И.А. Ворончихин, М.А. Батурин, М.Б. Атманских

Тюменский государственный университет, г. Тюмень

УДК 004.056, 004.314.4

ЭФФЕКТИВНЫЕ АППАРАТНЫЕ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ СДВИГОВЫХ РЕГИСТРОВ

Аннотация. В статье рассмотрены регистры сдвига с линейной и нелинейной обратной связью (РСЛОС и РСНОС) и их сравнение. Приведены их конфигурации Галуа и Фибоначчи, для регистров сдвига с линейной обратной связью рассмотрен пример реализации на Arduino.

Ключевые слова: сдвиговые регистры, криптография, аппаратная реализация, РСЛОС, РСНОС.

Введение

Определяющим на ближайшие годы направлением развития Интернета будет Интернет Вещей [1]. Это направление характеризуется переходом от персональных компьютеров к сети между объектами на подобии бытовых приборов, транспортных средств, различных сенсоров и датчиков.

Особую актуальность приобретает задача эффективной реализации алгоритмов защиты информации. Основным средством обеспечения информационной безопасности в Интернете Вещей является так называемая «легковесная криптография». Типичными ограничениями для аппаратной реализации являются: размер микросхемы, потребляемая энергия и время, затраченное на выполнение программы. Поэтому необходимо использовать специализированные вычислительные устройства, удовлетворяющие требованиям.

Сдвиговые регистры представляют собою цепочку разрядных схем, связанных цепями переноса. Основной режим работы – сдвиг разрядов кода от одного триггера к другому на каждый импульс тактового сигнала. В однотактных регистрах со сдвигом на один разряд вправо слово сдвигается при поступлении тактового сигнала. Чаще всего регистр сдвига собирается на основе

последовательно соединенных D-триггеров, притом количество этих триггеров определяет разрядность регистра [2].

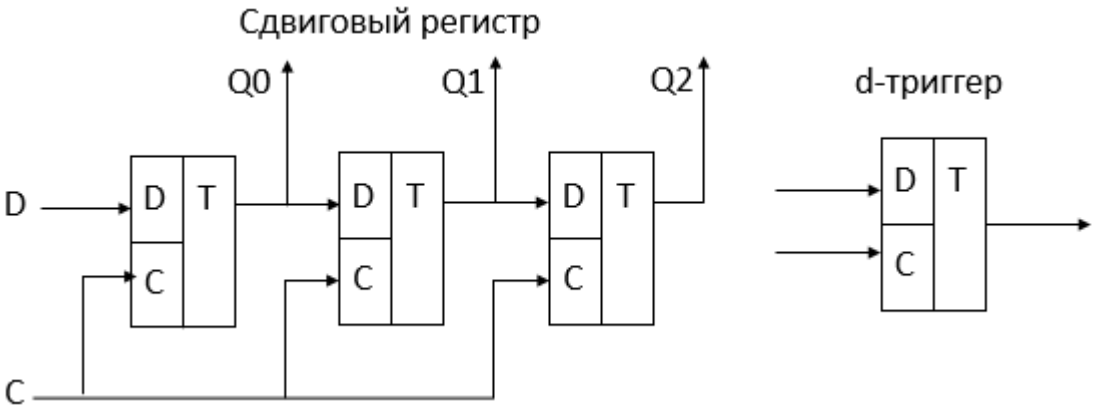

Рис. 1. Сдвиговый регистр

Математические модели РСЛОС

Регистр сдвига с линейной обратной связью, сокращенно РСЛОС – сдвиговый регистр битовых слов, у которого значение входного бита однозначно задается некоторой функцией, исходя из значений остальных битов регистра до сдвига. Добавление обратной связи превращает регистр сдвига в генератор псевдослучайных чисел. Также РСЛОС применяется для поточных шифров таких, как A5/1, Grain, Bean и др.

Обратная связь организуется с помощью булевой функции. Эта функция и определяет какое значение придет на вход регистра. В зависимости от конфигурации имеются разные влияния на состояние ячеек памяти.

