РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2457535

СПОСОБ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКОЙ ИЛИ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Патентообладатель(ли): ***Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный политехнический университет" (ФГБОУ ВПО "СПбГПУ") (RU)***

Автор(ы): ***Ростовцев Александр Григорьевич (RU)***

Заявка № **2010121292**

Приоритет изобретения **25 мая 2010 г.**

Зарегистрировано в Государственном реестре изобретений Российской Федерации ***27 июля 2012 г.***

Срок действия патента истекает **25 мая 2030 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 457 535** (13) **C2**

(51) МПК
G06F 21/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010121292/08, 25.05.2010**

(24) Дата начала отсчета срока действия патента:
25.05.2010

Приоритет(ы):
(22) Дата подачи заявки: **25.05.2010**

(43) Дата публикации заявки: **27.11.2011** Бюл. № 33

(45) Опубликовано: **27.07.2012** Бюл. № 21

(56) Список документов, цитированных в отчете о поиске: **RU 2380838 C1, 27.01.2010. RU 2308080 C2, 10.10.2007. US 2009/0214023 A1, 27.08.2009. RU 2369974 C1, 10.10.2009.**

Адрес для переписки:
195251, Санкт-Петербург, ул. Политехническая, 29, ФГБОУ ВПО "Санкт-Петербургский государственный политехнический университет" , Отдел интеллектуальной и промышленной собственности

(72) Автор(ы):
Ростовцев Александр Григорьевич (RU)

(73) Патентообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Санкт-Петербургский государственный политехнический университет" (ФГБОУ ВПО "СПбГПУ") (RU)

RU 2457535 C2

(54) СПОСОБ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКОЙ ИЛИ ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

(57) Реферат:

Способ относится к электросвязи и вычислительной технике и позволяет ускорить формирование и проверку электронной цифровой подписи. Технический результат заявленного изобретения заключается в увеличении скорости формирования и проверки электронной цифровой подписи с использованием эллиптических или гиперэллиптических кривых. Способ, заключающийся в преобразовании битовых строк и выполнении операций с битовыми строками, в котором при формировании или при проверке подписи умножают по крайней мере одну заранее определенную точку (соответственно приведенный дивизор) P простого порядка q эллиптической (соответственно гиперэллиптической) кривой на целое число k путем сложений и удвоений, при формировании подписи допускается случайный выбор числа k, причем на первом этапе выбирают число w=-2 при q=1,3 (mod 8) или w=2 при q=1,7 (mod 8), вычисляют значение $t=\sqrt{w} \pmod q$, а на втором этапе число k преобразовывают в систему счисления с основанием t: $k=K_0+K_1t+\ldots+K_{2h}t^{2h}+K_{2h+1}t^{2h+1}$, где все коэффициенты $K_0, \ldots, K^{2h+1}$ принимают значения 0, 1 или -1, а число 2h близко к $\log_2 q$, а в ходе рекурсивного перехода к предыдущей цепочке коэффициентов выполняют n/2 удвоений точки (приведенного дивизора) R. 3 з.п. ф-лы.

RU 2457535 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 457 535** (13) **C2**

(51) Int. Cl.
G06F 21/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010121292/08, 25.05.2010**

(24) Effective date for property rights:
25.05.2010

Priority:
(22) Date of filing: **25.05.2010**

(43) Application published: **27.11.2011** Bull. 33

(45) Date of publication: **27.07.2012 Bull. 21**

Mail address:
195251, Sankt-Peterburg, ul. Politekhnicheskaja, 29, FGBOU VPO "Sankt-Peterburgskij gosudarstvennyj politekhnicheskij universitet" , Otdel intellektual'noj i promyshlennoj sobstvennosti

(72) Inventor(s):
Rostovtsev Aleksandr Grigor'evich (RU)

(73) Proprietor(s):
Federal'noe gosudarstvennoe bjudzhetnoe obrazovatel'noe uchrezhdenie vysshego professional'nogo obrazovanija "Sankt-Peterburgskij gosudarstvennyj politekhnicheskij universitet" (FGBOU VPO "SPbGPU") (RU)

(54) METHOD OF GENERATING AND VERIFYING ELECTRONIC DIGITAL SIGNATURE BASED ON ELLIPTIC OR HYPERELLIPTIC CURVE

(57) Abstract:

FIELD: information technology.

SUBSTANCE: method involves transformation of bit strings and performing operations with bit stings, in which during generation or verification of a signature, at least one predetermined point (corresponding reduced divisor) P of the simple order q on the elliptic (corresponding hyperelliptic) curve is multiplied by an integer k via summation and doubling; when generating the signature, random selection of the number k is allowed, wherein the first step involves selecting a number w=-2 for q=1, 3 (mod 8) or w=2 for q=1, 7 (mod 8), the value $t=\sqrt{w}$ (mod q) is calculated; and at the second step, the number k is transformed to a number system with base t: $k=K_0+K_1t+\ldots+K_{2h}t^{2h}+K_{2h+1}t^{2h+I}$, where all coefficients $K_0,\ldots, K^{2h+1}$ assume values 0, 1 or -1, and a number 2h close to $\log_2 q$, and during recursive transition to the previous chain of coefficients, n/2 doublings of the point (reduced divisor) R are carried out.

EFFECT: high speed of generating and verifying an electronic digital signature using elliptic or hyperelliptic curves.

4 cl, 1 app

RU 2457535 C2

RU 2457535 C2

Изобретение относится к электросвязи и вычислительной технике, в частности к области криптографической защиты электронных данных, передаваемых по телекоммуникационным сетям и сетям ЭВМ, с использованием эллиптических и гиперэллиптических кривых, и может быть использовано в системах передачи данных. Используемые в данном описании специфические термины поясняются в Приложении 1.

Известны системы электронной цифровой подписи (ЭЦП) электронного документа на основе эллиптических кривых [ГОСТ Р 34.10-2001. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Госстандарт России, М., 2001]; [ANSI X9.62. Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005, http://www.comms.scitech.susx.ac.uk/fft/crypto/ecdsa.pdf], предусматривающие процессы формирования и проверки ЭЦП. Указанные стандарты ЭЦП по сути являются вариантами схем ЭЦП Эль-Гамаля [ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms // IEEE Transactions on Information Theory. 1985. Vol.IT-31. P.469-472.] и Шнорра [Schnorr C.P. Efficient identification and signatures for smart cards // Advances in Cryptology - CRYPTO '89. Lecture Notes in Computer Science. Springer-Verlag. 1990. Vol.435. P.239-252.].

Предусмотренная известными способами ЭЦП эллиптическая кривая состоит из конечного числа точек P=(x, y), удовлетворяющих уравнению $y^2+a_1xy=x^3+a_2x^2+a_4x+a_6$, допускающих операции сложения и удвоения, см. также Приложение 1. Вычисление точки P+…+P соответствует умножению (называемому также скалярным умножением) точки P на целое число k, обозначаемое kP; умножение точки на число выполняется с использованием сложений и удвоений точек.

