УДК 681.3

НОВЫЙ МЕТОД И АЛГОРИТМ ВЫПОЛНЕНИЯ БАЗОВЫХ ОПЕРАЦИЙ В ЭЛЛИПТИЧЕСКИХ КРИВЫХ, ИСПОЛЬЗУЕМЫХ В СИСТЕМАХ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Червяков Н.И., Головко А.Н., Кондрашов А.В.

В статье рассмотрен новый метод и алгоритм выполнения базовых операций в эллиптических кривых с использованием модифицированной системы координат Якобиана и усовершенствованного бинарного алгоритма скалярного умножения точек. Предложенный подход с использованием эллиптических кривых позволяет обеспечить более высокую скорость шифрования информации по сравнению с известными подходами.

Развитие инфокоммуникационных технологий с использованием эллиптических кривых неразрывно связано с проблемой обеспечения информационной безопасности информации при ее передаче и обработке. Процесс глобализации инфокоммуникационных комплексов, внедрение телекоммуникационных технологий существенно обострили проблему зависимости качества процессов передачи и обработки информации от возможных преднамеренных и непреднамеренных воздействий нарушителя на передаваемые данные пользователя, информацию управления и аппаратно-программные средства, обеспечивающие эти процессы.

Увеличение объемов хранимой и передаваемой информации, территориальная распределенность сетей связи приводят к наращиванию потенциальных возможностей нарушителя по несанкционированному доступу к информационной сфере, воздействию на процессы ее функционирования.

Обеспечение гарантированных качественных характеристик процесса передачи данных в условиях возможных воздействий нарушителя составляет основу проблемы обеспечения информационной безопасности.

Обеспечение информационной безопасности должно достигаться комплексным использованием организационных, технических, аппаратно-программных и криптографических средств защиты информационной сферы.

В основе современных криптографических систем шифрования данных лежат два принципа управления ключами. К первым относятся блочные и поточные алгоритмы шифрования, которые используют один секретный ключ. Он должен быть известен только абонентам, передающим информацию. Достоинством такого подхода выступает высокая скорость шифрования, а недостатком – их низкая эффективность в управлении ключами, которая требует дополнительных механизмов безопасности.

Ассиметричные алгоритмы или алгоритмы с открытым ключом, принадлежащие ко второму подходу, устроены так, что ключ, используемый для зашифрования, отличается от ключа расшифрования. Более того, ключ расшифрования не может быть вычислен из ключа зашифрования. Данное обстоятельство избавляет от многих проблем с ключевой информацией, характерной для симметричной криптографии.

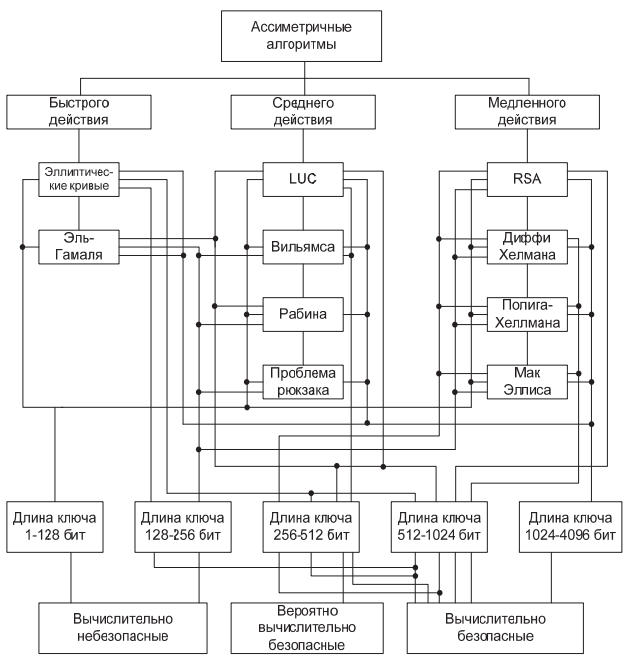

Рис. 1. Классификация ассиметричных алгоритмов

С момента появления ассиметричных алгоритмов в 1976 г. было предложено множество алгоритмов с открытым ключом. Многие из них небезопасны, другие не пригодны для реализации. На рис. 1 представлены лишь те, которые считаются и безопасными и практичными. Большинство из них основываются на труднорешаемых проблемах для взлома факторизации или разложения больших чисел на множители, как RSA или система Полига-Хеллмана, или на проблеме дискретного логарифмирования в мультипликатив-

ных группах конечных полей, как криптосистемы Эль-Гамаля и Диффи-Хеллмана.