В конфигурации Фибоначчи в зависимости от многочлена обратной связи выбираются участвующие в сумме по модулю два ячейки памяти. I-тая ячейка участвует в сумме если в многочлене присутствует i-тая степень. (рис 1) Математическая модель выглядит следующим образом:

$$b_i^+ = b_{i-1}^-,\ i = \overline{1,\ n};$$

$$b_0^+ = \bigoplus_{j=1}^{n} a_j\ * b_j^-,\ a_j\ \in \{0,1\}.$$

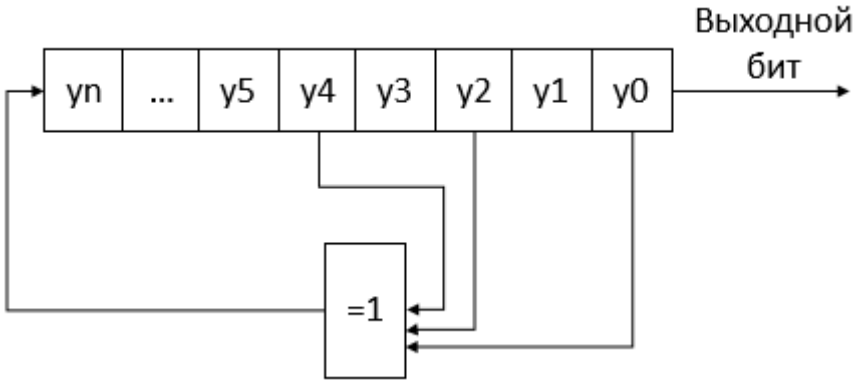

Рис. 2. РСЛОС конфигурации Фибоначчи

В конфигурации Галуа для генерации нового состояния выполняется операция XOR с выходным битом, заменяя старый бит участвующих в операции ячеек памяти. Участие ячейки определяется аналогично наличием *i*-й степени в многочлене. (рис. 2) Математическая модель выглядит следующим образом [3, 4]:

$$b_i^+ = b_{i-1}^- \underset{j=1}{\overset{n}{\oplus}} a_{i-1} * b_n^-,\ i = \overline{1,\ \mathrm{n}};$$

$$b_0^+ = b_n^-.$$

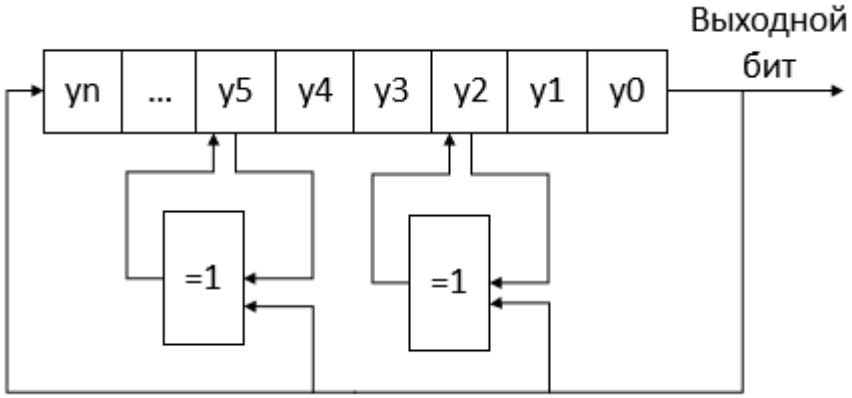

Рис. 3. РСЛОС конфигурация Галуа

Аппаратная реализация РСЛОС

Для аппаратной реализации криптографических сдвиговых регистров понадобятся микросхемы, приведенные на рис. 4:

