ПРАКТИЧЕСКОЕ ОПРЕДЕЛЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ МИКРОКОНТРОЛЛЕРОВ ДЛЯ РЕАЛИЗАЦИИ ПОПУЛЯРНЫХ КРИПТОАЛГОРИТМОВ

Гараев Р.А.[1], Китаева С.В.[2]

[1]Гараев Рашит Аюпович – кандидат физико-математических наук, доцент;
[2]Китаева Светлана Владимировна – магистрант,
кафедра вычислительной техники и защиты информации,
Уфимский государственный авиационный технический университет,
г. Уфа

Аннотация: *при проектировании современных защищенных сетей вычислителей на базе микроконтроллеров необходимо предусматривать, в числе прочего, шифрование трафика с использованием криптоалгоритмов. Приводятся результаты экспериментальных исследований, направленных на получение реальных оценок затрат вычислительных ресурсов микроконтроллеров с архитектурой RISC при выполнении криптоалгоритмов асимметричного и симметричного шифрования.*
Ключевые слова: *криптография, микроконтроллеры, вычислительные ресурсы, RSA, AES, ГОСТ 28147-89.*

Большинство современных технически сложных устройств, характеризуются наличием в своем составе микроконтроллера или даже нескольких микроконтроллеров (МК). Во многих случаях наряду с сенсорными задачами МК генерирует и управляющие воздействия на различные объекты. Некорректные воздействия со стороны МК могут приводить к серьезным проблемам. Очевидно, что причинами некорректного поведения ПО МК могут являться не только не выявленные на этапе отладки и тестирования ошибки разработчиков-программистов, но и злонамеренные воздействия на МК через каналы связи, при помощи которых МК взаимодействуют с системами верхнего уровня в виде более мощных вычислителей (как минимум класса ПК) или с другими аналогичными МК. Необходимость введения криптографической защиты информации при передаче по этим каналам достаточно очевидна, однако затраты вычислительных ресурсов МК на реализацию указанных алгоритмов могут значительно снижать возможности рассматриваемых микроконтроллерных вычислителей с точки зрения выполнения основной задачи сбора данных или управления объектом. На практике соображения экономии средств или снижения энергопотребления при автономном питании, компактности вычислителя и т.п. нередко приводят к выбору относительно маломощного в вычислительном смысле МК. Соответственно, если выбор конкретной модели МК при проектировании системы производится без учета затрат на криптоалгоритмы, общей производительности центрального процессора МК и ресурсов памяти может оказаться недостаточно для поддержания, по крайней мере, режима реального времени в управлении объектом.

Целью проведенного экспериментального исследования было получение реалистичных оценок затрат времени на выполнение операций шифрования / расшифровывания с использованием некоторых широко применяемых криптографических алгоритмов. В качестве вычислителей в экспериментах были использованы МК с RISC-архитектурой (ARM и AVR). По мнению авторов, использование полученных результатов могло бы еще на этапе проектирования системы реального времени с использованием МК с приемлемой точностью зарезервировать ресурсы, необходимые для поддержки собственно криптоалгоритмов.

При проведении измерений для всех использованных моделей МК применялся единый подход, основанный на определении общего времени выполнения некоторого количества циклов шифрования или расшифровывания информации в программе, разработанной на языке Си путем подсчета числа периодических таймерных прерываний МК. Типичная длительность периода прерываний составляла 0,01 с. Для достижения низкой относительной погрешности измерений полное число циклов для быстрых алгоритмов выбиралось таким, чтобы итоговое время вычислений составляло не менее нескольких секунд.

Аппаратное обеспечение экспериментов представляло из себя персональный компьютер (ПК) и набор популярных оценочных плат (evaluation boards):

- AT91SAM7S-EK на базе 32-разрядного микроконтроллера AT91SAM7S256;
- STM32F4-Discovery на базе 32-разрядного микроконтроллера STM32F407VGT6;
- Аппаратная платформа Arduino Uno на базе 8-разрядного МК ATmega328.

