COMPARING THE PERFORMANCE OF ALGORITHMS OF FORMATION DIGITAL SIGNATURE

Korolev M.[1], Lapina N.[2]

СРАВНЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМОВ ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Королев М. Е.[1], Лапина Н. А.[2]

[1]Королев Михаил Евгеньевич / Korolev Mihail – студент;
[2]Лапина Надежда Андреевна / Lapina Nadezhda - студент,
кафедра компьютерных систем и сетей, факультет информатики и систем управления,
Московский государственный технический университет им. Н. Э. Баумана, г. Москва

***Аннотация**: данная работа посвящена сравнению производительности асимметричных алгоритмов формирования электронной цифровой подписи, приведено краткое описание существующих алгоритмов и описаны их недостатки, показаны преимущества схемы на основе эллиптических кривых, описано уравнение эллиптической кривой, применяемое в криптографии, и дано подробное описание алгоритма на его основе, в работе рассмотрены способы задания кривых и продемонстрирована целесообразность использования алгоритмов на основе эллиптических кривых, заданных над векторными конечными полями.*
***Abstract**: this work is devoted to the comparison of performance of asymmetric algorithms of formation digital signature, in article briefed description of existing algorithms and described limitations, the advantages of the scheme based on elliptic curves, described equation elliptic curve used in cryptography, and a detailed description of the algorithm based on it, the paper discusses ways of defining curves and demonstrated the feasibility of using algorithms based on elliptic curves defined over finite fields by vector.*

***Ключевые слова**: электронно-цифровая подпись, асимметричный алгоритм, логарифмирование, эллиптическая кривая, векторное поле, шифрование.*
***Keywords:** digital signature, asymmetric algorithm, logarithm, elliptic curve, vector field, encryption.*

Основная информация об электронной подписи

Электронная цифровая подпись (ЭЦП) - некоторые данные, получаемые на основе других данных, позволяющие проверить авторство и целостность последних. В асимметричных алгоритмах ЭЦП используются два криптографических ключа. Секретный ключ, известный только автору документа, служит для шифрования файлов, с помощью него формируется ЭЦП. С помощью открытого ключа можно выполнить обратное криптографическое преобразование и проверить подлинность полученных данных. Дубликат открытого ключа находится в Удостоверяющем Центре.

Криптостойкость асимметричных криптосистем

В асимметричных криптосистемах используются односторонние функции, поэтому, чтобы найти по известному результату f(x) исходное значение x, необходимо решить сложную математическую задачу. Основные задачи и наиболее распространенные криптосистемы приведены в таблице 1.

Таблица 1. Основные ассиметричные криптосистемы

Математическая проблема	**Система**
Факторизация больших чисел. Для шифрования используется операция возведения в степень по модулю большого числа или же последовательности Люка.	RSA, LUC
Поиск квадратных корней составного числа.	Криптосистема Рабина
Дискретное логарифмирование (ДЛ) в конечном поле.	Схема Эль-Гамаля

ДЛ в группе точек эллиптической кривой.	Эллиптические кривые

В схеме Эль-Гамаля используется сложность задачи ДЛ в мультипликативных группах, имеющих большой простой порядок [1]. В качестве простого поля Галуа (конечного поля) GF(p), в котором содержится группа, обычно используется конечное кольцо Z_n , где n численно равно произведению простых чисел p и q, причем $p \neq q$. Кроме того, в некоторых алгоритмах используются расширенные конечные поля $GF(p^k)$, обычно это $GF(2^k)$ бинарное конечное поле. Как для GF(p), так и для $GF(p^k)$ существующие методы решения задачи ДЛ имеют субэкспоненциальную сложность порядка $O(\exp(c(\log p \log\log p)^d))$, где c и d некоторые константы, а p - размер поля. В схеме RSA используется задача факторизации числа n, которая эквивалентна задаче извлечения квадратного корня. Обе задачи тоже имеют субэкспоненциальную сложность, поэтому для обеспечения достаточной стойкости алгоритмов ЭЦП на основе RSA, LUC, схемы Эль-Гамаля и схемы Рабина при нынешних вычислительных мощностях размер порядка полей должен быть более 2^{10} бит, а значения $|n|>2^{10}$ бит [2], при этом обеспечивается уровень стойкости 2^{80} операций. С ростом вычислительных мощностей увеличивается и необходимый порядок полей, что негативно сказывается на производительности.