- Логический И
- Исключающее ИЛИ
- Регистр сдвига

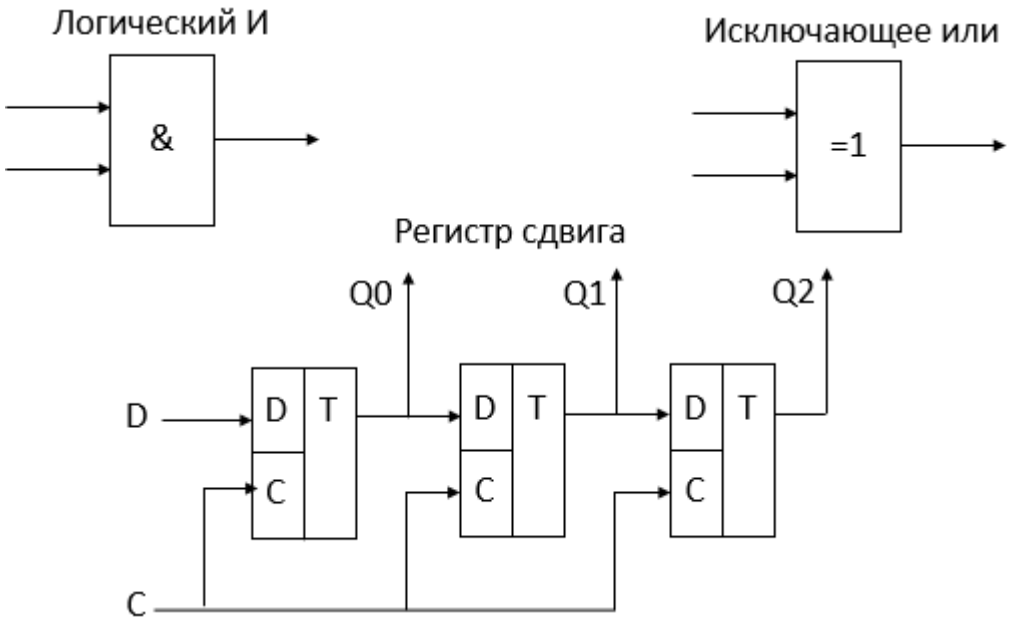

Рис. 4. Необходимые схемы для аппаратных реализаций

Для установки многочлена обратной связи воспользуемся схемами “Логичсекий И” и вспомогательным регистром сдвига. В ячейках памяти вспомогательного регистра сдвига, хранится информация о наличии *i*-й степени в многочлене, 1 – степень присутствует, 0 – отсутствует. Так-как слагаемое ноль не влияет на итог суммы по модулю два, то при обнулении i-ой ячейки памяти основного регистра сдвига, убирается влияние этой ячейки на итог операции (рис. 5).

Рис. 5. Установка многочлена обратной связи в РСЛОС конфигурации Фибоначчи

Далее необходимо со всеми выходами схем “Логичсекий И” произвести операцию XOR. Для этого достаточно последовательно подать значения на схемы “Исключающее ИЛИ”. Итоговый бит всех операций и будет новым входным битом РСЛОС (рис. 6).

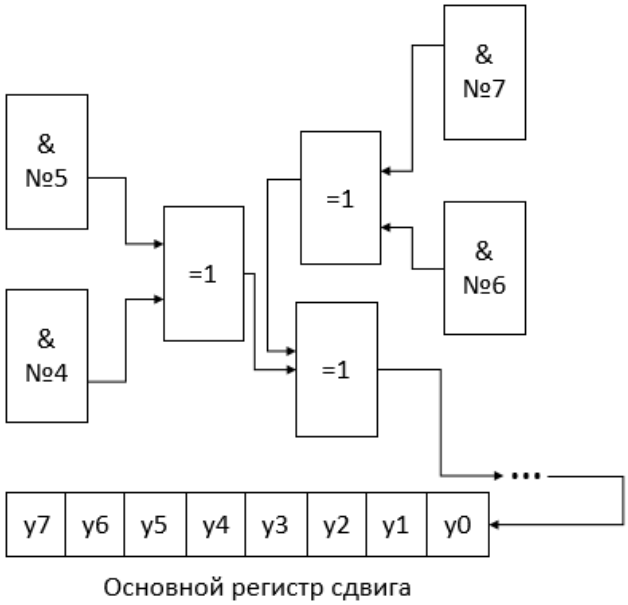

Рис. 6. Вычисление следующего входящего бита в РСЛОС

Для конфигурации Галуа аналогично, обнулив выходной бит перед операций XOR с i-ой ячейкой памяти основного регистра сдвига, значение в ячейке изменено не будет. Итог этих операций и будет новым состоянием РСЛОС (рис. 7).

