BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 5, Number 5(2014), 88 – 93

UDC 681.322

ASPECTS OF HARDWARE REDUCTION MODULO IN ASYMMETRIC CRYPTOGRAPHY

E.Zh. Aithozhayeva, S.T. Tynymbayev
ait_evg@mail.ru
Kazakh national technical university named after K.I.Satpayev, Almaty

Key words: hardware encryption, asymmetric encryption algorithms, reduction modulo, classification.

Abstract. The advantages and disadvantages of software and hardware implementation of encryption and asymmetric cryptosystems are considered. For hardware implementation of an asymmetric cryptographic algorithm we determine time-critical basic operation - reduction modulo. Due to analysis of structures for devices hardware implementation of reduction modulo the characteristics of structures are identified. We obtain the following characteristics of structures: parallelism of operations, number of cycles required to produce a result, presence of control scheme (of the control automaton) for reduction modulo operation, usage of certain radix. The paper proposes four types of classifications of devices with these features that allow to systematize known structures of devices and to use systematic approach in their design and analyze.

УДК 681.322

АСПЕКТЫ АППАРАТНОГО ПРИВЕДЕНИЯ ПО МОДУЛЮ В АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Е.Ж. Айтхожаева, С.Т. Тынымбаев
ait_evg@mail.ru
Казахский национальный технический университет им. К.И.Сатпаева, г. Алматы

Ключевые слова: аппаратное шифрование, асимметричные криптоалгоритмы, приведение по модулю, классификация.

Аннотация. Рассматриваются достоинства и недостатки программной и аппаратной реализации шифрования и асимметричных криптосистем. Определяется критичная по времени базовая операция – приведение по модулю для аппаратной реализации асимметричных криптоалгоритмов. На основе анализа структур устройств аппаратной реализации приведения по модулю выявляются характерные признаки структур. Получены следующие характеристики структур: параллелизм выполнения операций умножения и получения остатков от деления на модуль; количество тактов, необходимых для получения результата; наличие схемы управления (управляющего автомата) операцией приведения по модулю; использование определенной системы счисления. В статье предлагается четыре типа классификаций устройств с учетом этих признаков, что позволяет систематизировать известные структуры и использовать системный подход при проектировании и анализе устройств приведения по модулю.

По мере развития и усложнения средств, методов и форм автоматизации процессов сбора, хранения и обработки информации повышается ее уязвимость. Защита данных – это совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных [1]. Одним из наиболее надежных способов решения проблемы безопасности данных в компьютерных системах и сетях считается криптографическая защита, обеспечивающая превращение открытого текста в шифртекст путем шифрования исходного текста с помощью криптографических алгоритмов [1, 2].

Шифрование возможно осуществить программно, аппаратно и программно-аппаратно. Аппаратное шифрование имеет ряд существенных преимуществ перед программным шифрованием:

- аппаратные средства шифрования обладают большей скоростью (аппаратная реализация любого алгоритма, в том числе и криптографического, обеспечивает более высокое быстродействие, чем программная реализация);

- аппаратуру шифрования легче физически защитить от проникновения извне, чем программу;

- аппаратуру шифрования проще установить.

Поэтому большинство средств криптографической защиты данных реализовано в виде специализированных аппаратных устройств. Эти устройства встраиваются в линию связи и осуществляют шифрование всей передаваемой по ней информации. Преобладание аппаратного шифрования над программным шифрованием обусловлено не только указанными выше причинами, перечень достоинств аппаратных шифраторов значительно шире:

- аппаратная реализация криптоалгоритма гарантирует его целостность;

- шифрование и хранение ключей осуществляются в самой плате шифратора, а не в оперативной памяти компьютера;

- аппаратный датчик случайных чисел создает действительно случайные числа для формирования надежных ключей шифрования и электронной цифровой подписи;

- на базе аппаратных шифраторов можно создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру;

- применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера; возможна также установка на одном компьютере нескольких аппаратных шифраторов, что еще более повышает скорость обработки информации;

- использование парафазных шин в архитектуре шифрпроцессора исключает угрозу снятия ключевой информации по возникающим в ходе криптографических преобразований колебаниям электромагнитного излучения в цепях "земля - питание" микросхемы.

