РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ИЗОБРЕТЕНИЕ

№ 2457625

СПОСОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКОЙ 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 № **2010149164**

Приоритет изобретения **30 ноября 2010 г.**

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

Срок действия патента истекает **30 ноября 2030 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 457 625** (13) **C1**

(51) МПК
H04L 9/32 (2006.01)
G06F 17/10 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010149164/08, 30.11.2010**

(24) Дата начала отсчета срока действия патента:
30.11.2010

Приоритет(ы):
(22) Дата подачи заявки: **30.11.2010**

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

(56) Список документов, цитированных в отчете о поиске: **US 2008/0205638 A1, 28.08.2008. US 7308096 B2, 11.12.2007. WO 02/093411 A1, 21.11.2002. RU 2401513 C2, 10.10.2010. RU 2232476 C2, 10.07.2004.**

Адрес для переписки:
195251, Санкт-Петербург, ул. Политехническая, 29, ФГБОУ ВПО "Санкт-Петербургский государственный политехнический университет" (ФГБОУ ВПО "СПбГПУ"), 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)

(54) СПОСОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в повышении скорости формирования и проверки ЭЦП и повышении защищенности системы ЭЦП от атак по внешнему каналу. Способ электронной цифровой подписи на основе эллиптической кривой в форме Вейерштрасса, в котором генерируют параметры системы электронной цифровой подписи, а также формируют и проверяют подпись, причем при формировании и проверке подписи находят результирующую точку путем удвоений и сложений точек эллиптической кривой, заданных проективными координатами (X,Y,Z), находят битовую строку, представляющую значение $XZ^{-1}(modp)$ координат результирующей точки, причем выполняют линейное преобразование координат (X,Y,Z) точки эллиптической кривой в форме Вейерштрасса в координаты (U,V,W) точки эллиптической кривой в форме Гессе, операции сложения и удвоения точек выполняют на эллиптической кривой в форме Гессе, после чего выполняют линейное преобразование координат (U,V,W) результирующей точки эллиптической кривой в форме Гессе в координаты (X,Z) точки эллиптической кривой в форме Вейерштрасса. 5 з.п. ф-лы, 1 табл., приложение.

RU 2457625 C1

RU 2457625 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 457 625** (13) **C1**

(51) Int. Cl.
H04L 9/32 (2006.01)
G06F 17/10 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010149164/08, 30.11.2010**

(24) Effective date for property rights:
30.11.2010

Priority:
(22) Date of filing: **30.11.2010**

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

Mail address:
195251, Sankt-Peterburg, ul. Politekhnicheskaja, 29, FGBOU VPO "Sankt-Peterburgskij gosudarstvennyj politekhnicheskij universitet" (FGBOU VPO "SPbGPU"), 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) ELLIPTIC CURVE-BASED ELECTRONIC DIGITAL SIGNATURE METHOD

(57) Abstract:

FIELD: information technology.

SUBSTANCE: method for electronic digital signature based on an elliptic curve in Weierstrass form, in which electronic digital signature system parameters are generated and a signature is formed and verified, wherein when forming and verifying the signature, the resultant point is found via doubling and summation of points of the elliptic curve given by projective coordinates (X, Y, Z), a bit string is found, representing the value XZ-1(modp) of the coordinates of the resultant point, wherein linear transformation of coordinates (X, Y, Z) of the point of the elliptic curve in Weierstrass form to coordinates (U, V, W) of a point of an elliptic curve in Hesse form is performed, operations for doubling and summation of the points are carried out on the elliptic curve in Hesse form, after which linear transformation of coordinates (U, V, W) of the resultant point of the elliptic curve in Hesse form to coordinates (X, Z) the point of the elliptic curve in Weierstrass form is carried out.

EFFECT: high rate of forming and verifying an electronic digital signature and high security of the electronic digital signature system from attack through an external channel.