Особое место в этой классификации занимают криптосистемы на эллиптических кривых. Они основываются на проблеме дискретного логарифмирования в аддитивной группе конечных полей, которая на сегодня является самой трудноразрешимой. Уже при длине ключа 100-250 бит такие системы способны обеспечить гарантированные характеристики системы, что не дает ни один из других алгоритмов.

В случае произвольного порядка любую эллиптическую кривую можно описать формой

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \quad (1)$$

Однако такая форма тяжела для практического применения и с помощью замены координат может быть преобразована к пяти основным формам (см. рис. 2).

Исследования показали, что наиболее сильными криптографическими свойствами обладают

Рис. 2. Классификация эллиптических кривых

эллиптические кривые E, определяемые уравнением Вейерштрасса

$$E: y^2 = x^3 + ax + b(\mathrm{mod}\, p), a,b \in p, p > 3, \quad (2)$$

где a,b – коэффициенты уравнения, $P(x,y)$ – координаты точек P на эллиптической кривой заданного вида, при этом x может содержать исходное шифруемое двоичное сообщение или его часть.

Коэффициенты уравнения, как правило, задаются дискриминантом, который определяет форму кривой: с положительным (см. рис. 3) или отрицательным (см. рис. 4) дискриминантом.

$$\Delta E = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 = \frac{4a^3 + 27b^2}{108} \neq 0. \quad (3)$$

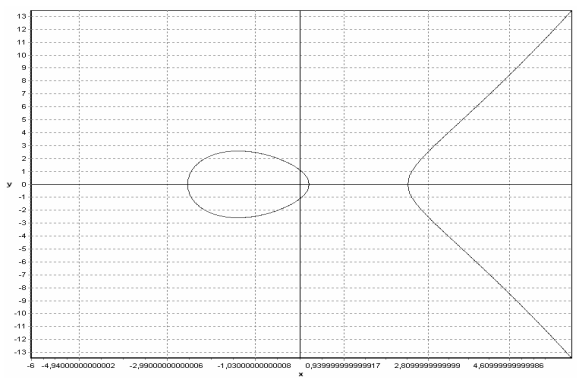

Рис. 3. Эллиптическая кривая $y^2 = x^3 + 6x + 5$

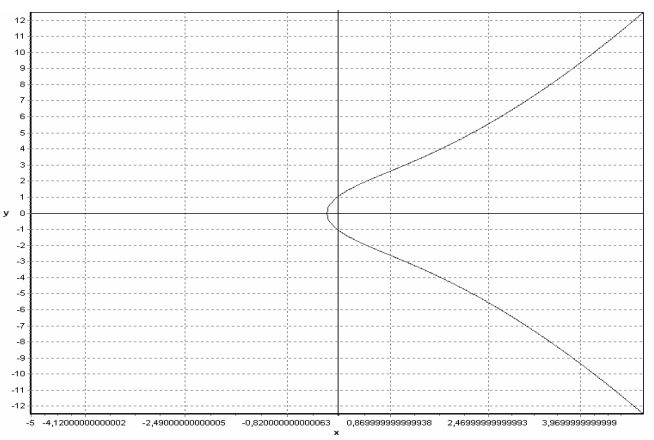

Рис. 4. Эллиптическая кривая $y^2 = x^3 + 6x + 1$

Преимуществом криптосистем на эллиптических кривых является то, что при выполнении операции шифрования отсутствует очень медленная операция возведения больших чисел в степень по модулю, характерная для других криптосистем с открытым ключом. Базовой операцией в группе точек эллиптической кривой, определяемой конкретным уравнением, являются операции сложения и удвоения точек в аффинных координатах (A), для осуществления которых применяется следующий алгоритм.

