УДК 519:616-079.4:616.5

ПАРАЛЛЕЛЬНЫЕ ВЫЧИСЛЕНИЯ В КРИПТОГРАФИЧЕСКИХ АЛГОРИТМАХ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Е.Г. КАЧКО, С.С. БАТЮШКО

В статье рассмотрены параллельные варианты вычислений для полиномов, точек эллиптической кривой и скалярного произведения с целью уменьшения их вычислительной сложности. Использование предложенных алгоритмов позволило существенно увеличить эффективность вычислений.

Ключевые слова: криптография, цифровая подпись, эллиптические кривые, параллельные вычисления

1. ПОСТАНОВКА ЗАДАЧИ И ЕЕ АКТУАЛЬНОСТЬ

Большинство современных несимметричных криптографических алгоритмов используют операции над эллиптическими кривыми. Это связано с тем, что эллиптические кривые позволяют уменьшить размер цифровой подписи без уменьшения криптографической стойкости алгоритмов. Примерами таких алгоритмов являются стандарты [1–3]. С другой стороны, большинство современных процессоров являются много ядерными. Поэтому актуальной является задача разработки параллельных алгоритмов как для простых операций над полями, так и основной операции, лежащей в основе формирования и проверки цифровой подписи – скалярного умножения точки эллиптической кривой на скаляр.

В данной работе рассматривается преобразование последовательных алгоритмов в параллельные для выполнения операций над целыми числами, полиномами и точками эллиптической кривой. Для каждого типа алгоритма определяются теоретические оценки с учетом числа ядер процессора и параметров эллиптической кривой. Приведены практические результаты, получаемые за счет их параллельного выполнения, для 2-х ядерного процессора.

2. МОДУЛЬНОЕ ВОЗВЕДЕНИЕ В СТЕПЕНЬ

Операция модульного возведения в степень используется для проверки простоты числа [1–3]. Эта проверка выполняется для формирования параметров эллиптической кривой для всех типов алгоритмов. Для операции используется, как правило, блочный алгоритм Кнута, реализация которого описана в [4]. Суть алгоритма состоит в последовательном выполнении операций вычисления квадрата и умножения с многократной точностью. Для параллельного вычисления степени можно разделить показатель степени на порции и вычислять степень для каждой порции параллельно. Число порций совпадает с числом ядер процессора, а размер порции определяется с учетом того, что после вычисления степени ее необходимо откорректировать с учетом позиции порции. Ускорение [5] за счет параллельных вычислений определяется как отношение времени наилучшего последовательного и параллельного алгоритмов.

Приведенный алгоритм позволил получить ускорение от 20 до 50% в зависимости от числа ядер. В табл. 1 приведены результаты экспериментальной проверки алгоритма для двух ядерного процессора.

Таблица 1

Временные характеристики последовательного и параллельного вычисления модульного возведения в степень[1]

Модуль преобразования	Время (с) при последовательном выполнении	Время (с) при параллельном выполнении (2 ядра)	Ускорение
1024	0.0466112	0.0387393	1.2032
2048	0.349978	0.2901	1.20641
3072	1.15529	0.949829	1.21631

3. ПОЛИНОМИАЛЬНЫЕ ОПЕРАЦИИ

Стандарт [1] наряду с простым полем использует двоичное поле $GF(2^m)$, стандарт [3] полностью построен на использовании двоичного поля $GF(2^m)$. В этом случае вместо традиционных арифметических операций над числами многократной точности используются операции над полиномами. Все полиномиальные операции выполняются с учетом модуля (неприводимого полинома). Основная идея параллельного выполнения состоит в том, что вычисление значения и вычисление модуля выполняется параллельно. Удалось полностью совместить операции вычисления квадрата полинома, операции умножения и инверсии удалось параллельно выполнить лишь частично. Эффективность параллельных вычислений для операций этого класса будет рассмотрена ниже.