6 cl, 1 tbl, 1 app, 1 dwg

RU 2457625 C1

RU 2457625 C1

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

Известны системы электронной цифровой подписи (ЭЦП) на эллиптических кривых, в которых обрабатываемые данные представлены точками эллиптической кривой в форме Вейерштрасса (ЭКВ), заданной уравнением $y^2 \equiv x^3 + ax + b \pmod p$ для большого простого числа p [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, доступно с http://www.comms.scitech.susx.ac.uk/fft/crypto/ecdsa.pdf], также см. 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.

Процессы формирования и проверки подписи предусматривают выполнение операций сложения точек, представленных БС, и нахождение БС, представляющей значение x-координаты результирующей точки, и реализуются в вычислительном устройстве, например в процессоре персонального компьютера. В качестве не зависящей от типа вычислительного устройства меры длительности криптографической обработки данных удобно использовать число операций модульного умножения. Для ускорения операций удвоения и сложения точек координаты точек представляются в проективной форме. В этом случае удвоение точки ЭКВ требует выполнения 13 операций модульного умножения, а сложение двух различных точек ЭКВ требует выполнения 15 операций модульного умножения. Если одна из складываемых точек имеет единичную третью координату, то для сложения точек требуется 12 операций модульного умножения [Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. - «Профессионал», СПб., 2005, с.171, 172].

Стандарты подписи [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, доступно с http://www.comms.scitech.susx.ac.uk/fft/crypto/ecdsa.pdf] аналогичны и по сути различаются размером задачи: длина цикла $\{P, 2P, 3P, \ldots\}$, образованного точкой P, является простым числом q, длина которого в первом случае не менее 254 бит, а во втором случае не менее 160 бит. Поэтому достаточно рассмотреть только операции с точками

эллиптической кривой, предусмотренные в ГОСТ Р 34.10-2001.

Известные системы ЭЦП предусматривают этап генерации параметров системы ЭЦП и открытого ключа (далее для краткости этап генерации параметров системы ЭЦП). Параметрами системы ЭЦП являются: простое число p длиной не менее 256 бит, коэффициенты *a*, b ЭКВ, число точек ЭКВ, простое число $q>2^{254}$, являющееся делителем числа точек, и точка P порядка q. При этом число q является делителем числа точек ЭКВ. Конфиденциальным ключом создания подписи является натуральное число d, $1\leq d\leq q-1$. Открытым ключом проверки ЭЦП является точка Q=dP.

Параметры системы ЭЦП, открытый и конфиденциальный ключ представлены БС.

Для формирования подписи вырабатывается случайное число k, $0<k<q$, и вычисляется точка kP путем сложений и удвоений точки P. Значение r как x-координата точки kP по модулю q является частью ЭЦП.

Для проверки подписи вычисляется точка z_1P+z_2Q по известным z_1, z_2, и ее x-координата по модулю q сравнивается с r. При совпадении x-координаты точки z_1P+z_2Q (mod q) и r делают вывод о подлинности ЭЦП.

Однократное вскрытие числа k ведет к вычислению конфиденциального ключа [Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. - «Профессионал», СПб., 2005]. На практике умножение точки P на число k выполняют методом удвоений и сложений. Поскольку операции сложения и удвоения выполняются по разным формулам, они могут быть распознаны в реальном масштабе времени путем анализа мгновенной потребляемой мощности. Такая скрытая атака возможна, если подпись формируется в смарт-карте, которая получает электропитание от внешнего терминала.

Аналогом заявленного способа является патент РФ 2232476, МПК H04L 9/30, опубл. 7.10.04, позволяющий сократить суммарную длину коэффициентов ЭКВ за счет преобразования уравнения ЭКВ и координат точки. Недостатком этого способа является то, что он практически не увеличивает скорость обработки данных.