Персональный компьютер обеспечивал как загрузку с жесткого диска в ППЗУ МК соответствующего, заранее подготовленного ПО, так и управление со стороны оператора выбором режима измерений с индикацией результатов по завершению заданного числа циклов. Связь ПК с оценочными платами реализовывалась посредством интерфейса USB.

Набор реализованных популярных алгоритмов шифрования / расшифровывания включал в себя асимметричный алгоритм RSA и два симметричных: AES и отечественный алгоритм по ГОСТ 28147-89.

Трудоемкость вычислений при выполнении операций по алгоритму RSA (от фамилий авторов: Rivest, Shamir, Adleman) нелинейно зависит от длины ключа шифрования. Учитывая современный уровень требований к минимальной длине ключа, были проведены вычисления со следующими размерами: 1024 бита, 1536 бит, 2048 бит, 2560 бит, 3072 бита, 3584 бита и 4096 бит.

AES (Advanced Encryption Standard, известен также как Rijndael) – алгоритм блочного шифрования (размер блока 128 бит), из возможных размеров ключа в работе был выбран один – 256 бит.

Российский стандарт ГОСТ 28147-89 обеспечивает симметричное блочное шифрование для блоков длиной 64 бита с использованием 256-битного ключа.

Наибольшие затраты вычислительных ресурсов для выбранной тройки алгоритмов наблюдаются при работе с RSA. Фактически для выбранных в работе длин ключей шифрования попытка реализации алгоритма на маломощном 8-разрядном МК ATmega328 с тактовой частотой 16 МГц приводила бы к неприемлемо большому с практической точки зрения времени при длине ключа 1024 бита, а кроме того, потребность в объеме памяти для реализации алгоритма при подобной длине ключа превосходит возможности отладочной платы. Поэтому реально на Arduino Uno проводились исследования по алгоритму RSA только для ключа длиной 256 бит и двух симметричных алгоритмов.

При выборе определенной длины ключа для алгоритма RSA изменение самого значения ключа потенциально может влиять на длительность операций шифрования / расшифровывания. Для получения достоверных результатов была собрана статистика по разбросу реального времени расчетов для целого набора конкретных значений ключей шифрования по всем длинам ключа. Поскольку трудоемкость таких экспериментов на МК достаточно высока, оценка разброса была получена путем прогона специальной версии программы с измененным интерфейсом на персональном компьютере с микропроцессором (МП) архитектуры Intel Atom (тактовая частота – 1,86 ГГц). Результаты испытаний, в которых для каждой длины ключа использовались по три разных значения ключа, приведены в таблице 1.

Таблица 1. Результаты для ключей RSA различной длины на МП Intel Atom

	Длина ключа в битах						
	1024	1536	2048	2560	3072	3584	4096
Время шифрования (мсек)	29	78	110	246	297	344	416
	30	79	111	247	298	345	438
	31	80	112	248	299	347	477
Относительное среднее	1,00	2,63	3,70	8,23	9,93	11,51	14,79
Время расшифро-вывания	1850	7237	13714	38137	55165	76743	104675
	1853	7245	13723	38163	55180	76815	104727
	1863	7250	13773	38182	55245	76860	104845
Относительное среднее	1,00	3,90	7,40	20,57	29,75	41,40	56,46

Нетрудно заметить, что относительный разброс времени выполнения операции при каждой длине ключа достаточно мал, по крайней мере, с точки зрения поставленной цели – получения оценок.

Проведение вычислений в RSA при использовании длинных ключей требует программной реализации арифметических операций с числами большой разрядности. В данной работе для всех вычислителей была использована разработанная Дэвидом Айрландом (David Ireland) библиотека BigDigits [1], часть функций из которой была модифицирована.

Алгоритм AES был реализован с использованием модифицированной библиотеки Павла Соколовского aes256 [2].