Известны способы электронной цифровой подписи на основе гиперэллиптических кривых [FR WO/2004/084485, опубл. 11.03.2004], предусматривающие выполнение действий с битовыми строками (БС), представляющими приведенные дивизоры (см. также Приложение 1).

В известных системах ЭЦП обрабатываемые данные представлены битовой строкой или набором битовых строк. Под битовой строкой (БС) понимается электромагнитный сигнал в цифровой двоичной форме, параметром которого является число битов и порядок следования нулевых и единичных значений. Битовые строки допускают операцию конкатенации, логические и арифметические операции. Формирование и проверка ЭЦП заключается в выполнении действий с БС (преобразованиях БС и выполнении операций с БС) и выполняется с помощью вычислительных устройств, например персональных компьютеров или смарт-карт [доступно с http://www.aloaha.com/press_en/elliptic-curves-and-sha-256-support.php].

В соответствии с Федеральным законом об электронной цифровой подписи юридическая значимость ЭЦП на территории РФ обеспечивается только при реализации ее в соответствии с ГОСТ Р 34.10-2001. Поэтому практически наиболее интересны способы ЭЦП, реализованные в соответствии с действующими стандартами.

Стандарты подписи России [ГОСТ Р 34.10-2001. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Госстандарт России, М., 2001], США [ANSI X9.62. Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005, доступно с http://www.comms.scitech.susx.ac.uk/fft/crypto/ecdsa.pdf], Германии [Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway. Notifications in

Accordance with the Electronic Signature Act and the Electronic Signature Ordunance (Overview of suitable algorithms) // Federal Gazette, No 19, pp.376, February 5, 2008 (in German)] аналогичны и различаются размером задачи - порядком точки P эллиптической кривой (длиной цикла {P, 2P, 3P, …}), который должен быть большим простым числом q, длина q в ГОСТ Р 34.10-2001 не менее 254 бит, а в ECDSA и стандарте подписи Германии не менее 160 бит.

Стандарты ЭЦП, использующие эллиптические кривые, могут быть легко адаптированы для гиперэллиптических кривых, при этом точка эллиптической кривой заменяется на приведенный дивизор (ПД) гиперэллиптической кривой, сложение точек эллиптической кривой заменяется сложением ПД, а число точек эллиптической кривой заменяется числом ПД гиперэллиптической кривой [Scholten J., Vercauteren F. An introduction to elliptic and hyperelliptic curve cryptography and the NTRU cryptosystem, доступно с http://homes.esat.kuleuven.be/~fvercaut/papers/cc03.pdf], [Ростовцев А.Г. Алгебраические основы криптографии. - СПб.: Мир и Семья, Интерлайн, 2000, главы 6, 7], см. также Приложение. Поэтому для изложения сути заявленного способа достаточно рассмотреть только преобразования БС и операции с БС, предусмотренные в ГОСТ Р 34.10-2001.

Параметрами системы ЭЦП является эллиптическая кривая и точка P простого порядка $q>2^{254}$ (см. Приложение 1) длиной 254-256 бит. Секретным ключом формирования ЭЦП является натуральное число d, $1\leq d\leq q-1$. Открытым ключом проверки ЭЦП является точка Q=dP, которая задается парой координат длиной по 256 бит каждая. Таким образом, точка эллиптической кривой задается битовой строкой длиной 512 бит.

Для формирования ЭЦП вырабатывают случайную БС, представляющую целое число k, $0<k<q$, вычисляют БС, представляющую точку kP, и вычисляют БС, представляющую собственно подпись для электронного документа. В ходе проверки ЭЦП на основе БС, представляющей подпись, и соответствующего электронного документа вычисляют числа z_1, z_2, $0<z_1$, z_2, $<q$, и вычисляют БС, представляющие точки z_1P, z_2Q, с помощью которых судят о подлинности подписи. При умножении точки на число выполняются преобразования БС и логические и арифметические операции с БС.

Скорость формирования и проверки ЭЦП определяется числом выполняемых операций сложения и умножения точек эллиптической кривой. Для повышения скорости процесса формирования и проверки ЭЦП достаточно снизить число операций, выполняемых при умножении фиксированной точки эллиптической кривой на заранее неопределенное число.

Известно устройство, где числа представлены в системе счисления с нецелым основанием [RU 99103806, МПК G06F 7/49, опубл. 27.01.2001]. Однако оно не может быть использовано в системах ЭЦП.

Известен способ [RU 2232476, МПК H04L 9/30, опубл. 7.10.2004]. Недостатком этого способа является то, что он практически не увеличивает скорость формирования и проверки ЭЦП.

Известны способы формирования и проверки ЭЦП [RU 2382505, МПК H04L 9/32, опубл. 20.02.2010], [RU 2380838, МПК H04L 9/32, опубл. 27.01.2010]. Недостатком этих способов является то, что они не совместимы с ГОСТ Р 34.10-2001.

Известны способы формирования и проверки ЭЦП на эллиптической кривой [US 6898284, 7590235 МПК H04L 9/30]. Недостатком данных способов является то, что они не применимы к большинству используемых на практике эллиптических кривых.

Известен способ формирования и проверки ЭЦП на эллиптической кривой [US 20030123655, H04K 1/00, опубл. 29.01.2002], предусматривающий два этапа при умножении точки на число. Недостатком способа является то, что он не применим к подавляющему числу эллиптических кривых, которые могут быть использованы для криптографических целей, и не совместим с ГОСТ Р 34.10-2001.

За прототип принят способ умножения фиксированной точки P простого порядка q на число k, представленное в двоичной системе счисления при формировании и проверке ЭЦП, заключающийся в использовании операций сложения и удвоения точек в соответствии с двоичным представлением числа k, предусматривающий разбиение числа k на цепочки небольшой длины n и использование таблицы предвычислений [US 20090214023, H04L 9/30, опубл. 26.02.2008]. Способ предусматривает два этапа. На первом этапе вычисляются вспомогательные БС, зависящие от P и q и представляющие произведения всевозможных значений цепочек на точку P. При этом каждая из указанных вспомогательных БС состоит из идентификатора, соответствующего значению цепочки, и значения точки эллиптической кривой. На втором этапе точку kP вычисляют рекурсивно, начиная со старших разрядов. При этом вектор двоичных коэффициентов числа k разбивают на цепочки n бит, выбирают вспомогательную БС, полученную на первом этапе, идентификатор которой соответствует старшей цепочке, выбирают из указанной БС координаты точки эллиптической кривой и присваивают их значение точке R. Под присвоением значения точке понимается присвоение ее координатам соответствующих значений. Выполняют рекурсивный переход к предыдущей цепочке. Для этого выполняют n удвоений точки R, значение полученной суммы присваивают точке R, выбирают вспомогательную БС, первая часть которой соответствует указанной предыдущей цепочке, складывают точку R с точкой, заданной второй и третьей частями указанной вспомогательной БС, и значение суммы присваивают точке R. Рекурсию повторяют до тех пор, пока не будет использована цепочка младших коэффициентов.