В большинстве современных криптосистем используется асимметричное шифрование [3]. Особенностью асимметричных (двухключевых) алгоритмов шифрования является то, что для шифровки и дешифровки информации используются разные ключи. Знание открытого ключа, с помощью которого был зашифрован документ, не позволяет расшифровать этот документ, а знание закрытого (секретного) ключа, позволяющего расшифровать сообщение, не даёт возможности его зашифровать. Широко известны такие двухключевые алгоритмы, как алгоритмы RSA, Эль-Гамаля, Диффи-Хелмана, Фиата-Шамира, Рабина, Окамото-Саранси, Мацумото-Имаси, Шнорра.

Главным достоинством криптосистем с открытым ключом по сравнению с симметричными (одноключевыми) криптосистемами с секретным ключом является их потенциально высокая безопасность: нет необходимости передавать и убеждаться в подлинности секретных ключей. Главным недостатком криптосистем с открытым ключом является низкое быстродействие, так как в процедурах шифрования и дешифрования используются гораздо более сложные и громоздкие математические вычисления над очень большими числами (например, в RSA, Эль-Гамаля и Рабина используются числа, имеющие порядки 10^{309}). Поэтому часто криптосистемы с открытым ключом применяются для шифрования, передачи и последующей расшифровки только секретного ключа симметричной криптосистемы. А симметричная криптосистема применяется для шифрования и передачи сообщений. Это, так называемая, схема электронного цифрового конверта. Широкое использование двухключевых средств защиты связано также с электронной цифровой подписью, являющуюся реквизитом электронного документа, предназначенным для защиты данного электронного документа от подделки. В 1997 году был разработан стандарт ANSI X9.30, поддерживающий Digital Signature Standard (стандарт Цифровой подписи), а годом позже был введен ANSI X9.31, в котором сделан акцент на цифровых подписях RSA, что отвечает фактически сложившейся ситуации, в частности для финансовых учреждений.

Разработанные на сегодня криптосистемы с открытым ключом опираются на один из следующих типов необратимых (и сложных) преобразований: разложение больших чисел на простые множители, вычисление логарифма в конечном поле, вычисление корней алгебраических уравнений.

На практике наибольшее распространение получил асимметричный алгоритм шифрования RSA (Ривеста, Шамира и Адлемана, 1978 г.), который основан на необратимом преобразовании -

разложении больших чисел на простые множители. Криптоалгоритм отличается хорошей криптостойкостью, которая базируется на сложности факторизации больших целых чисел. Алгоритм RSA стал первым полноценным алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи. Он стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ.

В настоящее время алгоритм RSA используется во многих стандартах. Стандарт ISO 9796 описывает RSA как совместимый криптографический алгоритм, соотвествующий стандарту безопасности ITU-T X.509. Кроме этого криптосистема RSA является частью стандартов SWIFT, ANSI X9.31 rDSA и проекта стандарта X9.44 для американских банков. Австралийский стандарт управления ключами AS2805.6.5.3 также включает систему RSA. Алгоритм RSA активно реализуется как в виде самостоятельных криптографических продуктов, так и в качестве встроенных средств в приложениях. Например, для защиты баз данных в серверах используются встроенные механизмы шифрования, которые предусматривают использование RSA [4].

Алгоритм RSA используется в Internet, в частности, он входит в такие протоколы, как SSL, S-HHTP, S-MIME, S/WAN, STT, PCT, IPSEC (Internet Protocol Security) и TLS (которым предполагается заменить SSL), а также в стандарт PKCS, применяемый в важных приложениях. Для разработчиков приложений с применением PKCS организация OSI Implementers' Workshop (OIW) выпустила соглашение, которое в частности, посвящено алгоритму RSA.