Рис. 7. Установка нового состояния в РСЛОС конфигурации Галуа

Предварительное тестирование будет происходить на онлайн платформе Tinkercad (рис. 8). Для 8-битной РСЛОС конфигурации Фибоначчи понадобиться:

- Два регистра сдвига 74hc595;
- Два двойных “Логическое И” 74hc08;
- Два двойных “Логическое исключающее ИЛИ” 74hc86.

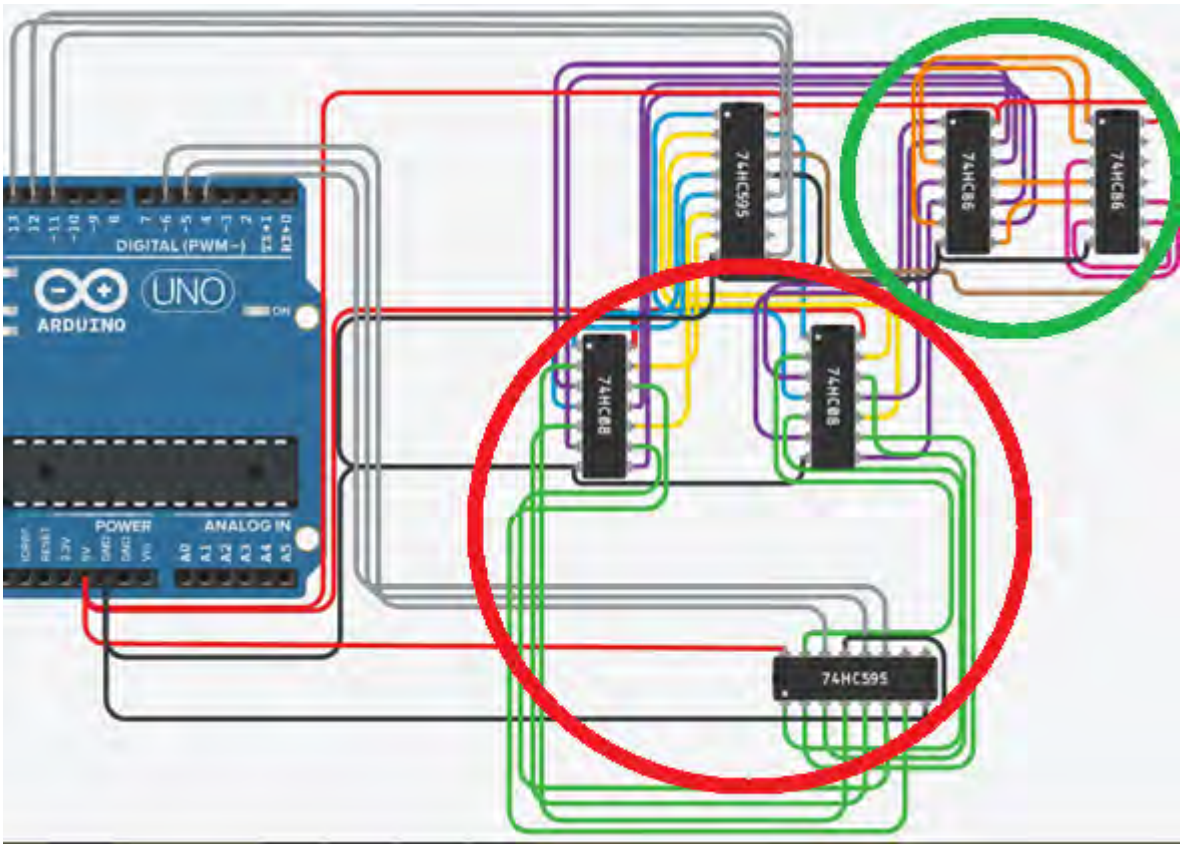

Рис. 8. РСЛОС конфигурации Фибоначчи в Tinkercad

На рисунке в красной области происходит установка многочлена обратной связи. Для этого необходимо отключить вывод на вспомогательном регистре, протолкнуть в него байт, который указывает о наличии или отсутствии *i*-й степени в многочлене обратной связи, включить вывод на вспомогательном регистре.

В зеленой области происходит вычисление следующего входящего бита. Для этого необходимо отключить вывод на регистре, а затем включить его.