Известны способ и устройство, реализующее ЭЦП на основе эллиптической кривой в форме Гессе (ЭКГ), заданной уравнением

$U^3+V^3+W^3\equiv 3mUVW(\text{mod } p)$, $m^3\neq 1(\text{mod } p)$

[патент FR 2624653, МПК G06F 17/10, опубл. 15.11.02], см. также статью [Joye M., Quisquater J.-J. Hessian elliptic curves and side channel attacks // Cryptographic hardware and embedded systems (CHES 2001), Lecture Notes in Computer Science, v.2162, 2001, pp.402-410, доступно с http://www.gemplus.com/smart/rd/publications/pdf/JQ01hess.pdf]. Данное устройство реализует более быстрый способ, чем в указанном аналоге (удвоение точки ЭКГ требует 9 операций модульного умножения, а сложение точек ЭКГ требует 12 операций модульного умножения и 10 операций модульного умножения, если одна из складываемых точек имеет единичную координату, см. также Приложение 1). Недостатком этого технического решения является невозможность применения его при реализации стандартов электронной цифровой подписи ГОСТ Р 34.10-2001 и FIPS 186-3 (ECDSA), предусматривающих использование ЭКВ.

Известен способ, позволяющий преобразовывать данные, представленные точкой ЭКВ, в данные, представленные точкой ЭКГ, и обратно [Joye M., Quisquater J.-J. Hessian elliptic curves and side channel attacks // Cryptographic hardware and embedded systems (CHES 2001), Lecture Notes in Computer Science, v.2162, 2001, pp.402-410, доступно с http://www.gemplus.com/smart/rd/publications/pdf/JQ01hess.pdf], см. также Приложение 1. Недостатком данного способа является то, что преобразование точки ЭКВ в точку ЭКГ занимает сравнительно много времени, поскольку задается нелинейными

выражениями. Кроме того, это преобразование определено не для всех точек, так как знаменатель этого преобразования иногда может обращаться в 0 (см. Приложение 1).

За прототип выбран способ криптографической обработки данных, представленных в виде битовой строки БС, заключающийся в удвоении и сложении точки ЭКВ, в котором точка задана тремя проективными координатами (X,Y,Z), хотя бы одна из координат ненулевая, причем (X,Y,Z)=(cX,cY,cZ) для любого ненулевого параметра c, а обработка данных ведется с использованием проективных координат (US 20080205638, H04L 9/30, опубл. 28.08.08). Недостатком прототипа является низкая скорость обработки данных, обусловленная тем, что сложение и удвоение точек выполняют на ЭКВ. Кроме того, если процесс формирования ЭЦП в соответствии с прототипом выполняется смарт-картой, которая получает электропитание от внешнего терминала, то конфиденциальный ключ может быть вскрыт атакой по внешнему каналу (см. Приложение 1).

В основу предлагаемого изобретения положена задача создания способа формирования и проверки цифровой подписи на эллиптической кривой, с помощью которого достигается увеличение скорости формирования и проверки ЭЦП на основе ЭКВ, а также обеспечивается возможность защиты от атак по внешнему каналу.

Решение задачи обеспечивается тем, что выполняют линейное преобразование координат (X,Y,Z) точки ЭКВ в координаты (U,V,W) точки ЭКГ с параметром m (см. формулы (II)), предусмотренные ГОСТ Р 34.10-2001, и ECDSA, операции сложения и удвоения точек выполняют на ЭКГ, после чего выполняют обратное линейное преобразование трех проективных координат точки (U,V,W) ЭКГ в две проективных координаты (X,Z) точки ЭКВ (см. формулы (II).

Для вычисления указанного линейного преобразования проективных координат точки ЭКВ в проективные координаты точку ЭКГ и обратного линейного преобразования находят БС, представляющие параметры u, m такие, что выполняются условия

$u^4 a \equiv -3^{-1} m(8+m^3) \pmod p$, $u^6 b \equiv 27^{-1} 2(-8-20m^3+m^6) \pmod p$.