Вход: коэффициент a эллиптической кривой (1), точки $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$.

Выход: $P = P_1 + P_2$ (см. рис. 5-6).

1. Если $x_1 \neq x_2$, то вычислить $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$, $x_3 = \lambda^2 - x_1 - x_2$.

2. Вернуть $P = (x_3, -y_1 + \lambda(x_1 - x_3))$.

3. Иначе принять $x = x_1$, $y = y_1$, вычислить $\lambda = \dfrac{3x^2 + a}{2y}$, $x_3 = \lambda^2 - 2x$.

4. Вернуть $P = (x_3, -y + \lambda(x - x_3))$.

Если обозначить время выполнения «трудных» операций как: I – операцию деления, M – операцию умножения и S – операцию возведения в квадрат, то оценка времени сложения точек в аффинных координатах составляет $t(A + A) = I + 2M + S$, а удвоения – $t(2A) = I + 2M + 2S$.

При применении этого алгоритма в группе точек эллиптической кривой в кольце вычетов возникают две операции деления по модулю

$$\lambda = \left| \frac{y_1 + y_2}{x_1 + x_2} \right|_p \text{ и } \lambda = \left| \frac{3x^2 + a}{2y} \right|_p .$$

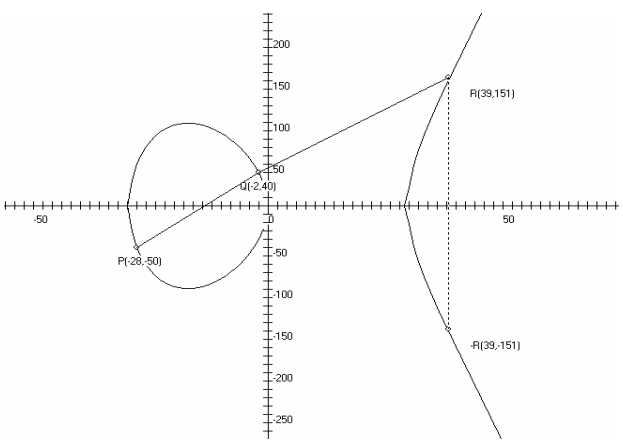

Рис. 5. Сложение точек на эллиптической кривой

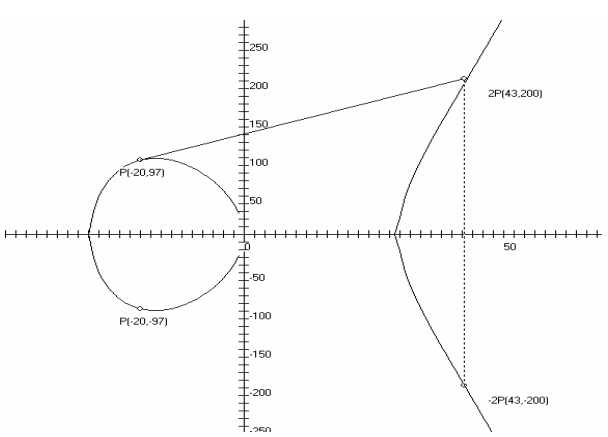

Рис. 6. Удвоение точек на эллиптической кривой

В общем случае операцию деления по модулю можно осуществить двумя методами. Первый метод основан на использовании обратной мультипликативной величины

$$\lambda = \left| \frac{A}{B} \right|_p = \left| A \cdot \left| \frac{1}{B} \right|_p \right|_p , \qquad (4)$$

где $\left| \dfrac{1}{B} \right|_p = k$ – обратная мультипликативная величина, определяемая итерационно в соответствии со сравнением

$$kB \equiv 1 \bmod p , \; k = 1; 2... \qquad (5)$$

Второй метод основан на следующем итерационном процессе

$$\lambda = \left| \frac{A}{B} \right|_p = \frac{kp + A}{B}, \qquad (6)$$

где $k = 0;1;2...$, определяется до тех пор, пока A будет нацело делится на B.