Произойдет сдвиг данных и в первую ячейку попадет входной бит, полученный с последовательности схем “Исключающее ИЛИ”.

PCHOC

В зависимости от функции обратной связи, существуют и регистры сдвига с нелинейной обратной связью, или PCHOC. Как следует из названия, в PCHOC используется нелинейная операция (например, умножение) (рис. 9). В частности, PCЛОС – частный случай PCHOC, в случае, когда суммируются по модулю многочлена лишь исходные биты и выходные биты, результаты нелинейной операции в сумму не входят. PCHOC, как и PCЛОС, используются в генераторах псевдослучайной последовательности, а также в шифрах, таких как Achterbahn, Grain (совместно с PCЛОС).

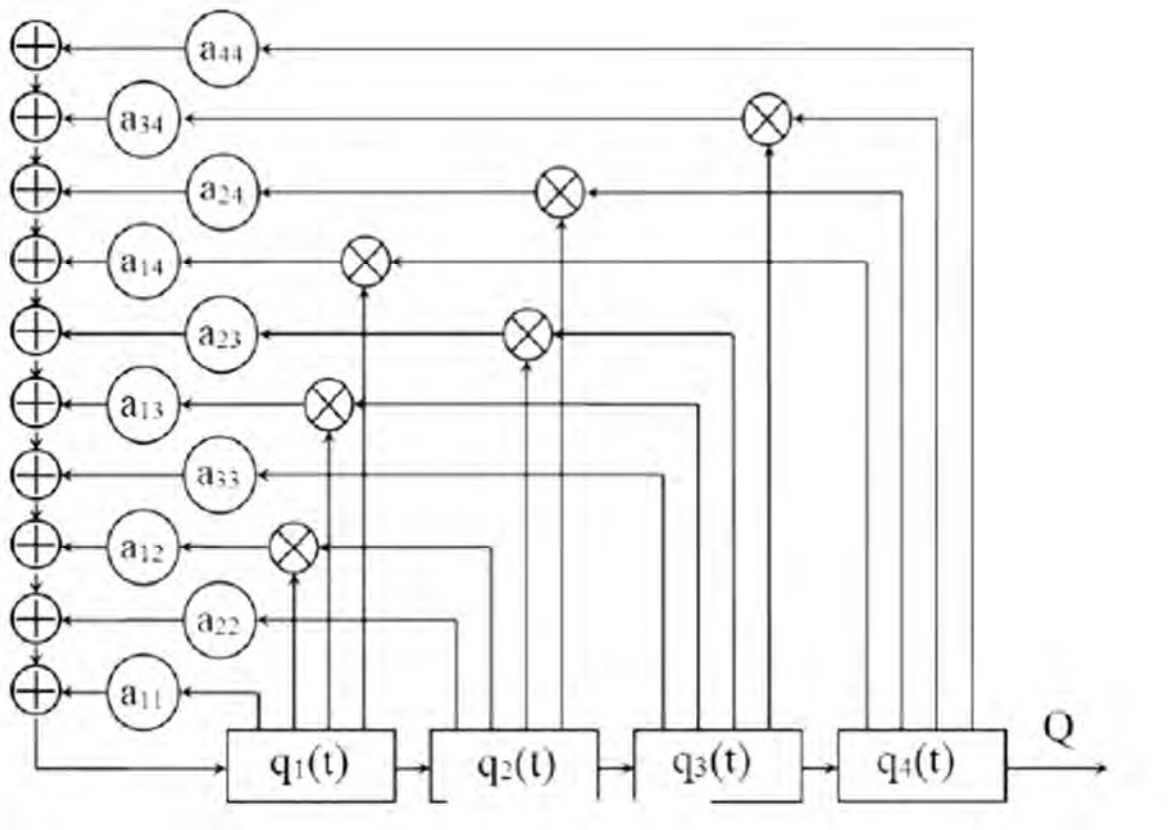

Рис. 9. Пример функции обратной связи в PCHOC

Существуют конфигурации Фибоначчи (рис. 10) и Галуа (рис. 11), которые определяются так же, как и в PCHOC.