При генерации параметров системы ЭЦП выбирают $p \equiv 5 \pmod 6$, а число точек эллиптической кривой выбирают кратным 3, либо выбирают $p \equiv 1 \pmod 6$, а число точек эллиптической кривой выбирают кратным 9.

Увеличение скорости криптографической обработки данных связано с тем, что сложение и умножение точек ЭКГ выполняется быстрее, чем на ЭКВ, а предложенное линейное преобразование точки ЭКВ в точку ЭКГ и обратно практически не снижает скорость обработки данных.

Существенные признаки заявленного способа:

1. Способ электронной цифровой подписи на ЭКВ, заданной уравнением $Y^2Z=X^3+aXZ^2+bZ^3 \pmod p$, в котором генерируют параметры (p,*a*,b,P,Q) системы ЭЦП, где P - точка большого простого порядка q и Q=dP для конфиденциального ключа d, а также формируют и проверяют ЭЦП, причем при формировании и проверке ЭЦП находят результирующую точку путем удвоений и сложений точек эллиптической кривой, заданных проективными координатами (X,Y,Z). По проективным координатам (X,Y,Z) результирующей точки находят БС, представляющую значение $XZ^{-1} \pmod p$ координат результирующей точки.

2. Выполняют линейное преобразование координат (X,Y,Z) точки ЭКВ в координаты (U,V,W) точки ЭКГ, заданной уравнением $U^3+V^3+W^3=3mUVW \pmod p$, операции удвоения и сложения точек выполняют на ЭКГ.

3. Выполняют операции сложения и удвоения точек на ЭКГ.

4. Выполняют линейное преобразование координат (U,V,W) результирующей точки ЭКГ в координаты (X,Z) точки ЭКВ.

5. Находят два параметра (u,m) линейного преобразования, для которых выполняются условия

$$u^4a \equiv -\frac{m\left(8+m^3\right)}{3}(\mathrm{mod}\,p),\ u^6b \equiv \frac{2\left(-8-20m^3+m^6\right)}{27}(\mathrm{mod}\,p).$$

6. Линейное преобразование координат (X,Y,Z) в координаты (U,V,W) выполняют по формулам

$U\equiv u^2mX+u^3Y+3^{-1}(4-m^3)Z(\mathrm{mod}\ p)$,

$V\equiv u^2mX-u^3Y+3^{-1}(4-m^3)Z(\mathrm{mod}\ p)$,

$W\equiv -2(u^2X+m^2Z)(\mathrm{mod}\ p)$.

7. Линейное преобразование координат (U,V,W) в координаты (X,Z) выполняют по формулам

$X\equiv m^2(U+V)+3^{-1}(4-m^3)W(\mathrm{mod}\ p)$,

$Z\equiv -u^2(U+V+mW)(\mathrm{mod}\ p)$.

8. При генерации параметров системы ЭЦП выбирают $p\equiv 5\ (\mathrm{mod}\ 6)$, а число точек ЭКВ выбирают кратным 3.

9. При генерации параметров системы ЭЦП выбирают $p\equiv 1\ (\mathrm{mod}\ 6)$, а число точек ЭКВ выбирают кратным 9.

10. При генерации параметров системы подписи для каждой из точек P, Q находят координаты (U,V,W), затем заменяют ее координаты на $(1, VU^{-1}(\mathrm{mod}\ p), WU^{-1}(\mathrm{mod}\ p))$ при $U\neq 0$, или на $(UV^{-1}(\mathrm{mod}\ p), 1, WV^{-1}(\mathrm{mod}\ p))$ при $V\neq 0$, или на $(UW^{-1}(\mathrm{mod}\ p), VW^{-1}(\mathrm{mod}\ p), 1)$ при $W\neq 0$.