Как видно, недостатком этих методов выступает то, что на сегодняшний день не известны эффективные методы деления больших чисел по модулю или их не существует.

Для того чтобы уйти от операции деления, применяется проективная система координат (P) путем замены $x = X / Z$ и $y = Y / Z$ с последующим переходом от (1) к уравнению

$$Y^2 Z = X^3 + aXZ^2 + bZ^3 (\bmod p) . \qquad (7)$$

Алгоритм сложения и удвоения приводится к следующему виду [1].

Вход: коэффициент a эллиптической кривой (7), точки $P_1 = (X_1, Y_1, Z_1)$ и $P_2 = (X_2, Y_2, Z_2)$.

Выход: $P = P_1 + P_2 = (X_3, Y_3, Z_3)$.

1. Если $X_1 \neq X_2$, то $X_3 = vA$,

$Y_3 = u(v^2 X_1 Z_2 - A) - v^3 Y_1 Z_2$, $Z_3 = v^3 Z_1 Z_2$,

где $u = Y_2 Z_1 - Y_1 Z_2$, $v = X_2 Z_1 - X_1 Z_2$,

$$A = u^2 Z_1 Z_2 - v^3 - 2v^2 X_1 Z_2 .$$

2. Иначе $X_1 = X_2$, $Y_1 = Y_2$, $Z_1 = Z_2$,

то $X_3 = 2hs$, $Y_3 = w(4B - h) - 8Y_1^2 s^2$,

$Z_3 = 8s^3$,

где $w = aZ_1^2 + 3X_1^2$, $s = Y_1 Z_1$, $B = X_1 Y_1 s$,

$$h = w^2 - 8B .$$

Анализ этого алгоритма показывает, что время операции сложения точек оценивается как

$t(P+P)=12M+2S$, а время операции удвоения точек – $t(2P)=7M+5S$.

Однако, представленный алгоритм не приводит к существенному повышению производительности криптосистемы, так как замена операции деления приводит к увеличению числа операций умножения примерно в 4,5 раза.

Для сокращения операций умножения может использоваться система координат Якобиана (*J*). В этой системе используется замена координат и $x=X/Z^2$ и $y=Y/Z^3$, а уравнение (2) приводится к виду:

$$Y^2=X^3+aXZ^4+bZ^6 \pmod p. \qquad (8)$$

Тогда алгоритм сложения и удвоения точек на эллиптической кривой в системе координат Якобиана примет вид [2]:

Вход: коэффициент *a* эллиптической кривой (8), точки $P_1=(X_1,Y_1,Z_1)$ и $P_2(X_2,Y_2,Z_2)$.

Выход: $P=P_1+P_2=(X_3,Y_3,Z_3)$.

1. Если $X_1\neq X_2$, то вычислить

$$X_3=-H^3-2U_1H^2+r^2,$$

$$Y_3=-S_1H^3+r(U_1H^2-X_3),\ Z_3=Z_1Z_2H,$$

где $U_1=X_1Z_2^2,\ U_2=X_2Z_1^2,\ S_1=Y_1Z_2^3,$

$$S_2=Y_2Z_1^3,\ H=U_2-U_1,r=S_2-S_1.$$

2. Иначе принять $X_1=X_2$, $Y_1=Y_2$, $Z_1=Z_2$, тогда вычислить $X_3=T$,

$$Y_3=-8Y_1^4+M(S-T),\ Z_3=2Y_1Z_1,$$

где $S=4X_1Y_1^2$, $M=3X_1^3+aZ_1^4$, $T=-2S+M^2$.

Анализ показывает, что операция сложения точек оценивается как $t(J+J)=12M+4S$, а операция удвоения точек – $t(2J)=4M+6S$.

Как видно, в системе координат Якобиана удвоение точки осуществляется быстрее, а сложение точек осуществляется медленнее, чем в проективных координатах.