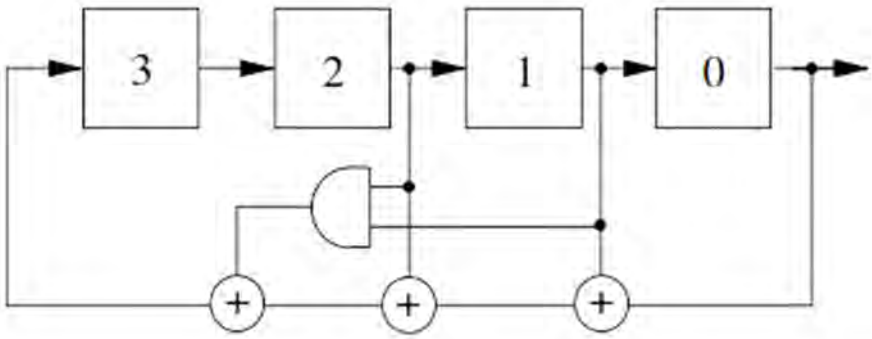

Рис. 10. РСНОС конфигурации Фибоначчи

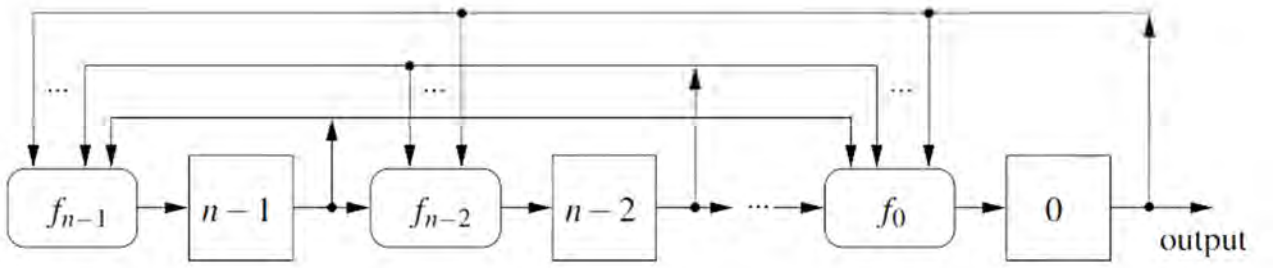

Рис. 11. РСНОС конфигурации Галуа

В РСНОС существует, по сравнению с РСЛОС, большее количество возможных структур при одинаковом размере регистра, что обеспечивает большую криптостойкость. Один и тот же набор ключей дает в РСНОС больше возможных последовательностей. Однако, в отличие от РСЛОС, поиск структур, обеспечивающих максимальный период выходной последовательности, не до конца изучен [5]. В данный момент вычислены такие структуры для длины регистра до 30 бит.

Несмотря на это, программное увеличение времени работы в среднем на 30% оказывает незначительное влияние на производительность, из-за чего использование РСНОС в будущем является перспективным, так как они обеспечивают большую криптостойкость.

Выводы

Были рассмотрены и сравнены РСЛОС и РСНОС в конфигурации Фибоначчи и Галуа. Для РСЛОС приведена реализация на Arduino, рассмотрены

математические модели. Для РСНОС была поставлена проблема поиска структур максимальной последовательности.

Рассмотренные регистры сдвига предлагается сравнить по аппаратной эффективности, для чего были поставлены следующие задачи: реализовать в симуляторе РСЛОС, РСНОС конфигурации Галуа, собрать и протестировать схемы, произвести замеры производительности, проанализировать полученные данные.

СПИСОК ЛИТЕРАТУРЫ

1. European Research Cluster on the Internet of Things [Электронный ресурс]. – URL: www.internet-of-thingsresearch.eu/documents.htm (дата обращения: 10.04.2021).

2. Габриелян Ш., Вахтина Е. Электротехника и электроника: Методические рекомендации. – Ставрополь: Изд-во Аргус, 2013. – 32 с.

3. Токарева Н.Н. Симметричная криптография. Краткий курс: учеб. пособие. – Новосибирск: Изд-во НГУ, 2012. – 134 с.

4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Изд-во Триумф, 2013. – 816 с.

5. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии: учеб. пособие. – СПб.: Изд-во СПб ГУ ИТМО, 2004. – 65 с.