Однако на данный момент не существует субэкспонециального алгоритма решения задачи ДЛ в группе точек ЭК, поэтому достаточная криптостойкость достигается на ключах, с существенно меньшей длиной, это положительно отражается на времени создания и расшифровки ЭЦП [3]. Самые быстрые методы решения ДЛ на ЭК имеют сложность $O(q^{0.5})$, где q — порядок ЭК. Для обеспечения уровня стойкости в 2^{80} операций необходимо q^{160}.

Уравнение ЭК в криптографии

В настоящее время наилучшие показатели демонстрируют алгоритмы ЭЦП, основанные на конечных группах точек ЭК, групповой операцией является композиция точек. Конечные векторные поля и группы могут конкурировать с эллиптическими кривыми по эффективности синтезируемых алгоритмов ЭЦП, но на данный момент задача ДЛ в векторных структурах является малоизученной [4].

В криптографии под ЭК понимается набор точек, чьи координаты удовлетворяют некоторому уравнению ЭК и принадлежат конечному полю, в котором в виде формул заданы правила выполнения операций над парами координат. Формулы могут иметь различный вид, так как от характеристики поля зависит вид уравнения ЭК. Уравнение ЭК над произвольным полем F имеет вид:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \qquad (1)$$

где $a \in F$

Если характеристика данного поля (char F) не равна двум или трем, то уравнение ЭК можно записать в форме Вейерштрасса:

$$y^2 = x^3 + ax + b, \qquad (2)$$

где $a, b \in F$, причем

$$4a^3 + 27b^2 \neq 0 \qquad (3)$$

Описываемая этим уравнением кривая, к каждой точке которой можно провести касательную, называется гладкой ЭК. Если же

$$4a^3 = -27b^2, \qquad (4)$$

то кривая становится сингулярной, такие кривые не рекомендуется использовать, так как это снижает стойкость схемы ЭЦП [4].

Алгоритм генерации и проверки ЭЦП на основе ЭК

Алгоритм, являющийся стандартом в РФ, основан на ЭК и описан в ГОСТ Р 34.102012. Стандарт содержит алгоритм формирования ЭЦП на основе некоторых параметров, но не описывает механизм их генерации.

Согласно ГОСТ Р 34.102012 в качестве модуля ЭК используется простое число p, p>3. Порядок циклической подгруппы группы точек ЭК обозначается q, q - простое число, $2^{254}<q<2^{256}$ или $2^{508}<q<2^{512}$ [5].

ЭК задается уравнением:

$$y^2 = x^3 + ax + b \bmod p, \qquad (5)$$

где $a, b \in GF(p)$

Стандарт регламентирует использование точки P с координатами (x_P, y_P), такой что $P \neq O$, и произведение q на P равно 0. В качестве секретного ключа выбирается целое число d, а в открытым ключом является точка [5].

$$Q = dP \qquad (6)$$

Формирование подписи (R, S) осуществляется в соответствии с алгоритмом, описанным ниже. Вычисляется точка С ЭК:

$$C = kP, \qquad (7)$$

где k случайное целое число, 0<k<q.

И для этой точки вычисляется значение R:

$$R = x_C mod q, \qquad (8)$$

где x_C — координата точки С. Затем находится

$$S = (Rd + ke) mod q, \qquad (9)$$

$$e = H mod q, \qquad (10)$$

где H — значение хэш-функции от подписываемого сообщения.

Для значений R и S вычислить векторы $\overline{R}$ и $\overline{S}$, цифровой подписью будет являться конкатенация этих векторов. К исходному сообщению добавляется ЦП длиной 2^9 или 2^{10} бит и текстовое поле с дополнительной информацией, например с идентификаторами субъекта, подписавшего сообщение, или же датой и временем отправки сообщения.

Для проверки подписи необходимо вычислить R':

$$R' = x_C mod q, \qquad (11)$$

и проверить равенство R' = R. Координаты точки С находятся из уравнения:

$$C = ((Se^{-1})\ mod\ q)G\ +\ ((q - R)e^{-1} mod\ q)Q, \qquad (12)$$

Производительность данного алгоритма на порядок выше, чем производительность RSA и DSA. ГОСТ Р 34.102012, также содержит требования к длине хеш-кода, необходимый размер 256 или же 512 бит.