Например, при длине цепочки 4 бита на первом этапе подготавливают вспомогательные БС вида $(1\|P)$, $(2\|2P)$, $(3\|3P)$, … $(15\|15P)$, где $\|$ - символ конкатенации битовых строк, левая часть битовой строки - идентификатор, правая часть - координаты точки эллиптической кривой. На втором этапе для $k = 56103 = 1101\|1011\|0010\|0111\|$ (старшие разряды слева) получают $k=13*16^3+11*16^2+2*16+7$. При вычислении точки kP выбирают вспомогательную БС с идентификатором 13, соответствующим старшему коэффициенту числа k, выбирают из этой битовой строки точку 13P, выполняют 4 удвоения этой точки, полученную точку складывают с точкой 11P, которую выбирают как вторую и третью части БС, первая часть которой имеет код 11 второго коэффициента числа k, выполняют 4 удвоения полученной суммы, полученную точку складывают с точкой 2P, которую выбирают как вторую и третью части БС, первая часть которой имеет код 2 третьего коэффициента числа k, выполняют 4 удвоения, полученную точку складывают с точкой 7P, которую выбирают как вторую и третью части БС, первая часть которой имеет код 7 четвертого коэффициента числа k, и получают окончательный результат. Недостатком этого способа является низкая скорость обработки данных, обусловленная тем, что число удвоений точки равно длине БС, представляющей число k.

Существенные признаки прототипа:

1. Способ умножения фиксированной точки P простого порядка q эллиптической

кривой на целое число k, причем допускается случайный выбор числа k, который может использоваться при формировании и проверке ЭЦП, обрабатываемые данные представляют собой БС, способ предусматривает преобразование БС и выполнение операций с БС и состоит из двух этапов: на первом этапе подготавливают вспомогательные БС, на втором этапе выполняют умножение P на k путем удвоений и сложений точек эллиптической кривой с помощью вспомогательных БС.

2. Число k представляют в системе счисления с целым основанием.

3. На первом этапе выбирают длину цепочки n и вычисляют БС, представляющие точки m_iP, где $1 \le m_i < 2^n$ (для целых чисел m_i, представленных всеми возможными ненулевыми значениями цепочек), причем каждая БС содержит идентификатор (число m_i) и координаты точки m_iP.

4. На втором этапе вектор коэффициентов двоичного числа k разбивают на цепочки размера n. Умножение точки на число выполняют рекурсивно, начиная со старших разрядов. При этом из вспомогательной БС, идентификатор которой соответствует коду старшей цепочки, выбирают точку эллиптической кривой и значение этой точки присваивают точке R. Рекурсивный переход к предыдущей цепочке состоит из n удвоений точки R и присвоения результата точке R, выбора точки эллиптической кривой из БС, идентификатор которой соответствует значению предыдущей цепочки, сложения этой точки с точкой R и присвоения значения суммы точке R.

Задачей заявляемого технического решения является увеличение скорости формирования и проверки электронной цифровой подписи с использованием эллиптических или гиперэллиптических кривых.

Поставленная цель достигается тем, что число k переводят в систему счисления с основанием $\sqrt{\pm 2}$ так, что длина БС, представляющей число k, практически не меняется, в результате при использовании четного n число удвоений точек сокращается примерно вдвое. Указанный перевод числа k возможен благодаря тому, что для чисел вида $k_0 + k_1\sqrt{\pm 2}$, где k_0, k_1 - целые числа, существует алгоритм Евклида [Lemmermeyer F. The Euclidean algorithm in algebraic number fields, Expo. Math. 13, No.5 (1995), 385-416]. При этом при формировании ЭЦП случайное число k изначально генерируют в виде $k = k_0 + k_1\sqrt{\pm 2}$.

Ниже перечислены существенные признаки предлагаемого способа. Поскольку способ применим для формирования и проверки ЭЦП на основе как эллиптических, так и гиперэллиптических кривых, то соответствующие существенные признаки для гиперэллиптических кривых указаны в скобках.

1. Способ формирования и проверки электронной цифровой подписи на основе эллиптической или гиперэллиптической кривой, заключающийся в преобразовании БС и выполнении операций с БС, в котором при формировании или при проверке ЭЦП умножают по крайней мере одну заранее определенную точку (ПД) P простого порядка q эллиптической (гиперэллиптической) кривой на целое число k путем сложений и удвоений, при формировании ЭЦП допускается случайный выбор числа k, причем для указанного умножения используют два этапа: на первом этапе выбирают четную длину цепочки n и подготавливают вспомогательные БС, содержащие произведение точки эллиптической кривой (ПД гиперэллиптической кривой) на целые числа, представленные всеми допустимыми значениями цепочек, причем каждая указанная БС содержит хотя бы один идентификатор, на втором этапе рекурсивно выполняют указанное умножение с использованием указанных вспомогательных БС, при этом вектор коэффициентов числа к разбивают на цепочки длины n, выбирают

вспомогательную БС, один из идентификаторов которой соответствует старшей цепочке, и значение этой точки (приведенного дивизора) этой БС присваивают точке эллиптической кривой (ПД гиперэллиптической кривой) R, и выполняют рекурсивный переход к предыдущей цепочке, присваивая точке R значения удвоений R и суммы R с точкой эллиптической кривой (ПД гиперэллиптической кривой) БС, один из идентификаторов которой соответствует предыдущей цепочке.

2. На первом этапе выбирают число w=-2 при q≡1, 3 (mod 8) или w=2 при q≡1, 7 (mod 8), вычисляют значение $t \equiv \sqrt{w} \pmod q$, а на втором этапе число k преобразовывают в систему счисления с основанием t:

$$k = \sum_{i=0}^{2h+1} t^i K_i ,$$

где все коэффициенты K_i принимают значения 0, 1 или -1 и $2h \approx \log_2 q$, а в ходе рекурсивного перехода к предыдущей цепочке коэффициентов выполняют n/2 удвоений точки (приведенного дивизора) R.

3. При формировании подписи случайное число k выбирают в виде пары целых случайных чисел (k_0, k_1) так, что выполняется условие $|k_0^2 - wk_1^2| < q$, и полагают $k = k_0 + tk_1$.

4. Если n≥4 и w=-2, то каждая вспомогательная битовая строка содержит все эквивалентные идентификаторы, обладающие одинаковым значением по модулю q, либо каждая вспомогательная битовая строка содержит идентификатор, значение которого равно абсолютно наименьшему из эквивалентных идентификаторов, а на втором этапе выполняют преобразование цепочек коэффициентов числа k, при котором цепочки вида (…, 1, z, 1, …) заменяются на цепочки вида (…, -1, z, 0, …), а цепочки вида (…, -1, z, -1, …) заменяются на цепочки вида (…, 1, z, 0, …,) причем z означает любую из цифр 0, 1, -1.

5. На первом этапе дополнительно подготавливают БС, представляющие целые числа A и B, такие, что выполняются условия: $eq = A^2 - wB^2$, e=±1, и целое число A+Bt делится на q.