Чтобы выполнить операцию сложения быстрее, можно применить обобщенную систему координат Якобиана-Чудновского (J^C). В этой системе координаты представляются пятерками $P=(X,Z,Y,Z^2,Z^3)$. Тогда алгоритм сложения и удвоения точек на эллиптической кривой в системе Якобиана-Чудновского осуществляется следующим образом.

Вход: коэффициент *a* эллиптической кривой (8), точки $P_1=(X_1,Y_1,Z_1,Z_1^2,Z_1^3)$ и $P_2(X_2,Y_2,Z_2,Z_1^2,Z_1^3)$.

Выход: $P=P_1+P_2=(X_3,Y_3,Z_3,Z_3^2,Z_3^3)$.

1. Если $X_1\neq X_2$, то вычислить

$$X_3=-H^3-2U_1H^2+r^2,$$

$$Y_3=-S_1H^3+r(U_1H^2-X_3),\ Z_3=Z_1Z_2H,$$

$$Z_3^2=Z_3^2,Z_3^3=Z_3^3,$$

где $U_1=X_1(Z_2^2),\ U_2=X_2(Z_1^2),\ S_1=Y_1(Z_2^3),$

$$S_2=Y_2(Z_1^3),\ H=U_2-U_1,r=S_2-S_1.$$

2. Иначе принять $X_1=X_2$, $Y_1=Y_2$, $Z_1=Z_2,Z_1^2=Z_2^2,Z_1^3=Z_2^3$, тогда вычислить

$$X_3=T,\ Y_3=-8Y_1^4+M(S-T),\ Z_3=2Y_1Z_1,$$

$$Z_3^2=Z_3^2,Z_3^3=Z_3^3,$$

где $S=4X_1Y_1^2,\ M=3X_1^3+a(Z_1^2)^2,$

$$T=-2S+M^2.$$

Как видно, время выполнения сложения точек оценивается как $t(J^c+J^c)=11M+3S$, а время операции удвоения точек – $t(2J^c)=5M+6S$.

Для сокращения операций при удвоении точек на эллиптической кривой авторами предлагается новый метод, основанный на новой системе координат, названной модифицированной системой координат Якобиана (J^m). В этой системе используется четверка координат (X,Y,Z,aZ^4). Тогда алгоритм сложения и удвоения точек на эллиптической кривой в модифицированной системе координат Якобиана примет следующий вид.

Вход: коэффициент *a* эллиптической кривой (8), точки $P_1(X_1,Y_1,Z_1,aZ_1{}^4)$ и $P_2(X_2,Y_2,Z_2,aZ_2{}^4)$.

Выход: $P=P_1+P_2=(X_3,Y_3,Z_3,aZ_3^4)$.

1. Если $X_1\neq X_2$, $X_3=-H^3-2U_1H^2+r^2$,

$$Y_3=-S_1H^3+r(U_1H^2-X_3),\ Z_3=Z_1Z_2H,$$

$$aZ_3^4=aZ_3^4,$$

где $U_1=X_1Z_2^2,\ U_2=X_2Z_1^2,$

$$S_1=Y_1Z_2^3,S_2=Y_2Z_1^3,\ H=U_2-U_1,r=S_2-S_1.$$

2. Иначе принять $X_1=X_2$, $Y_1=Y_2$, $Z_1=Z_2$,

$aZ_1^4=aZ_2^4$, то $X_3=T$, $Y_3=M(S-T)-U$,

$$Z_3=2Y_1Z_1,\ aZ_3^4=2U(aZ_1^4),$$

где $S=4X_1Y_1^2$, $U=8Y_1^4$, $M=3X_1^3+(aZ_1^4)$,

$$T=-2S+M^2.$$

Время выполнения сложения и удвоения точек на эллиптической кривой в модифицированной системе координат Якобиана оценивается как $t(J^m + J^m) = 11M + 3S$, а время удвоения точек – $t(2J^m) = 4M + 4S$.

