobile Computing*, 2007, vol. 2, no. 1, pp. 86–93. Available at: http://inderscience.metapress.com/index/j463lh7251257262.pdf, accessed 01.09.2013.

24. Hoory S., Linial N., Wigderson A. Expander graphs and their applications. *Bulletin of the American Mathematical Society*, 2006, vol. 43, no. 4, pp. 439–562. DOI: S0273-0979-06-01126-8.

25. Lubotzky A., Phillips R., Sarnak P. Explicit expanders and the Ramanujan conjectures. *STOC086 Proceedings of the eighteenth annual ACM symposium on Theory of computing*, New York, NY, ACM, 1986, pp. 240–246. DOI: 10.1145/12130.12154.

26. Lubotzky A., Phillips R., Sarnak P. Ramanujan graphs. *Combinatorica*, 1988, vol. 8, no. 3, pp. 261–277. DOI: 10.1007/BF02126799.

27. O'Neil S., Gittins B., Landman H. A. *VEST Hardware-Dedicated Stream Ciphers*. IACR Cryptology ePrint Archive: Report 2005/413. Available at: https://eprint.iacr.org/2005/413, accessed 01.09.2013.

28. Poschmann A. Y. *Lightweight cryptography: Cryptographic engineering for a pervasive world. PH.D. Thesis*. From: CiteSeerX, 2009. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.1450, accessed 01.09.2013.

29. Rogawski M. *Hardware evaluation of eSTREAM Candidates: Grain, Lex, Mickey128, Salsa20 and Trivium*. From: eSTREAM: the ECRYPT Stream Cipher Project. 2007/025 (SASC 2007), 2007. Available at: http://www.ecrypt.eu.org/stream/papersdir/2007/025.pdf, accessed 01.09.2013.

30. Sarnak P. *Some applications of modular forms*. Cambridge: Cambridge University Press, 1990. (Ser. *Cambridge Tracts in Mathematics*; vol. 99).

31. Braeken A., Lano J., Mentens N.. Preneel B., Verbauwhede I. SFINKS: A synchronous stream cipher for restricted hardware environments. *Proc. of SKEW — Symmetric Key Encryption Workshop, Network of Excellence in Cryptology ECRYPT*, Aarhus, Danemark, 2005.

32. Hell M., Johansson Th., Maximov A., Meier W. A stream cipher proposal: Grain-128. *2006 IEEE International Symposium on Information Theory*, 2006, pp. 1614–1618. DOI: 10.1109/ISIT.2006.261549.

33. Yalla P., Kaps J.-P. Lightweight cryptography for FPGAs. *Reconfigurable Computing and FPGAs, 2009. ReConFigэ09. International Conference on IEEE*, 2009, pp. 225–230. DOI: 10.1109/ReConFig.2009.54.

34. Hecht A., Bard G., Dunkelman O. et al. Gressel C., Granot R. *The ZK-Crypt Algorithm Specication*. FortressGB, 2007.