4. СКАЛЯРНОЕ УМНОЖЕНИЕ

Операция скалярного умножения выполняется и на этапе формирования, и на этапе проверки цифровой подписи. Для параллельного выполнения операции скалярного умножения на этапе формирования цифровой подписи используются те же идеи, что и при вычислении модульной операции возведения в степень, рассмотренные выше. Особенностью операции проверки цифровой подписи является необходимость вычисления

[1] Все эксперименты выполнены на вычислительной системе с процессором Intel(R) Pentium (R) Dual CPU E2160 @ 1.80 GHz в среде Visual Studio 2005, с поддержкой Open MP.

двух скалярных умножений, причем для второй операции предвычисления не могут быть выполнены, так как используется каждый раз новый открытый ключ. Вот почему операция проверки цифровой подписи обычно выполняется значительно дольше, чем операция ее формирования. Это приводит к дисбалансу системы, использующей цифровые подписи. Вот почему проблема сближения времени формирования и проверки цифровой подписи является столь же важной, как и проблема ускорения самих операций.

В работе предложены алгоритмы параллельного выполнения указанных выше операций и исследовано соотношение между временами формирования и проверки цифровой подписи.

Параллельное вычисление основано на делении скаляра на порции и обработке каждой порции параллельно. Для определения размеров порций определялось соотношение времен операций удвоения (D) и сложения (A) точек. В табл. 2 приведены экспериментальные результаты для полиномиального базиса ДСТУ 4145-2002 значений D, A, число итераций d для Comb метода, а также экспериментальное значение ускорения (S).

Таблица 2

Отношение времен операций удвоения и сложения точек (для якобиановский координат), размер окна равен 8

№	m	D (мкс.)	A (мкс.)	R = = A / D	Число циклов (d)	S
1	163	9.23485	37.5794	4.0693	20	1,70
2	167	8.10486	22.8046	2.8137	20	1,70
3	173	9.63484	23.7146	2.46134	21	1,70
4	179	8.51486	23.5096	2.76101	22	1,71
5	191	8.09486	22.9396	2.83385	23	1,71
6	233	11.0098	30.8745	2.80427	29	1,72
7	257	11.6498	33.5744	2.88197	31	1,72
8	307	14.8898	39.0193	2.62055	38	1,72
9	367	16.6897	47.8992	2.86998	45	1,73
10	431	22.1446	60.4090	2.72793	53	1,73

Для последовательных вычислений в общем виде необходимо d операций удвоения и сложения, т.е. время вычислений равно $d (D + A) = d D (1 + r) = 4 d D$.

Параллельные вычисления

Рассмотрим определение размера порции для двух ядерного процессора. Пусть старшая часть задается k цифрами, тогда младшая часть d – k цифр.

Для вычисления старшей части необходимо выполнить d операций удвоения и k операций сложения. Т.е. время вычисления равно

$$k (D + A) + (d – k) D.$$

Для вычисления младшей части необходимо выполнить (d – k– 1) операций удвоения и сложения. Время вычисления младшей части составляет (d – k – 1) (D + A).

Для достижения максимального эффекта обе части должны завершиться одновременно. Определим значение k для этого.

$$(d – k –1) (D + A) = k (D + A) + (d – k) D.$$

Так как r = A / D, то k = (dr – 1 - r) / (1 + 2r).

После округления в большую сторону получаем k = (dr – 1 + r) / (1 + 2r).

Из табл. 2 следует, что r ≈ 3, т.е. k = (3d +2)/7.

Так, для m = 163 число итераций для обработки старшей части равно 8 и число итераций для младшей части равно 12.

Время выполнения операций для параллельного вычисления равно:

$$k (D + A) + (d- k) * D + A = (16dD + 9D)/7.$$

Теоретическое ускорение для параллельных вычислений:

$$S = 4 d D * 7 / (16dD + 9D) = 28d/(16d + 9) \approx 7/4.$$

Из последней формулы видно, что ускорение тем больше, чем больше d. Величина ускорения не превышает 1,75, т.е. 75 процентов для двух ядер. Значения ускорений, полученные в результате вычислительного эксперимента, приведены в табл. 2 (последняя колонка).