Множество других разрабатываемых в настоящее время стандартов включают в себя либо сам алгоритм RSA или его поддержку, либо рекомендуют криптосистему RSA для обеспечения секретности и/или установления подлинности (аутентификации). Например, включают в себя систему RSA рекомендации IEEE P1363 и WAP WTLS.

Для аппаратной реализации операций шифрования и дешифрования RSA разработаны специальные процессоры. Эти процессоры, реализованные на сверхбольших интегральных схемах (СБИС), позволяют выполнять операции RSA, связанные с возведением больших чисел в очень большую степень по модулю P, за относительно короткое время. Одна из самых быстрых аппаратных реализаций RSA с модулем 512 бит на сверхбольшой интегральной схеме имеет быстродействие 64 Кбит/с. Лучшими, из серийно выпускаемых СБИС, являются процессоры фирмы CYLINK, выполняющие 1024-битовое шифрование RSA. Для сравнения, криптографический программный пакет BSAFE 3.0, реализующий RSA на компьютере Pentium-90 осуществляет шифрование со скоростью 21.6 Кбит/с для 512-битного ключа и со скоростью 7.4 Кбит/с для 1024 битного.

Тем не менее, аппаратная реализация RSA выполняет операции шифрования и дешифрования примерно в 1000 раз медленнее, чем аппаратная реализация DES - симметричного криптоалгоритма. Такой существенный разрыв в быстродействии возникает из-за того, что в RSA используется возведение очень больших (многоразрядных) чисел в очень большую степень по модулю P. Лаборатория RSA рекомендует для обычных задач ключи размером 1024 бита, а для особо важных задач – 2048 битов и более. А в стандарте Республики Казахстан СТ РК 1073-2007 для достижения 3-го уровня безопасности рекомендуется использование ключа длиной 4000 бит, для достижения 4-го уровня безопасности – 8000 бит. Этим и объясняется повышенное внимание теоретиков и практиков криптографии к проблеме ускорения возведения чисел в степень по модулю P.

Определим базовые операции над числами, которые используются в асимметричных криптоалгоритмах шифрования. Возведение чисел в степень по модулю P (a^x mod p) реализуется через использование таких операций как умножение, возведение в квадрат и приведение по модулю. И одним из подходов для повышения производительности криптосистем с открытым ключом, является ускорение выполнения этих операций.

Самой громоздкой из них является операция приведения по модулю, так как она представляет собой получение остатка от деления числа на модуль P, а операция деления – самая сложная из арифметических операций. И эта операция повторяется многократно, так как вместо многократного умножения и затем деления очень большого числа (a^x) на модуль, для ускорения возведения в степень по модулю, используется многошаговое последовательное умножение с приведением по модулю на каждом шаге каждый раз нового произведения. При этом также

понижается разрядность перемножаемых чисел и, соответственно, разрядность произведения, подлежащего перемножению.

Например, если нужно вычислить a^{16} mod p, то вместо выполнения пятнадцати перемножений и одного приведения по модулю очень большого числа (a*a*a*a*a*a*a*a*a*a*a*a*a*a*a*a) выполняют четыре возведения в квадрат, используя после каждого возведения в квадрат приведение по модулю: a^{16} mod p = $(((a^2)^2)^2)^2$ mod p = $(((a^2$ mod p$)^2$ mod p$)^2$ mod p$)^2$ mod p. Это позволяет уменьшить разрядность операндов и ускорить возведение чисел в степень по модулю P. И чем длиннее число, тем заметнее ускорение.