Таблица 1. Варианты гибридных координат

Сложение	
Операция	Время выполнения
$t(J^m + J^m)$	$13M + 6S$
$t(J^m + J^c = J^m)$	$12M + 5S$
$t(J + J^c = J^m)$	$12M + 5S$
$t(J + J)$	$12M + 4S$
$t(P + P)$	$12M + 2S$
$t(J^c + J^c = J^m)$	$11M + 4S$
$t(J^c + J^c)$	$11M + 3S$
$t(J^c + J = J)$	$11M + 3S$
$t(J^c + J^c = J)$	$10M + 2S$
$t(J + A = J^m)$	$9M + 5S$
$t(J^m + A = J^m)$	$9M + 5S$
$t(J^c + A = J^m)$	$8M + 4S$
$t(J^c + A = J^c)$	$8M + 3S$
$t(J + A = J)$	$8M + 3S$
$t(J^m + A = J)$	$8M + 3S$
$t(A + A = J^m)$	$5M + 4S$
$t(A + A = J^c)$	$5M + 3S$
$t(A + A)$	$2M + S + I$
Удвоение	
Операция	Время выполнения
$t(2P)$	$7M + 5S$
$t(2J^c)$	$5M + 6S$
$t(2J)$	$4M + 6S$
$t(2J^m = J^c)$	$4M + 5S$
$t(2J^m)$	$4M + 4S$
$t(2A = J^c)$	$3M + 5S$
$t(2J^m = J)$	$3M + 4S$
$t(2A = J^m)$	$3M + 4S$
$t(2A = J)$	$2M + 4S$
$t(2A)$	$2M + 2S + I$

Представленный алгоритм работает быстрее аналогичных алгоритмов в проективной системе, системе Якобиана и Якобиана-Чудновских. При этом алгоритм также работает быстрее аффинных координат за счет увеличения числа умножений примерно в 3,6 раза, что не доступно ни одной из выше перечисленных систем координат.

Особый интерес представляет гибридная система координат, например, когда при сложении двух точек одна из них представлена в одной системе, а другая точка – в другой системе координат. В таблице 1 проанализированы возможные варианты организации гибридных систем координат и оценка времени выполнения операций с их использованием.

На основе комбинаций сложений-удвоений точек организуется процесс шифрования на эллиптической кривой, известный как скалярное умножение точки на константу – kP. При этом константа k является секретным ключом и проблема нахождения его для криптоаналитика при известных kP и P является труднорешимой. Например, для того, чтобы найти точку $25P$, может использоваться наглядный метод аддитивных цепочек, представленный ориентированным графом [3], показанным на рис. 7.

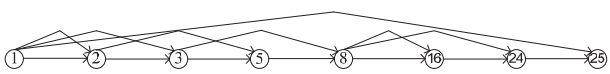

Рис. 7. Минимальная аддитивная цепочка для $25P$

Однако этот метод характеризуется избыточным числом итераций. Для сокращения числа итераций предлагается использовать бинарный алгоритм возведения числа в степень, переложенный на язык операций эллиптических кривых.

Вход: точка P известной аддитивной группы E точек эллиптической кривой; коэффициенты (k_0; k_1 … k_{n-1}) бинарного разложения константы

$$k = k_0 2^0 + k_1 2^1 + ... + k_{n-1} 2^{n-1}.$$

Выход: точка эллиптической кривой $b = kP$.

1. $b := 0$.
2. Для i от 1 до n: $b := 2b + P_E \cdot k_{n-i}$.
3. Вернуть b.

Пример. Вычислить с помощью бинарного алгоритма $25P$. Тогда

$$k = 25 = (k_0 = 1) \cdot 2^0 + (k_1 = 0) \cdot 2^1 +$$
$$+ (k_2 = 0) \cdot 2^2 + (k_3 = 1) \cdot 2^3 + (k_4 = 1) \cdot 2^4.$$

Рассмотрим работу алгоритма в этом случае:

0. $b := 0$.
1. $b := 2b + P \cdot (k_4 = 1) = P$.
2. $b := 2b + P \cdot (k_3 = 1) = 2P + P = 3P$.