6. На втором этапе вычисляют ближайшее к дроби (Ak/(eq)) целое число n_1 и ближайшее к дроби (Bk/(eq)) целое число n_2, вычисляют числа $k_0 = k - An_1 + wBn_2$, $k_1 = -Bn_1 + An_2$, преобразовывают их в двоичный вид $k_0 = k_{00} + 2k_{01} + \ldots + 2^h k_{0h}$, $k_1 = k_{10} + 2k_{11} + \ldots + 2^h k_{1h}$ и для i=0, 1, …, 2h+1 полагают $K_{2i} = \pm k_{0i}$, $K_{2i+1} = \pm k_{1i}$ для всех i≥0, где знаки определяют с учетом знака w.

В п.1 указаны существенные признаки, общие с прототипом, в п.2 указаны отличительные признаки, общие для данного изобретения. В пп.3-6 указаны признаки для вариантов исполнения.

Способ содержит два этапа. На первом этапе подготавливают вспомогательные битовые строки, зависящие от P, q. Выбирают числа w=-2 при q≡1, 3 (mod 8) или w=2 при q≡±1 (mod 8), вычисляют значение $t \equiv \sqrt{w} \pmod q$, выбирают длину цепочки - малое четное число n (на практике обычно n=2 или n=4, так как необходимый объем памяти растет как экспонента от n), и подготавливают следующие вспомогательные БС, зависящие от P и q: вычисляют точки (ПД), представляющие все возможные значения точек (ПД) вида $\left(\sum_{i=0}^{n-1} c_i t^i\right) P$, где c_i=0, 1 или -1, при этом для четных i все c_i либо неотрицательны либо неположительны и для нечетных i все c_i либо

неотрицательны либо неположительны. Поскольку по точке (ПД) легко найти противоположную точку (противоположный ПД), достаточно вычислить точки (ПД) вида $\left(\sum_{i=0}^{n-1} c_i t^i\right)P$ с точностью до знака суммы $\sum_{i=0}^{n-1} c_i t^i$, являющейся идентификатором.

Для n=2 возможны следующие значения пар (c_0, c_1): (0, 0) (соответствует нулевому элементу группы, см. Приложение 1), (1, 0) (соответствует заданной точке (ПД) P), (-1, 0) (соответствует точке (ПД) -P), (0, 1), (0, -1) (противоположна к предыдущей точке (предыдущему ПД)), (1, 1), (-1, -1) (противоположна к предыдущей точке (предыдущему ПД)), (1, -1), (-1, 1) (противоположна к предыдущей точке (предыдущему ПД)). Поэтому кроме P вычисляют 3 точки (ПД) {tP, (1+t)P, (1-t)P)}.

Для n=4 и w=2 вычисляют БС, представляющие 23 точки (ПД), здесь множитель элемента P является идентификатором:

$$\sqrt{2}P,\ \left(1+\sqrt{2}\right)P,\ \left(1-\sqrt{2}\right)P,\ 2P,\ (1+2)P=3P,\ \left(\sqrt{2}+2\right)P=\left(2+\sqrt{2}\right)P,$$

$$\left(-\sqrt{2}+2\right)P=\left(2-\sqrt{2}\right)P,\ \left(1+\sqrt{2}+2\right)P=\left(3+\sqrt{2}\right)P,\ \left(1-\sqrt{2}+2\right)P=\left(3-\sqrt{2}\right)P,$$

$$\sqrt{2}^3P=2\sqrt{2}P,\ \left(1+\sqrt{2}^3\right)P=\left(1+2\sqrt{2}\right)P,\ \left(1-\sqrt{2}^3\right)P=\left(1-2\sqrt{2}\right)P,$$

$$\left(\sqrt{2}+\sqrt{2}^3\right)P=3\sqrt{2}P,\ \left(1+\sqrt{2}+\sqrt{2}^3\right)P=\left(1+3\sqrt{2}\right)P,$$

$$\left(1-\sqrt{2}-\sqrt{2}^3\right)P=\left(1-3\sqrt{2}\right)P,\ \left(2+\sqrt{2}^3\right)P=2+2\sqrt{2}P,\ 2-2\sqrt{2}P,$$

$$\left(1+2+\sqrt{2}^3\right)P=\left(3+2\sqrt{2}\right)P,\ \left(1+2-\sqrt{2}^3\right)P=\left(3-2\sqrt{2}\right)P,$$

$$\left(\sqrt{2}+2+\sqrt{2}^3\right)P=\left(2+3\sqrt{2}\right)P,\ \left(-\sqrt{2}+2-\sqrt{2}^3\right)P=\left(2-3\sqrt{2}\right)P,$$

$$\left(1+\sqrt{2}+2+\sqrt{2}^3\right)P=\left(3+3\sqrt{2}\right)P,\ \left(1-\sqrt{2}+2-\sqrt{2}^3\right)P=\left(3-3\sqrt{2}\right)P.$$

Для n=4 и w=-2 вычисляют БС, представляющие 11 точек (ПД):

$$2P,\ \sqrt{-2}P,\ 2\sqrt{-2}P,\ \left(1+\sqrt{-2}\right)P,\ \left(1-\sqrt{-2}\right)P,\ \left(2+2\sqrt{-2}\right)P,\ \left(2-2\sqrt{-2}\right)P,$$

$$\left(2+\sqrt{-2}\right)P,\ \left(2-\sqrt{-2}\right)P,\ \left(1+2\sqrt{-2}\right)P,\ \left(1-2\sqrt{-2}\right)P,$$

поскольку справедливо равенство $1+\sqrt{-2}^2=-1$, задающее эквивалентность некоторых сумм $\left(c_0+c_1\sqrt{-2}+c_2\sqrt{-2}^2+c_3\sqrt{-2}^3\right)P$. Например,

$$-\left(1-\sqrt{-2}\right)P=\left(1+\sqrt{-2}+\sqrt{-2}^2\right)P=\left(1-\sqrt{-2}+\sqrt{-2}^2-\sqrt{-2}^3\right)P.$$

При формировании ЭЦП по ГОСТ Р 34.10-2001, ECDSA, схемам Эль-Гамаля, Шнорра необходимо выбрать случайное число k и умножить на него точку (ПД) P. В этом случае выбирают пару случайных целых чисел k_0, k_1, суммарная длина которых близка к длине БС, представляющей число q так, что выполняется условие $|k_0^2-wk_1^2|<q$, полагают $k=k_0+k_1t$, при этом перевод числа k в систему счисления с основанием t выполняют следующим образом. Находят представление чисел k_0, k_1 в системе счисления с основанием 2: $k_0=k_{00}+2k_{01}+2^2k_{02}+\ldots2^hk_{0h}$ и $k_1=k_{10}+2k_{11}+2^2k_{12}+\ldots+2^hk_{1h}$. Находят число k в системе счисления с основанием t: $k=\sum_{i=0}^{2h+1} t^iK_i$, где $K_{2i}=\pm k_{0i}$, $K_{2i+1}=\pm k_{1i}$, знак определяется с учетом равенства $t^2=\pm2$. Вектор коэффициентов (K_0, …, K_{2h+1}) при необходимости дополняют нулями справа так, чтобы его длина, равная 2h+2, была кратна n. В остальном процесс формирования ЭЦП аналогичен

ГОСТ Р 34.10-2001 (ECDSA, схемам Эль-Гамаля, Шнорра). Сформированная ЭЦП для электронного документа представляется битовой строкой.