ЭКСПЕРИМЕНТАЛЬНЫЕ РЕЗУЛЬТАТЫ

При проведении экспериментальных исследований были получены значения времени выполнения операций шифрования / расшифрования для вышеупомянутых криптоалгоритмов на трех микроконтроллерах и одном микропроцессоре Intel Atom. При этом очевидно, что практический интерес результаты представляют лишь при возможности пересчета тактовых частот на реальные значения, используемые в проектируемых системах. Частоты в проведенных экспериментах определялись фактически архитектурными особенностями использованных оценочных плат и особенностями реализации интерфейса USB в рассмотренных МК. Конкретно нижеприведенные усредненные по нескольким реализациям результаты измерений для алгоритма RSA получены на процессорах AT91SAM7S256 , STM32F407VGT6 и Intel Atom, работавших на тактовых частотах 48 МГц, 168 МГц, 1,86 ГГц, соответственно, т.е. измеренные времена работы алгоритмов в пересчете, например, на N МГц

тактовой частоты должны быть умножены на коэффициенты 48/N, 168/N или 1860/N. Если же сравнивать эффективность процессорных архитектур с точки зрения поддержки криптоалгоритмов безотносительно к реальным тактовым частотам, временные затраты для криптовычислений могут быть умножены на корректирующие коэффициенты: 1, 3,5 и 38,75, соответственно (пересчет на единую тактовую частоту 48 МГц).

В таблице 2 представлены сводные результаты по всем вычислителям при выполнении операций шифрования/расшифровывания по алгоритму RSA с длинами ключей 1024/256 бит.

Таблица 2. Сводная таблица для алгоритма RSA

Тип МК/МП	**Atmega328P-PU**	**AT91SAM7S 256**	**STM32F407 VGT6**	**Intel Atom**
Длина ключа – 1024 бита				
Реальное время выполнения (сек)				
Шифрование	–	0,035	0,014	0,03
Расшифровывание	–	30,514	0,885	0,1853
Время в пересчете на тактовую частоту 48 МГц				
Шифрование	–	0,035	0,049	1,1625
Расшифровывание	–	30,514	3,0975	7, 1804
Длина ключа – 265 бит				
Реальное время выполнения (сек)				
Шифрование	0,14	0,03	0,01	0,006
Расшифровывание	2,41	2,27	0,16	0,089
Время в пересчете на тактовую частоту 48 МГц				
Шифрование	0,046	0,030	0,035	0,233
Расшифровывание	0,795	2,270	0,560	3,449

Аналогичные по смыслу результаты для симметричного алгоритма AES с 256-битным ключом представлены в таблице 3. В силу симметричности операций длительности операций шифрования/расшифровывания с высокой точностью совпадают, что подтверждается экспериментально.

Таблица 3. Сводная таблица для алгоритма AES

Atmega328P-PU	**AT91SAM7S256**	**STM32F407VGT6**	**Intel Atom**
Реальное время выполнения (сек)			
0,038	0, 1044	0,00057	0,0022
Время в пересчете на тактовую частоту 48 МГц			
0,0125	0,1044	0,0020	0,0853

Экспериментальные результаты для симметричного блочного алгоритма по ГОСТ 28147-89 с 256-битным ключом и блоков размером 64 бита представлены в таблице 4. Как и для алгоритма AES время операций шифрования / расшифровывания совпадает.

Таблица 4. Сводная таблица для алгоритма ГОСТ 28147-89

Atmega328P-PU	**AT91SAM7S256**	**STM32F407VGT6**	**Intel Atom**
Реальное время выполнения (сек)			
0,0056	0,0047	0,00016	0,0002
Время в пересчете на тактовую частоту 48 МГц			
0,0018	0,0047	0,0006	0,0078

Помимо затрат процессорного времени, для разработчика систем на базе МК интерес представляет и такой параметр, как объем кода, необходимый для реализации криптоалгоритма. Для упомянутых выше алгоритмов соответствующие значения составили порядка 620 КБ для RSA, 410 КБ – для AES и 648 КБ – для ГОСТ 28147-89.

Список литературы

1. BigDigits. [Электронный ресурс]. Режим доступа: http://www.di-mgt.com.au/ bigdigitsmanual/index.html/ (дата обращения: 02.02.2018).

2. AES. [Электронный ресурс]. Режим доступа: https://github.com/pfalcon/ aes256_128/ (дата обращения: 02.02.2018).