3. $b := 2b + P \cdot (k_2 = 0) = 6P + 0 = 6P.$
4. $b := 2b + P \cdot (k_1 = 0) = 12P + 0 = 12P.$
5. $b := 2b + P \cdot (k_0 = 1) = 24P + P = 25P.$

Выход: $kP = 25P$.

Как видно, для получения точки $25P$ необходимо 5 итераций вместо 7 итераций метода аддитивных цепочек. Преимуществом предложенного алгоритма является требование всего одного ОЗУ для хранения промежуточных значений b.

Итак, разработанный метод показывает, что для того, чтобы эффективно использовать модифицированную систему координат Якобиана, необходимо выбирать ключи k, которые в двоичной системе имеют меньшее число единиц. При таком выборе ключа для выполнения скалярного умножения точек количество операций сложения уменьшается за счет увеличения числа удвоений, которые в модифицированной системе Якобиана выполняются с минимальным временем.

Литература

1. Cohen H. Efficient elliptic curve exponentiation // Advances in Cryptology-proceeding of ICICS'97. Springer-Verlag, 1997. – P. 282-290.
2. Chudnovsky D.V., Chudnovsky G.V. Sequences of numbers generated by addition in formal groups and new primary and factorization tests // Advances in Applied Math. №7, 1986. – P. 385-434.
3. Червяков Н.И., Головко А.Н. Модифицированный алгоритм Монтгомери скалярного умножения точки на эллиптической кривой // Компьютерные науки и технологии. Белгород: Изд. ГиК, 2009. – С. 104-108.

УДК 681.3

МАТЕМАТИЧЕСКИЕ МОДЕЛИ ХРАНЕНИЯ И ОБРАБОТКИ ДАННЫХ БОЛЬШОЙ РАЗМЕРНОСТИ С ВЫСОКОЙ СТЕПЕНЬЮ ДОСТОВЕРНОСТИ

Мезенцева О.С., Алексеев А.И.

В статье представлены математические модели распределенного хранения и обработки данных большой размерности, базирующиеся на аппарате пороговых схем и обладающие высокой степенью достоверности и отказоустойчивости. Для их построения используется аппарат модулярной арифметики, что позволяет добиться существенного повышения коэффициента ускорения и отказоустойчивости предложенных алгоритмов, открывает перспективы использования разработанных моделей в системах реального времени. Предложено эффективное отображение алгоритмических решений для реализации действий с данными большой размерности на аппаратную базу нейропроцессора NM6403.

Введение

Задачи факторизации, тестирования и определения простоты чисел специального вида, системы спутниковой навигации, и многие другие ресурсоемкие задачи требуют обработки больших объемов информации в широком диапазоне с высокой достоверностью и точностью вычислений. Как правило, подобные задачи сводятся к вычислительным проблемам, оперирующим целочисленными переменными, значения которых на несколько порядков превышают максимум машинного диапазона.

Для решения многих прикладных и теоретических проблем необходимо проведение вычислений уже в сверхбольших диапазонах, которые, с одной стороны, являются обобщением больших диапазонов, но в то же время принципиально отличаются от последних. Так как вычисления в них должны проводиться над потенциально бесконечными математическими объектами, их явные числовые записи невозможно или нецелесообразно хранить в памяти по причине принципиальной недостаточности вычислительных ресурсов, в результате чего в один момент времени возможны хранение и обработка лишь одного элемента представления. При таком подходе к распределенному хранению и обработке данных высокой размерности неизбежно повышается вероятность потери части представления числа. Выход из строя даже незначительного количества узлов вкупе с высокой трудоемкостью алгоритмов обработки чисел из большого и сверхбольшого диапазонов может привести к серьезным и сложно решаемым проблемам восстановления.

Параллельные вычислительные структуры являются идеальной основой для построения устойчивых к отказам вычислительных средств. Ключевую роль в процессе функционирования таких вычислительных устройств играет способность сохранения работоспособного состояния за счет снижения в допустимых пределах каких-либо показателей качества при возникновении сбоев и отказов в системе. Достоинство данного