Эллиптическая криптография над векторными полями

В существующих алгоритмах на основе ЭК используются либо конечное поле Z_p — кольцо вычетов по модулю простого числа, либо расширенные конечные поля $GF(p^k)$, обычно это $GF(2^k)$ бинарное конечное поле. Математические операции при этом являются обычными операциями в поле, над которым построена ЭК: умножение в полях представляет собой умножение по модулю p, т.е. результат арифметического умножения делится на простое число p. Кроме того, элементы поля $GF(p^k)$ можно представить как многочлены над GF(p) степени не выше n − 1. Если элементы в $GF(p^k)$ представлены в стандартном базисе

$$B\alpha = \{\alpha^0, \alpha^1, \dots, \alpha^{k-1}\}, \qquad (13)$$

где $\alpha \in GF(p^k) -$ генератор базиса Bα,то умножение в базисе представляет собой полиномиальное умножение по модулю неприводимого многочлена g(x) над GF(p),причем g(α)=0 [6]. При таком представлении разбить вычисления на несколько одновременно выполняемых операций трудно.

Существует также векторный способ представления ЭК. Если формировать поля в векторных пространствах, то все операции выполняются над множеством координат векторов, при этом координаты вычисляются по отдельности. Следовательно, можно распараллелить вычисления и повысить скорость создания и проверки ЭЦП при задании ЭК над полями, сформированными в конечных k-мерных векторных пространствах. Все конечные поля одного порядка изоморфны, поэтому использование векторной формы представления не повлияет на структурные свойства ЭК и сложность задачи ДЛ на ЭК, безопасность ЭЦП останется прежней.

Сравнение производительности

При выполнении умножения ЭК требуются операции сложения, умножения и операция инвертирования (вычисления мультипликативного обратного) в конечном поле, которая гораздо медленнее умножения, что значительно влияет на сложность вычислений. Используя проективные координаты при векторном представлении, можно устранить операции инвертирования, но при этом увеличивается количество операций умножения [4]. Поэтому наибольшее влияние на производительность оказывает сложность операции умножения.

При выполнении равенства (14)

$$|b| = k|p|, \qquad (14)$$

где |p| длина числа p в битах, размеры порядков векторного поля $GF(p^k)$ и простого поля Z_b равны. При этом производительность алгоритмов будет примерно одинаковой, так как сложность операции умножения M(GF(p)) в поле GF(p) пропорциональна $|p|^2$, а операция умножения элементов поля $GF(p^k)$ включает k^2 операций умножения в поле GF(p) [2]. Количество делений уменьшится в k раз, если делить на p сумму произведений пар координат, а не каждую пару в отдельности перед сложением. Это приводит к увеличению скорости вычислений примерно в k раз [2]. Возрастанием сложности деления из-за увеличения делимого можно пренебречь.

Выводы

Алгоритмы на основе эллиптических кривых являются наиболее эффективными для формирования ЭЦП. Реализация алгоритмов эллиптической криптографии на основе векторных полей обеспечивает значительный рост производительности при заданном уровне стойкости. Это обусловлено следующим:

- в полях, заданных в векторных пространствах, операция умножения является свободной от операции инвертирования;
- задача ДЛ не имеет решения субэкспоненциальными методами при корректном выборе размерности конечного векторного пространства;
- есть возможность распараллелить вычисления, так как при умножении координаты результирующего вектора могут быть вычислены одновременно;
- в векторных полях, при заданном размере порядка, сложность операций ниже, чем в конечных полях.

Литература

1. *Молдовян Н. А.* Практикум по криптосистемам с открытым ключом. СПб.: БХВ-Петербург, 2007. 298 с.
2. *Молдовян Н. А.* Теоретический минимум и алгоритмы цифровой подписи. СПб.: БХЧ Петербург, 2010. 304 с.: (Учебное пособие).
3. *Бухштаб А. А.* Теория чисел. М.: Просвещение, 1996. 384 с.
4. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на элептических кривых. М.: КомКнига, 2006. 274 с.
5. ГОСТ Р 34.102012. Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Введ. 20120807; взамен ГОСТ Р 34.102001.
6. *Гашков С. Б., Сергеев И. С.* Сложность вычислений в конечных полях, Фундаментальная и прикладная математика. М.: Открытые Системы, 2011/2012. Том 17. № 4. С. 95—131.