Для проверки ЭЦП по схемам ГОСТ Р 34.10-2001, ECDSA, а также по схемам Эль-Гамаля, Шнорра необходимо умножить точку (ПД) P на целое число k, зависящее от электронного документа или БС, представляющей ЭЦП. В этом случае выполняют перевод k в систему счисления с основанием t. Для этого на первом этапе находят БС, представляющие числа A, B, такие, что выполняются условия $eq=A^2-wB_2$, где $e=\pm 1$, и $A+Bt\equiv 0 \pmod q$. Числа A, B всегда существуют при $w=-2$ и $q\equiv 1, 3 \pmod 8$ и при $w=2$ и $q\equiv 1, 7 \pmod 8$. Их можно найти алгоритмом Полларда и Шнорра [Pollard J.M., Schnorr CP. An efficient solution of the congruence $x^2+ky^2=m \pmod n$ // IEEE Transactions on Information Theory. 1987. Vol.IT-33. №.5. p.702-709], см. также Приложение 1, при $w=-2$ числа можно найти с использованием пакета MATHEMATICA командой QuadraticRepresentation[2,q] [http://documents.wolfram.com/v5/Add-[onsLinks/StandardPackages/NumberTheory]./NumberTheoryFunctions. html].

Длина БС, представляющей значение $t \equiv \sqrt{w} \pmod q$, не превышает длины строки, представляющей число q, при этом выполняется условие $t^2-w\equiv 0 \pmod q$. Для вычисления t можно воспользоваться алгоритмом, описанным в работе [Ростовцев А.Г. Алгебраические основы криптографии. - СПб.: Мир и Семья, Интерлайн, 2000, глава 7], см. также Приложение 1.

На втором этапе число k переводят в систему счисления с основанием t с коэффициентами из множества {0, 1, -1}. Для этого находят ближайшее целое число n_1 к дроби Ak/(eq) и ближайшее целое число n_2 к дроби Bk/(eq), находят целые числа $k_0=k-An_1+wBn_2$, $k_1=-Bn_1+An_2$. При этом выполняется условие $k\equiv k_0+tk_1 \pmod q$, а длина БС, представляющих числа k_0, k_1, оказывается минимальной. Число k переводят в систему счисления с основанием t так же, как описано выше: $k=\sum_{i=0}^{2h+1} t^i K_i$. Вектор коэффициентов $(K_0, \ldots, K_{2h+1})$ при необходимости дополняют нулями справа так, чтобы его длина, равная 2h+2, была кратна n.

Для умножения точки (ПД) P на число k вектор коэффициентов $(K_0, \ldots, K_{2h+1})$ разбивают на цепочки из n элементов и вычисляют число k в виде:

$$k=\sum_{i=0}^{\frac{2h+2}{n}-1} w^{\frac{in}{2}}\left(K_{in}+tK_{in+1}+\ldots+t^{n-1}K_{in+n-1}\right).$$

В соответствии со значением цепочки старших коэффициентов:

$(K_{2h-n+2}+tK_{2h-n+3}+\ldots+t^{n-1}K_{2h+1})$

выбирают найденную на первом этапе БС с соответствующим идентификатором, из этой БС выбирают точку (ПД) вида:

$R=(K_{2h-n+2}+tK_{2h-n+3}+\ldots+t^{n-1}K_{2h+1})P$.

Если вспомогательные БС, представляющие точки (ПД), определены до знака, то может потребоваться смена знака выбранной точки (ПД). Выполняют рекурсивный переход к предыдущей цепочке коэффициентов. Для этого выполняют n/2 последовательных удвоений точки (ПД) R, при каждом удвоении заменяя R на 2R, при этом в случае нечетного n и $w=-2$ до начала удвоений или после их окончания заменяют R на -R, результат, равный $w^{n/2}R$, складывают с точкой (ПД), представленной вспомогательной БС, идентификатор которой соответствует предыдущей цепочке коэффициентов, при необходимости заменяя эту точку (ПД)

противоположной, и значение суммы присваивают точке (ПД) R. Рекурсивный переход выполняется ((2h+2)/n) - 1 раз.

В случае w=-2 и n≥4 одна точка эллиптической кривой (ПД гиперэллиптической кривой), найденная на первом этапе, может соответствовать нескольким значениям цепочек коэффициентов ($K_{in}+tK_{in+1}+\ldots+t^{n-1}K_{in+n-1}$). Для установления однозначного соответствия между указанными БС и значениями цепочек коэффициентов необходимо либо на втором этапе преобразовать цепочки коэффициентов либо на первом этапе дополнить указанные БС списком соответствующих цепочек коэффициентов.

В остальном процесс проверки ЭЦП аналогичен ГОСТ Р 34.10-2001 (ECDSA, схемам Эль-Гамаля, Шнорра).

Заявленный способ позволяет уменьшить число удвоений точек примерно вдвое и за счет этого повысить скорость формирования и проверки электронной цифровой ЭЦП примерно в 1,5 раза.

Предлагаемый способ может быть применен для формирования и проверки ЭЦП как во вновь проектируемых, так и в существующих системах ЭЦП, использующих эллиптические и гиперэллиптические кривые, в частности в системах ЭЦП, реализованных в соответствии с ГОСТ Р 34.10-2001, ECDSA, стандартом ЭЦП Германии. В одной и той же системе ЭЦП может использоваться указанный выбор случайного числа в виде $k=k_0+k_1t$ при формировании ЭЦП и перевод целого числа k в систему счисления с основанием t при проверке ЭЦП.

Рассмотрим примеры реализации заявленного способа для небольших чисел p, q. Достаточно проиллюстрировать умножение точки эллиптической кривой или ПД гиперэллиптической кривой на заданное целое число.

Пример 1. Используется система счисления с основанием $\sqrt{-2}$, n=2. Исходные данные. Эллиптическая кривая задана уравнением $y^2\equiv x^3+x+98 \pmod{1049}$, точка P=(1, 10). Число точек на эллиптической кривой равно q=1033. На первом этапе находят следующие числа: $t=\sqrt{-2}\equiv 167 \pmod{q}$, A=31, B=6, при этом выполняется условие $31+6\sqrt{-2}\equiv 0 \pmod{q}$. Находят вспомогательные БС, содержащие идентификаторы вида {1, t, 1+t, 1-t) и точки P=(1, 10), tP=(441, 731), (1+t)P=(705, 305), (1-t)P=(597, 412), соответствующие этим идентификаторам: $(1\|(1,10))$, $(t\|(441,731))$, $((1+t)\|(705,305))$, $((1-t)\|(597,412))$.

На втором этапе для формирования (проверки) подписи требуется умножение точки P на число k=527, это число представляют в системе счисления с основанием $\sqrt{-2}$, для чего вычисляют следующие числа: $n_1=\left[\frac{Ak}{q}\right]=16$, $n_2=\left[\frac{Bk}{q}\right]=3$, $k_0=k-An_1-2Bn_2=-5$, $k_1=-Bn_1+An_2=-3$, находят представление $k\equiv -1-t+t^3-t^4 \pmod{q}$,

$k\equiv -(1+t)+(-2)\cdot(0+t)+2^2(-1+0t) \pmod{q}$.