Вычисление a^x mod p, где x не является степенью 2, не намного сложнее. Например, необходимо вычислить a^{17} mod p. Двоичная запись степени (x) числа позволяет представить x как сумму степеней 2: $x = 17_{(10)} = 1\ 0\ 0\ 0\ 1_{(2)}$, поэтому $17 = 2^4 + 2^0$. Тогда

$$a^{17} \bmod p = (a*a^{16}) \bmod p = (a*(((a^2)^2)^2)^2) \bmod p = (((((a^2 \bmod p)^2 \bmod p)^2 \bmod p)^2 \bmod p)*a) \bmod p.$$

Такой подход уменьшает трудоемкость вычислений до 1,5xk операций в среднем, где x – степень числа, k-длина числа в битах.

Из этих примеров видно, что используется умножение на a (*a) и возведение a в квадрат (a^2), приведение полученных произведений (в том числе a^2) по модулю.

К настоящему времени накоплен большой опыт в разработке быстродействующих целочисленных умножителей и квадраторов для различного класса вычислительных систем. Для ускорения базовых операций умножения и возведения в квадрат можно использовать массивы двоичных сумматоров, дерево Уоллеса, счетчики Дадда, систолические умножители, ведические умножители, умножители на быстродействующих двоично-десятичных сумматорах (при использовании двоично-десятичной системы счисления) и т.д.[5, 6, 7].

Что касается ускорения базовой операции приведения по модулю, то такая задача в традиционных вычислительных системах не стояла. Поэтому быстродействующее аппаратное решение операции приведения по модулю является ключевой проблемой при аппаратной реализации криптоалгоритмов, использующих возведение чисел в степень по модулю P, в том числе и RSA.

При аппаратной реализации приведения по модулю могут быть использованы самые различные подходы, которые приводят к большому разнообразию структур устройств получения остатка от деления на модуль. Эти стуктуры представлены в различных публикациях, но систематизация и анализ их отсутствует.

Анализ структур и принципов функционирования различных устройств приведения по модулю позволил выявить их характерные признаки:

- последовательное или параллельное выполнение операций умножения (возведения в квадрат) и получения остатков от деления на модуль;
- однотактность или многотактность работы устройства;
- наличие или отсутствие схемы управления (управляющего автомата) операцией приведения по модулю;
- использование определенной системы счисления.

С учетом этих характеризующих признаков все устройства приведения по модулю могут быть разбиты на классы.

Ниже предлагается классификация устройств приведения по модулю на основе указанных выше критериев.

1. Классификация по степени параллельности процессов умножения и приведения произведения по модулю:

а) параллельные - приведение по модулю осуществляется в процессе умножения, параллельно. После получения каждого частичного произведения каждый раз выполняется его приведение по модулю и в дальнейшем для продолжения умножения используется не частичное произведение, а его остаток;

б) последовательные - приведение по модулю осуществляется после получения произведения, последовательно. Выполняется умножение на a или возведение a в квадрат, только потом находят его остаток от деления на модуль.

2. Классификация по количеству тактов, необходимых для получения остатка в устройстве приведения по модулю:

а) многотактные устройства, в которых остаток определяется путем многократного вычитания из исходного приводимого числа, (впоследствии из полученных положительных остатков) модуля, по которому осуществляется приведение. И здесь возможны два варианта:

- все вычитания реализуются на одних и тех же узлах, которые многократно циклически участвуют в процессе получения каждого остатка (циклическая организация);

- вычитания реализуются на аппаратном конвейере (конвейерная организация), каждая схема которого используется только один раз. Каждый остаток формируется на своем уровне конвейера, количество которых определяется максимальным количеством положительных остатков;

б) однотактные устройства, в которых параллельно выполняются вычитания из приводимого числа модуля P и чисел, кратных модулю (2P, 3P, 4P,….). Кратные модулю формируются предварительно на дополнительных узлах устройства. При этом получают множество остатков, результатом является наименьший положительный остаток.