Реальное ускорение меньше расчетного за счет того, что после вычисления скалярного произведения в полярных координатах результат необходимо перевести в аффинные координаты. Кроме этого, теоретические расчеты не учитывают накладных расходов, связанных с формированием потоков.

Для проверки цифровой подписи необходимо выполнить 2 операции скалярного умножения. Если процессор содержит 4 или более ядер, то каждую операцию можно выполнять параллельно. Если используется двух ядерный процессор, то одна итерация должна соответствовать одной операции скалярного умножения.

В табл. 3, 4 приведены результаты экспериментального исследования предложенных алгоритмов на примере ДСТУ 4145-2002, которые достигаются за счет параллельного выполнения базовых операций для работы с полиномом, точками эллиптической кривой и вычисления скалярных умножений.

Таблица 3

Формирование (S)и проверка (V)цифровой подписи для последовательного режима выполнения

№	m	Последовательный (Ts)		
		S	V	V/S
1	163	0,783699	2,42131	3,09
2	167	0,763359	2,40964	3,16
3	173	0,808407	2,46914	3,05
4	179	0,854701	2,6455	3,10
5	191	0,878735	2,76625	3,15
6	233	1,35044	4,41501	3,27
7	257	1,59109	5,44959	3,43
8	307	2,17865	7,38007	3,39
9	367	3,09598	10,989	3,55
10	431	4,31034	15,625	3,63
11	571	7,8125	28,5714	3,66

Обозначения в таблице: m – степень поля; S – время формирования цифровой подписи (миллисекунд); V – время проверки цифровой подписи (миллисекунд); S/V – отношение времени проверки к времени формирования цифровой подписи.

Таблица 4

Формирование (S) и проверка (V) цифровой подписи для параллельного режима выполнения

№	M	Параллельный (Tp)			Ускорение (Ts/Tp)	
		S	V	V/S	S	V
1	163	0,558347	0,855798	1,53	1,40	2,83
2	167	0,547945	0,838574	1,53	1,39	2,87
3	173	0,594354	0,903751	1,52	1,36	2,73
4	179	0,61237	0,921234	1,50	1,40	2,87
5	191	0,637349	0,990099	1,55	1,38	2,79
6	233	0,967586	1,52207	1,57	1,40	2,90
7	257	1,12423	1,77936	1,58	1,42	3,06
8	307	1,5361	2,11416	1,38	1,42	3,49
9	367	2,11416	3,68324	1,74	1,46	2,98
10	431	2,99401	5,27704	1,76	1,44	2,96
11	571	5,49451	9,70874	1,77	1,42	2,94

В последних двух колонках табл. 4 приведены значения ускорений для формирования (S) и проверки (V) цифровой подписи.

На рис. 1 изображены графики зависимости отношения времен для проверки и генерации цифровой подписи.

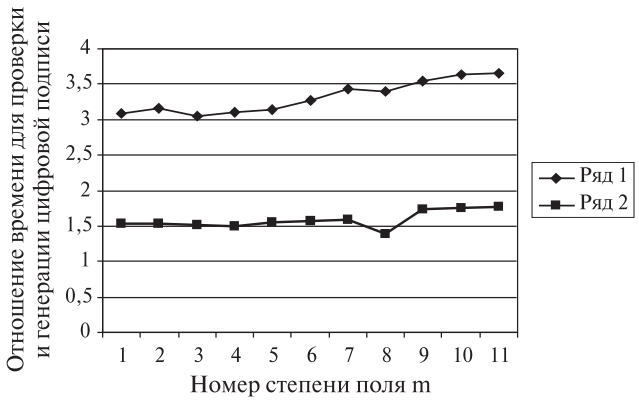

Рис. 1. Отношение времени для проверки и генерации цифровой подписи для последовательного и параллельного алгоритмов:
ряд 1 – последовательный алгоритм;
ряд 2 – параллельный алгоритм

Как видно из рисунка, соотношение времен незначительно зависит от степени поля m. Если проигнорировать выброс значения отношения для номера степени 8 (m = 307), то из графика для параллельных вычислений следует, что это значение плавно увеличивается в пределах 8%, такой же приблизительно относительный прирост отношения этих времен для последовательных вычислений.