Старшая пара коэффициентов в представлении числа k равна -(1+0·t). Выбирают вспомогательную БС с идентификатором 1 и полагают R=-P=(1, 1039). Выполняют удвоение точки R и вычисляют противоположную точку: -2R=(40, 192) и полагают R=(40, 192). Выбирают следующую пару коэффициентов (0+t), соответствующую идентификатору t. Выбирают из вспомогательных БС точку (0+t)P=(441, 731) и вычисляют точку R=(40, 192)+(441, 731)=(416, 56). Вычисляют точку -2R=(335, 62) и полагают R=(335, 62). Последняя пара коэффициентов равна (-1-t)=-(1+1), ей

соответствует идентификатор (1+t). Выбирают точку $\left(1+1\sqrt{-2}\right)P=(705,305)$ и находят противоположную к ней точку $-\left(1+1\sqrt{-2}\right)P=(705,744)$. Вычисляют точку (335, 62)+(705, 744)=(657, 694). Результат: kP=(657, 694). Потребовалось 2 удвоения точек, тогда как известный способ требует 8 удвоений.

Пример 2. Использование системы счисления с основанием, $\sqrt{2}$, n=2. Исходные данные. Эллиптическая кривая задана уравнением $y^2\equiv x^3+x+98 \pmod{1049}$, точка P=(1, 10). Число точек на эллиптической кривой равно q=1033. На первом этапе находят следующие числа: $t=\sqrt{2}\equiv 404 \pmod{q}$, A=5, B=23, при этом выполняется условие 5+23t≡0 (mod q). Находят точки (1+0t)P=(1, 10), (0+t)P=(945, 771), (1+t)P=(60,8), (1-t)P=(0,457) и составляют БС вида: $\left(1\|(1,10)\right)$, $\left(t\|(945,771)\right)$, $\left((1+t)\|(60,8)\right)$, $\left((1-t)\|(0,457)\right)$.

На втором этапе для формирования (проверки) подписи требуется умножение точки P на число k=527, это число представляют в системе счисления с основанием $\sqrt{2}$, для чего вычисляют следующие числа: $n_1=\left[\frac{Ak}{-q}\right]=-3$, $n_2=\left[\frac{Bk}{-q}\right]=-12$, $k_0=k-An_1+2Bn_2=-10$, $k_1=-Bn_1+An_2=9$, находят представление $k_0=-t^2-t^6$, $k_1=1+t^6$, $k\equiv t-t^2-t^6+t^7 \pmod{q}$, $k\equiv(0+t)+2(-1+0t)+4(0+0t)+8(-1+t) \pmod{q}$.

Старшая пара коэффициентов числа k соответствует идентификатору (1-t). Полагают R=-(1-t)P=(0, 592). Выполняют удвоение точки R: 2R=(190, 611) и полагают R=(190, 611). Вторая пара коэффициентов нулевая.

Для перехода к третьей паре коэффициентов (-1+0t)=-(1+0t) выполняют удвоение точки R: 2R=(427, 945), полагают R=(427, 945), по идентификатору находят точку -P=(1, 1039), вычисляют сумму R+(-P)=(177, 497) и полагают R=(177, 497). Для перехода к последней паре коэффициентов (0+t) выполняют удвоение точки R: 2R=(783, 537), полагают R=(783, 537), выбирают по идентификатору t точку tP=(945, 771) и находят сумму R+tP=(657, 694). Результат: kP=(657, 694). Потребовалось 3 удвоения точек, тогда как известный способ требует 8 удвоений.

Пример 3. Гиперэллиптическая кривая задана уравнением $y^2=x^5+2x^2+x+3 \pmod{31}$, приведенный дивизор $P=(2+5x+x^2, 5+x)$ имеет простой порядок q=1009. Используется система счисления с основанием $\sqrt{-2}$, n=2. На первом этапе находят следующие числа: $t=\sqrt{-2}\equiv 55 \pmod{q}$, A=19, B=18, при этом выполняется условие 19+18t≡0 (mod q). Вычисляют следующие ПД: $tP=(20+4x+x^2, 11+18x)$, $(1+t)P=(18+22x+x^2, 28x)$, $(1-t)P=(18+16x+x^2, 14+26x)$ и составляют соответствующие БС, у которых левые части равенств являются идентификаторами: $\left(1\|\left(2+5x+x^2,5+x\right)\right)$, $\left(t\|\left(20+4x+x^2,11+18x\right)\right)$, $\left(1+t\|\left(18+22x+x^2,28x\right)\right)$, $\left(1-t\|\left(18+16x+x^2,14+26x\right)\right)$.

На втором этапе для формирования (проверки) подписи требуется умножение P на число k=527, это число представляют в системе счисления с основанием t, для чего вычисляют следующие числа:

$$n_1=\left[\frac{Ak}{q}\right]=10,\quad n_2=\left[\frac{Bk}{q}\right]=9,$$

$k_0=k-An_1-2Bn_2=13$, $k_1=-Bn_1+An_2=-9$, находят представление $k\equiv 1-t+t^4-t^6+t^7 \pmod{q}$,

$k \equiv (1-t)+2(0-0t)+4(1-0t)+8(1-t) \pmod q$.

Старшая пара коэффициентов равна (1-t), ей соответствует ПД вида $(1-t)P=(18+16x+x^2, 14+26x)$. Это значение присваивают приведенному дивизору R. Выполняют переход ко второй паре коэффициентов (1-0t), соответствующей ПД P, используя одно удвоение: $2R=(9+4x+x^2, 12+25x)$ и присваивают это значение ПД R. Находят сумму ПД: $R+P=(8+21x+x^2, 15+5x)$ и присваивают это значение ПД R. Третья пара коэффициентов нулевая, поэтому выполняют два удвоения $R:=2R=(27+24x+x^2, 21+20x)$, $R:=2R=(17+2x+x^2, 19+x)$. Последняя пара коэффициентов соответствует ПД (1-t)P. Находят сумму $R+(1-t)P=(2+18x+x^2, 25+3x)$. Результат: $kP=(2+18x+x^2, 25+3x)$. Потребовалось 3 удвоения ПД, тогда как известный способ требует 8 удвоений.

Пример 4. Гиперэллиптическая кривая задана уравнением $y^2=x^5+2x^2+x+3 \pmod{31}$, приведенный дивизор $P=(2+5x+x^2, 5+x)$ имеет простой порядок q=1009. Используется система счисления с основанием $\sqrt{2}$, n=2. На первом этапе находят следующие числа: $t=\sqrt{2} \equiv 570 \pmod q$, A=7, B=23, при этом выполняется условие $A^2-2B^2=-q$, $7+23t \equiv 0 \pmod q$. Вычисляют вспомогательные БС, содержащие следующие ПД: $tP=(28+28x+x^2, 5+9x)$, $(1+t)P=(7+28x+x^2, 8+28x)$, $(1-t)P=(29+7x+x^2, 6+8x)$. Левые части равенств являются идентификаторами соответствующих БС: $(1\|(2+5x+x^2,5+x))$, $(t\|(28+28x+x^2,5+9x))$, $(1+t\|(7+28x+x^2,8+28x))$, $(1-t\|(29+7x+x^2,6+8x))$.

