ПРОЦЕССОР АЛГОРИТМА ШИФРОВАНИЯ «BELT» НА БАЗЕ ПЛИС

Ланкевич Ю. Ю.
Кафедра электронных вычислительных средств, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: yurafreedom18@gmail.com

Рассмотрены различные способы реализации процессора алгоритма шифрования "Belt"на базе программируемых логических интегральных схем(ПЛИС) типа FPGA. Выявлены предпочтительные области применения полученных реализаций.

Введение

В настоящее время широко используются различные криптоалгоритмы, и существует необходимость их аппаратной реализации. Реализация на ПЛИС позволяет использовать язык VHDL[1] для описания логики работы устройства и быстро оценить сложность аппаратной реализации. На практике в зависимости от целей использования процессора шифрования, необходимы различные варианты его реализации.

I. Алгоритм шифрования стандарта Belt

Алгоритмы шифрования стандарта «BelT»[2] делятся на 8 групп. В данной статье будет рассмотрена аппаратная реализация группы алгоритмов в режиме простой замены. Для зашифрования(расшифрования) одного 128 разрядного блока данных требуется 8 раундов. Алгоритмы зашифрования и расшифрования отличаются одним действием, что даёт возможность без больших затрат ресурсов реализовать их на одном устройстве.

II. Способы реализации

Первый способ - последовательная реализация. В этом способе используется наименьшее количество аппаратных ресурсов, при этом он имеет и наименьшее быстродействие.

Второй способ - конвейерная реализация. Этот вариант реализации имеет наибольшее быстродействие, при наибольших затратах аппаратных ресурсов.

Третий способ - уменьшенная конвейерная реализация, он имеет в два раза меньшие затраты аппаратных ресурсов и в два раза меньше производительность по сравнению со вторым способом.

III. Анализ полученных способов аппаратных реализаций

Для сравнения способов был выбран кристалл ПЛИС xc6vlx130t-1ff1156, семейства Virtex-6[3].

Последовательная реализация. Максимальная частота тактирования для данного способа реализации 112,4 МГц. Результат шифрования в данном случае будет появляться через 587,4 нс, так как на выполнение алгоритма затрачивается 66 тактов (8 на один раунд и по одному такту на запись во входной и выходной регистры). Скорость обработки данных на одном ключе в данном случае составляет примерно 27,2 Мбайт/с. Для реализации процессора шифрования по первому способу можно выбрать кристалл меньшей ёмкости, например 3S1000-5fg456, семейства Spartan-3, стоимость при этом уменьшится, однако ухудшатся характеристики: максимальная частота тактирования 41МГц, производительность 9,9 Мбайт/с.

Конвейерная реализация. Максимальная частота тактирования в данном случае 217,4 МГц. Первый результат появится через 524,4 нс (114 тактов), каждый последующий результат будет появляться в каждом такте. Скорость обработки данных на одном ключе после заполнения конвейера в данном случае составляет примерно 3478,4 Мбайт/с. Данный способ реализации можно поместить и на кристалле ПЛИС меньшей ёмкости, например 3S4000-5fg900 семейства Spartan-3, стоимость при этом уменьшиться, однако ухудшаться характеристики: максимальная частота тактирования 83МГц, производительность 1328 Мбайт/с.

Уменьшенная конвейерная реализация. Максимальная частота тактирования в данном случае 217,4 МГц. Первый результат появится через 524,4 нс (114 тактов), каждый последующий результат будет выдаваться в течение 14 тактов, затем 14 тактов ожидание. Скорость обработки данных на одном ключе после заполнения конвейера в данном случае составляет примерно 1739,2 Мбайт/с. Данный способ реализации можно также поместить и на более дешёвом кристалле меньшей ёмкости, например 3S2000-5fg900 семейства Spartan-3, стоимость при этом уменьшиться, однако ухудшаться характеристики: максимальная частота тактирования 83МГц, производительность 664 Мбайт/с.

IV. Сравнение

В таблицах 1 и 2 представлена обобщённая информация о затратах аппаратных ресур-

сов каждым из способов реализации. Сравним полученные результаты с результатами, приведенными в статье [4], в которой представлены два способа реализации процессора шифрования:

BeltSeq : вариант реализации с последовательным выполнением операций.

BeltPar : вариант реализации с параллельным выполнением операций.

Из таблицы 3 видно, что предложенные в статье [4] варианты аппаратной реализации алгоритма «BelT» уступают в производительности, но затрачивают меньшее количество аппаратных ресурсов.

Таблица 1 – Сводная таблица результатов проектирования

	Способ 1	Способ 2	Способ 3
Такт,нс	8.9	4.6	4.6
Число тактов ввода данных	1/4	1	1
Ожидание перед подачей следующего слова для обработки	66	0	1
Число вх/вых полюсов	325/516	516	516
Число тактов до начала работы	5	1	1
Время зашифрования/ расшифрования n-слов (такты)	66*n	113+n	112+2*n

Таблица 2 – Сводная таблица результатов проектирования

	Способ 1	Способ 2	Способ 3
Slice registers	847	10209	5598
Slice LUTs	1173	14816	7948
fully used LUT-FF pairs	423	9157	4829

Заключение

Предложенные способы реализации криптоалгоритма стандарта "Belt"на ПЛИС являются эффективными и позволяют выбирать компромис между необходимым быстродействием и стоимостью.

Список литературы

1. Бибило, П. Н. VHDL. Эффективное использование при проектировании цифровых систем / П. Н. Бибило, Н. А. Авдеев. – М. : –Солон-Пресс,2007.
2. СТБ 34.101.31-201. Государственный стандарт Республики Беларусь. Криптографические алгоритмы шифрования и контроля целостности.
3. Кнышев, Д. А. ПЛИС фирмы “Xilinx”: описание структуры основных семейств. / Д. А. Кнышев, М. О. Кузелин –М.: –Издательский дом “Додэка-XXI”, 2001. – 238 с.
4. Поляков, А. С. Характеристики аппаратной реализации некоторых симметричных алгоритмов шифрования / А. С. Поляков,В. Е. Самсонов // Информатика. – 2011. – № 1.

Таблица 3 – Сравнительная таблица полученных результатов с результатами работы [4]

	Способ 1	Способ 2	Способ 3	Belt Seq	Belt Par
Slice registers	847	10209	5598	649	302
Slice LUTs	1173	14816	7948	1392	2050
fully used LUT-FF pairs	423	9157	4829	750	1070
Время зашифрования/ расшифрования n-слов (такты)	66*n	113+ n	112+ 2*n	336*n	212*n