3. **Классификация по наличию управляющего автомата (УА) в устройстве приведения по модулю:**

а) комплексное устройство - представляется в виде совокупности операционного и управляющего автоматов (ОА и УА). УА вырабатывает управляющие сигналы и управляет процессом приведения по модулю, а все операции выполняются в ОА. Операционный автомат, в свою очередь, посылает осведомительные сигналы в управляющий автомат, которые служат для управляющего автомата ориентиром при выработке очредного управляющего сигнала. Это типичный случай классического операционного устройства (ОУ), при синтезе которого применимы известные методы синтеза цифровых автоматов, в том числе и микропрограммных автоматов (МПА). Здесь возможны следующие варианты:

- управляющий автомат может быть построен в виде схемы – УА с жёсткой логикой;

- управляющий автомат может быть построен на основе принципа программного управления – УА с программируемой логикой;

б) автономное устройство - не выделяется управляющая часть, всё реализовано в виде единой схемы, управляющие сигналы формируются в результате выполнения операций.

4. Классификация по системе счисления, используемой в устройстве приведения по модулю:

а) двоичная система счисления;

б) двоично-десятичная система счисления;

в) вспомогательные системы счисления с основанием 2^h, где h целое число и h>=2. Переход к вспомогательной системе счисления осуществляется условно из двоичной системы счисления путем разбиения двоичного числа на диады (h=2, 2^h=4), на триады (h=3, 2^h=8), на тетрады (h=4, 2^h=16) и т.д.

Предлагаемые критерии и классификации позволяют выполнить сравнительную оценку любой аппаратной реализации приведения по модулю еще на уровне структуры, так как у каждого класса во всех четырех классификациях есть свои достоинства и недостатки.

Например, умножитель по модулю, предлагаемый в патенте РФ № 2299461 (от 20.05.07), включает в себя устройство приведения по модулю, содержащее сумматоры, умножители на константу, инверторы и мультиплексор, которое относится к классам 1б, 2б, 4а, так как является последовательным, однотактным, использует двоичную систему счисления [8]. Соответственно, имеет те же плюсы и минусы, что и классы, к которым он относится. Что касается классификации по наличию управляющей схемы, то из описания и схемы устройства патента не ясно, какой метод управления операцией имели в виду авторы. Следовательно, устройство может быть реализовано или в виде единой схемы, или должно быть дополнено управляющей схемой. А это будут уже два разных устройства.

Другое устройство приведения по модулю, имеющее регистры, сумматор, схемы ИЛИ, схему сравнения относится к классам 1б, 2а, 3а, 4а, так как является последовательным, многотактным, комплексным, использует двоичную систему счисления [9]. Соответственно, имеет достоинства и недостатки, присущие этим классам.

Предлагаемая классификация устройств приведения по модулю позволяет систематизировать известные структуры устройств и использовать системный подход при их проектировании и анализе.

ЛИТЕРАТУРА

[1] Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2012. 592 с.

[2] Рябко Б.Я, Фионов А.И. Основы современной криптографии для специалистов в информационных технологиях. - М.: Научный мир, 2004. 173 с.

[3] Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. – СПб.: Профессионал, 2005. 490 с.

[4] Астанаева А.А., Айтхожаева Е.Ж. Шифрование баз данных средствами MS SQL Server. Журнал Поиск, № 2(3)/2014. - Алматы: Высшая школа Казахстана, 2014. С.226-230.

[5] Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. 2-е изд. -Спб.: Питер, 2011. 688 с.

[6] Sethi K., Panda R. An improved squaring circuits for binary numbers. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.3, No.2. 2012. 111-116 s.

[7] Тынымбаев С.Т., Айтхожаева Е.Ж., Жангисина Г.Д., Щербина В.П. Сравнительный анализ сумматоров двоично-десятичных чисел при реализации криптографических алгоритмов. Журнал Безопасность информации, том 19, №3 (2013).- Киев: НАУ, 2013. С.193-197.

[8] Петренко В.И., Кузьминов Ю.В. Умножитель по модулю. Патент РФ RU 2299461. Бюллетень № 14. Опубликован 20.05.07.