На втором этапе для формирования (проверки) подписи требуется умножение P на число k=135, это число представляют в системе счисления с основанием t, для чего вычисляют числа

$$n_1=\left[\frac{Ak}{-q}\right]=-1,\ n_2=\left[\frac{Bk}{-q}\right]=-3,$$

$k_0=k-An_1+2Bn_2=4$, $k_1=-Bn_1+An_2=2$, находят представление $k \equiv t^3+t^4 \pmod q$, $k \equiv (0+0t)+2(0+t)+4(1+0t) \pmod q$.

Старшая пара коэффициентов равна (1+0t), ей соответствует ПД: $R=P=(2+5x+x^2, 5+x)$. Выполняют переход ко второй паре коэффициентов (0+t), соответствующей ПД tP, используя удвоение: $2R=(16+14x+x^2, 2+8x)$ и присваивают это значение ПД R. Находят сумму ПД: $R+tP=(26+5x+x^2, 2+22x)$ и присваивают это значение R. Для перехода к последней паре коэффициентов (0+0t) умножают R на 2 и получают ПД вида $(27+8x+x^2, 26+5x)$.Результат: $kP=(27+8x+x^2, 26+5x)$. Потребовалось 2 удвоения ПД, тогда как известный способ требует 6 удвоений.

Приложение 1

Объяснение специальных терминов и описание заимствованных вычислительных алгоритмов:

Двоичный цифровой электромагнитный сигнал - последовательность битов в виде нулей и единиц.

Параметры двоичного цифрового электромагнитного сигнала: разрядность и порядок следования единичных и нулевых битов.

Разрядность двоичного цифрового электромагнитного сигнала - общее число его единичных и нулевых битов, например сигнал 10011 имеет разрядность 5. Разрядность числа называется также его длиной.

Битовая строка (БС) - двоичный цифровой электромагнитный сигнал конечной разрядности, представляемый в виде конечной последовательности цифр 0 и 1. БС

может интерпретироваться как набор независимых нулей и единиц и как целое число. С битовыми строками могут выполняться логические и арифметические операции. Конкатенация БС $S=(S_1, \ldots, S_n)$ и $T=(T_1, \ldots, T_m)$ представляет собой БС вида $S\|T = (S_1, \ldots, S_n, T_1, \ldots, T_m)$.

Электронная цифровая подпись (ЭЦП) - двоичный цифровой электромагнитный сигнал, параметры которого зависят от подписанного электронного документа и от секретного ключа. Проверка подлинности ЭЦП осуществляют с помощью открытого ключа, который зависит от секретного ключа.

Запись $a \equiv b \pmod p$, где a, b, p - целые числа, означает, что a - b делится на p (сравнимость по модулю простого числа). Запись $u \equiv v \pmod f$, где u, v, f - многочлены, означает, что u - v делится на f (сравнимость по модулю многочлена).

Поле из простого числа p элементов - множество {0, 1, …, p-1}. Сложение и умножение выполняются по модулю p и обозначается $a+b \pmod p$, $ab \pmod p$ (см. [Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. - М.: Гелиос-АРВ, 2003]), например, $3+4 \equiv 0 \pmod 7$, $3 \cdot 4 \equiv 5 \pmod 7$. Поле из p^n элементов представляет собой многочлены вида $a_0+a_1W+\ldots a_{n-1}W^{n-1}$, где f(W)=0, и многочлен f не раскладывается на множители по модулю p, сложение и умножение в поле выполняется по модулю p и по модулю f(W).

Абелева группа - непустое множество, на котором определена бинарная операция, называемая сложением, где для всех элементов группы выполняются равенства R+S=S+R, R+(S+T)=(R+S)+T, в группе существует нулевой элемент 0, такой, что R=0=0+R=R для всех элементов группы R, для каждого элемента группы R существует противоположный элемент -R, такой, что R+(-R)=0. Для каждого элемента R группы существуют кратные: 2R=R+R, 3R=2R+R, …. Конечная абелева группа состоит из конечного числа элементов. Наименьшее натуральное число n такое, что nR=0, называется порядком элемента R.

Эллиптическая кривая над полем из p^n элементов, $n \geq 1$, - подмножество точек P=(x,y) плоскости с координатами из конечного поля, удовлетворяющих уравнению $y^2+a_1xy=x^3+a_2x^2+a_4x+a_6{}^3$, дополненное бесконечно удаленной точкой, где ни в одной точке кривой обе частные производные многочлена, задающего кривую, не равны нулю одновременно. Точки эллиптической кривой образуют конечную абелеву группу [Silverman J. The arithmetic of elliptic curves, Springer, 1986]. Нулевым элементом группы является бесконечно удаленная точка. Сложение точек $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$ задается формулами: $x_3=\lambda^2+\lambda a_1-a_2-x_1-x_2$, $y_3=-(\lambda+a_1)x_3-\nu$,

где $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$, $\nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$ при $(x_1,y_1) \neq (x_2,y_2)$ и

$\lambda = \frac{2x_1{}^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1}$, $\nu = \frac{-x_1{}^3 + a_4x_1 + 2a_6}{2y_1 + a_1x_1}$ при $(x_1,y_1)=(x_2,y_2)$ - случай удвоения точек.

Битовая строка, представляющая точку эллиптической кривой, содержит две координаты этой точки. Бесконечно удаленная точка имеет знаменатель λ.

Гиперэллиптическая кривая над полем из p^n элементов, $n \geq 1$, - подмножество точек плоскости с координатами из конечного поля, в которых многочлен $y^2+h(x)y-f(x)$ обращается в нуль, при этом ни в одной точке кривой обе частные производные многочлена не равны нулю одновременно, степень deg(f) многочлена f(x) равна 2g+

1≥5, где g - натуральное число, deg(h)≤g. Пары многочленов (u(x),v(x)), таких, что u(x) имеет единичный старший коэффициент, $f(x)-hv(x)-v(x)^2$ делится на u(x), deg(v)<deg(u)≤g, образуют конечную абелеву группу и называются приведенными дивизорами (ПД) гиперэллиптической кривой. При этом -(u(x),v(x))=(u(x),-v(x)). Приведенные дивизоры могут быть представлены битовыми строками, содержащими списки коэффициентов многочленов u(x), v(x). Сложение приведенных дивизоров $(u_1,v_1)+(u_2,v_2)=(u_3, v_3)$ выполняется следующим алгоритмом [Scholten J., Vercauteren F. An introduction to elliptic and hyperelliptic curve cryptography and the NTRU cryptosystem, доступно с http://homes. esat. Kuleuven. be/~fvercaut/papers/cc03.pdf].

1. Найти расширенным алгоритмом Евклида представление наибольшего общего делителя $d_1=НОД(u_1,u_2)=e_1u_1+e_2u_2$.

2. Найти расширенным алгоритмом Евклида представление наибольшего общего делителя $d=НОД(d_1,v_1+v_2+h)=c_1d_1+c_2(v_1+v_2+h)$.