Таким образом, характер изменений степени эллиптической кривой на изменение отношения времени для проверки и формирования цифровой подписи не зависит от выбора типа вычислений.

ВЫВОДЫ

Параллельное выполнение базовых операций для эллиптических кривых позволило получить следующие результаты:

– среднее значение ускорения для формирования цифровой подписи составляет 1.41 и для ее проверки — 2.95;

– ускорение практически не зависит от значения *m* поля Галуа эллиптической кривой (отклонение от математического ожидания не превосходит 3.5 % для цифровой подписи и 18 % для проверки цифровой подписи);

– параллельное выполнение проверки подписи более эффективно, чем формирования подписи, так как при проверке подписи соотношение между параллельно и последовательно выполняемым кодом выше (Закон Амдаля);

– использование параллельных вычислений позволяет существенно улучшить соотношение между временем формирования и проверки цифровой подписи. В случае последовательных вычислений это значение не менее 3,09 и растет с увеличением m, в случае параллельных вычислений максимальное значение отношения равно 1.77.

Литература.

[1] FIPS PUB 186-3. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. Digital Signature Standard (DSS) Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900 Issued June, 2009.

[2] ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [http://dic.academic.ru/dic.nsf/ruwiki/261586].

[3] ДСТУ 4145-2002. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ, Держстандарт України. 2003. 36 с.

[4] *Качко Е.Г., Свинарев А.В., Головашич С.А., Лавриненко Д.И.* «Исследование методов оптимизации криптографических операций» Материалы юбилейной научно-технической конференции “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, Киев, 1998, 198-203.

[5] *Воеводин В.В., Воеводин Вл.В.* Параллельные вычисления. СПб: БХВ – Петербург, 2004. – 608 с.

Поступила в редколлегию 4.06.2010.

Качко Елена Григорьевна, кандидат технических наук, профессор кафедры ПОЭВМ ХНУРЭ. Область научных интересов: программные средства криптографических систем.

Батюшко Стас Стефанович, ассистент кафедры БИТ ХНУРЭ. Область научных интересов: защита информации в телекоммуникационных сетях, операционные системы, языки программирования, отказостойкие системы, создание больших разветвленных вычислительных систем, суперкомпьютеры.

УДК 519:616-079.4:616.5

Паралельні обчислення в критографічних алгоритмах на основі еліптичних кривих / Е.Г. Качко, С.С. Батюшко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 370-373.

В статті розглядаються паралельні варіанти обчислень для поліномів, точок еліптичної кривої та скалярного додатку з метою зменшення обчислювальної складності операцій формування та перевірки цифрового підпису. Використання запропонованих алгоритмів дозволило суттєво збільшити ефективність обчислень.

Ключові слова: криптографія, цифровий підпис, еліптичні криві, паралельне обчислення.

Табл. 04. Іл.01. Бібліогр.: 05 найм.

UDC 519:616-079.4:616.5

Parallel calculations in elliptic curve cryptographic algorithms / E.G. Kachko, S.S. Batyushko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 370-373.

The paper considers parallel variants of calculations for polynomials, elliptic curve points and scalar product with the aim of diminishing their computational complexity. The use of the algorithms suggested allowed to substantially increase the efficiency of calculations.

Key words: cryptography, digital signature, elliptic curves, parallel calculations.

Tab. 04. Fig. 01. Ref.: 05 items.