[9] Тынымбаев С.Т., Алимсеитова Ж.К., Баймагамбетова А. Разработка структурной схемы вычислителя $y=a^x \bmod p$. Труды Международных Сатпаевских чтений «Роль и место молодых ученых в реализации стратегии «Казахстан-2050», посвященных 80-летию КазНТУ имени К.И. Сатпаева. Том 3. – Алматы: УИЦ КазНТУ, 2014, С. 516-521.

REFERENCES

[1] Shan'gin V.F. Zashita informacii v kompiuternyh sistemah i setyah. M.: DMK Press, **2007**. 592 s. (in Russ.).

[2] Ryabko B.Ya., Fionov A.I. Osnovy sovremennoy kriptografii dlya specialistov v informacionnyh tehnologiyah. M.: Nauchnyi Mir, **2004**. 173 s. (in Russ.).

[3] Rostovcev A.G., Mahovenko E.B. Teoreticheskaya kriptografiya. SPb.: Professional, **2005**. S. 490 (in Russ.).

[4] Astanaeva A.A., Aithozhaeva E.Zh. *Jurnal Poisk, № 2(3)/2014.* Almaty: Vysshaya shkola Kazahstana, **2014**, 226-230 (in Russ.).

[5] Cil'ker B.Ya., Orlov S.A. Organizaciya EVM i system. 2-e izd. SPb.: Piter, **2011**. 688 s. (in Russ.).

[6] Sethi K., Panda R. An improved squaring circuits for binary numbers. *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol.3,No.2,* **2012**, 111-116.

[7] Tynymbaev S.T., Aithozhaeva E.Zh., Zhangisina G.D., Sherbina V.P. *Jurnal Bezopasnost' informacii, tom 19, №3 (2013).* Kiev: NAU, **2013**, 193-197 (in Russ.).

[8] Petrenko V.I., Kuz'minov U.V. Umnojitel' po modulu. Patent RF RU 2299461. *Bulleten' № 14.* Opublikovan **20.05.07** (in Russ.).

[9] Tynymbaev S.T., Alimseitova Zh.K., Baymagambetova A. *Trudy Mezhdunarodnyh Catpaevskih chtenii «Rol' i mesto molodyh uchenyh v realizacii ctrategii «Kazahstan-2050», posvyashennyh 80-letiu KazNTU imeni K.I.Satpaeva, tom 3.* Almaty: UIC KazNTU, **2014**, 328-330 (in Russ.).

Е.Ж. Айтхожаева, С.Т.Тынымбаев

Асимметриялық криптографияда модуль бойынша аппараттық келтірудең жайттары (аспектерілері)

Тірек сөздер: аппараттық шифрлау, ассиметриялық криптоалгоритмдер, модульге келтіру, жіктеу.

Андатпа. Ассиметриялық криптожүйелердің бағдарламалық және аппараттық іске асыру жолдарының артықшылықтары мен кемшіліктері қарастырылады**.** Ассиметриялық криптоалгоритмдерді аппараттық тәсілмен жүзеге асыру үшін модульге келтіру операциясы, яғни орындалу уақыты сын көтермейтін базалық операция анықталған. Модульге келтіру операциясын аппараттық іске асырудың әртүрлі құрылғылардың құрылымдарын талдау арқылы құрылымдардың әртүрлі сипаттамалық белгілері анықталды. Атап айтқанда олар мыналар: көбейту және модульге бөлу арқылы қалдық алу операцияларын орындаудың қатарластығы; нәтижені қалыптастыруға керекті такт сигналдарының саны; модульге келтіру операциясын басқару сұлбасының (басқару автоматтының) болуы; белгілі бір санақ жүйелерінің қолданылуы, т.б. белгілер. Мақалада жоғарыда аталған белгілерді қамтитын төрт түрлі жіктеу түрі ұсынылды. Ұсынылып отырған жіктелу түрлері құрылғылардың белгілі құрылымдарын бір жүйеге келтіруге, оларды әзерлеу және бағалау кезінде жүйелік келісті пайдалануға мүмкіндік береді.