3. Вычислить $s_1=c_1e_1$, $s_2=c_1e_2$, $s_3=c_2$.

4. Вычислить $u=(u_1u_2)/d^2$, $v=(s_1u_1v_2+s_2u_2v_1+s_3(v_1v_2+f)/d(\mathrm{mod}\ u)$.

5. Вычислить $u'=(f-vh-v^2)/u$, $v'=(-h-v)(\mathrm{mod}\ u')$.

6. Если deg(u')>g, то u=u', v=v' и возврат на шаг 5.

7. Поделить коэффициенты многочлена u' на старший коэффициент.

8. Выход: (u', v').

Квадратный корень $t \equiv \sqrt{w} \pmod q$, w=±2, можно вычислить следующим образом: [Ростовцев А.Г. Алгебраические основы криптографии. - СПб.: Мир и Семья, Интерлайн, 2000, глава 7]. Если q≡3 (mod 4), то $t \equiv w^{\frac{q+1}{4}} (\mathrm{mod}\ q).$ Если q≡1 (mod 4), то можно воспользоваться следующим алгоритмом.

1. Подбором найти элемент b такой, что $\left(b^2-4w\right)^{\frac{q-1}{2}} \equiv -1 \pmod q$.

2. Положить $f(y)=y^2-by+w$.

3. Вычислить $t=\pm y^{(q+1)/2} (\mathrm{mod}\ q, f(y))$.

Для вычисления представления $q=A^2-wB^2$ можно воспользоваться следующим алгоритмом:

1. Вычислить $t = \sqrt{w} \pmod q$.

2. Положить i=0, $t_i=t$, $m_i=q$.

3. Вычислить $m_{i+1} = \frac{t_i^2 - w}{m_i}$, $t_{i+1}=\min\{t_i(\mathrm{mod}\ m_{i+1}), m_{i+1}-t_i (\mathrm{mod}\ m_{i+1})\}$.

4. Если $m_{i+1}=1$, то перейти на шаг 5, иначе положить i=i+1 и вернуться на шаг 3.

5. Положить $A_i=t_i$, $B_i=1$.

6. Если i=0, то положить $A=A_i$, $B=B_i$ и перейти на шаг 8. Иначе положить $A_{i-1} = \frac{\pm t_{i-1}A_i - wB_i}{A_i^2 - wB_i^2}$, $B_{i-1} = \frac{-A_1 \pm t_{i-1}B_1}{A_1^2 - wB_i^2}$. Знаки подбираются так, чтобы деление было целочисленным.

7. Положить i=i-1 и вернуться на шаг 6.

8. Результат: A, B.

Для q≡1, 3 (mod 8) представление $q=A^2+2B^2$ единственно, а для q≡1, 7 (mod 8) существует бесконечно много представлений $\pm q=A^2-2B^2$, поэтому существуют числам, B, имеющие минимальную длину.

Формула изобретения

1. Способ формирования и проверки электронной цифровой подписи на основе эллиптической или гиперэллиптической кривой, заключающийся в преобразовании битовых строк и выполнении операций с битовыми строками, в котором при формировании или при проверке подписи умножают по крайней мере одну заранее определенную точку (соответственно приведенный дивизор) P простого порядка q эллиптической (соответственно гиперэллиптической) кривой на целое число k путем сложений и удвоений, при формировании подписи допускается случайный выбор числа k, причем для указанного умножения используют два этапа: на первом этапе выбирают четную длину n цепочки и подготавливают вспомогательные битовые строки, содержащие произведение точки эллиптической кривой (соответственно приведенного дивизора гиперэллиптической кривой) на целые числа, представленные всеми допустимыми значениями цепочек, получаемые умножением P на целые числа, соответствующие всем допустимым значениям цепочек, причем каждая указанная битовая строка содержит хотя бы один идентификатор, на втором этапе выполняют указанное умножение с использованием указанных вспомогательных битовых строк, при этом вектор коэффициентов числа k разбивают на цепочки длины n, выбирают вспомогательную битовую строку, один из идентификаторов которой соответствует старшей цепочке, и значение точки (соответственно приведенного дивизора) этой битовой строки присваивают точке (соответственно приведенному дивизору) R, и выполняют рекурсивный переход к предыдущей цепочке, присваивая R значение удвоений R и суммы R с точкой эллиптической кривой (соответственно с приведенным дивизором гиперэллиптической кривой) битовой строки, один из идентификаторов которой соответствует предыдущей цепочке, отличающийся тем, что на первом этапе выбирают число w=-2 при q=1, 3 (mod 8) или w=2 при q=1, 7 (mod 8), вычисляют значение $t=\sqrt{w} \pmod q$, а на втором этапе число k преобразовывают в систему счисления с основанием t: $k=K_0+K_1t+\ldots+K_{2h}t^{2h}+K_{2h+1}t^{2h+1}$, где все коэффициенты K_0, …, K^{2h+1} принимают значения 0, 1 или -1, а число 2h близко к $\log_2 q$, а в ходе рекурсивного перехода к предыдущей цепочке коэффициентов выполняют n/2 удвоений точки (приведенного дивизора) R.

2. Способ по п.1, отличающийся тем, что при формировании подписи случайное число k выбирают в виде пары целых случайных чисел (k_0, k_1) так, что выполняется условие $\left|k_0^2 - wk_1^2\right| < q$, и полагают $k=k_0+tk_1$.

3. Способ по п.1, отличающийся тем, что если w=-2 и n больше или равно 4, то в каждую вспомогательную битовую строку включают все эквивалентные идентификаторы, обладающие одинаковым значением по модулю q, либо каждая вспомогательная битовая строка содержит идентификатор, значение которого равно абсолютно наименьшему из эквивалентных идентификаторов, а на втором этапе выполняют преобразование цепочек коэффициентов числа k, при котором цепочки вида (…, 1, z, 1, …) заменяют на цепочки вида (…, -1, z, 0, …), а цепочки вида (…, -1, z, -1, …), заменяют на цепочки вида (…, 1, z, 0, …), причем z означает любую из цифр 0, 1 или -1.

4. Способ по п.1, отличающийся тем, что в том, что на первом этапе дополнительно подготавливают битовые строки, представляющие целые числа A и B, такие, что выполняются условия: $eq=A^2-wB^2$, где e=1 или e=-1, и целое число A+Bt делится на q, а на втором этапе вычисляют ближайшее к дроби (Ak/(eq)) целое число n_1 и ближайшее к

дроби (Bk/(eq)) целое число n_2, вычисляют числа $k_0=k-An_1+wBn_2$, $k1=-Bn_1+An_2$, преобразовывают их в двоичный вид $k_0=k_{00}+2k_{01}+\ldots+2^h k_{0h}$, $k_1=k_{10}+2k_{11}+\ldots+2^h*k_{1h}$ и для i=0, …, 2h+1 присваивают значения $K_{2i}=k_{0i}$ или $K_{2i}=-k_{0i}$, $K_{2i+1}=k_{1i}$ или $K_{2i+i}=-k_{1i}$, где знаки определяют с учетом знака w.