Признаки по п.1 - общие с прототипом. Признаки 2, 3, 4, 5 являются отличительными признаками, общими для всех вариантов исполнения заявленного способа. Признаки 6, 7, 8, 9, 10 могут варьироваться для вариантов исполнения. Так, линейное преобразование ЭКВ в ЭКГ и обратно по пп.6, 7 дает одинаковый результат при умножении всех элементов матрицы, задающей преобразование, на произвольный ненулевой элемент поля. При генерации параметров системы ЭЦП может использоваться любой из признаков 8 или 9. Признак по п.10 не является обязательным.

Указанная совокупность отличительных признаков позволяет решить задачу - повышение скорости формирования и проверки ЭЦП и повышение защищенности системы ЭЦП от атак по внешнему каналу.

Основой заявленного способа является обратимое линейное преобразование точки ЭКВ в точку ЭКГ. На этапе генерации по известным параметрам *a*, b ЭКВ и простому числу p, которые являются параметрами криптосистемы по ГОСТ Р 34.10-2001, ECDSA, с учетом эквивалентности ЭКВ находят параметры линейного преобразования (u, m) решением двух уравнений

$$u^4a \equiv -\frac{m\left(8+m^3\right)}{3}(\mathrm{mod}\,p),\ u^6b \equiv \frac{2\left(-8-20m^3+m^6\right)}{27}(\mathrm{mod}\,p). \qquad (I)$$

Параметры u, m могут быть найдены на персональном компьютере с использованием пакета MATHEMATICA на этапе генерации параметров системы ЭЦП. Линейное преобразование координат точки ЭКВ в координаты точки ЭКГ задается выражениями

$$U \equiv u^2mX + u^3Y + 3^{-1}\left(4-m^3\right)Z(\mathrm{mod}\,p),$$

$$V \equiv u^2 mX - u^3 Y + 3^{-1}\left(4 - m^3\right)Z \pmod{p},$$

$$W \equiv -2\left(u^2 X + m^2 Z\right) \pmod{p}. \qquad (II)$$

Это линейное преобразование можно также определить как умножение матрицы на вектор:

$$\begin{pmatrix} U \\ V \\ W \end{pmatrix} = \begin{pmatrix} u^2 m & u^3 & \dfrac{4 - m^3}{3} \\ u^2 m & -u^3 & \dfrac{4 - m^3}{3} \\ -2u^2 & 0 & -2m^2 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

при этом результат преобразования как точка на проективной плоскости не меняется при умножении всех элементов матрицы на произвольный ненулевой элемент. Определитель этой матрицы равен $\dfrac{16\left(m^3 - 1\right)}{3} \neq 0$, поэтому существует обратная матрица, задающая обратное линейное преобразование.

Обратное линейное преобразование координат (для формирования и проверки ЭЦП достаточно вычислить только координаты X, Z) задается выражениями

$$X \equiv m^2\left(U + V\right) + 3^{-1}\left(4 - m^3\right)W \pmod{p},$$

$$Z \equiv -u^2\left(U + V + mW\right) \pmod{p}. \qquad (III)$$

Это линейное преобразование можно также определить как умножение матрицы на вектор:

$$\begin{pmatrix} X \\ Z \end{pmatrix} = \begin{pmatrix} m^2 & m^2 & \dfrac{4 - m^3}{3} \\ -u^2 & -u^2 & -u^2 m \end{pmatrix} \begin{pmatrix} U \\ V \\ W \end{pmatrix}.$$

Указанные линейные преобразования ЭКВ в ЭКГ и обратно переводят сумму точек ЭКВ в сумму соответствующих точек ЭКГ и наоборот, а также переводят нулевой элемент для сложения точек в нулевой элемент.

При формировании подписи по ГОСТ Р 34.10-2001 ECDSA нужно найти БС, представляющую значение r как x-координату точки kP на ЭКВ, вычисленную по модулю q. Для формирования подписи по заявленному способу выполняют следующие преобразования БС.

1. Точку P=(X,Y,Z) на ЭКВ преобразуют в точку P'=(U,V,W) на ЭКГ. Это может быть сделано при генерации параметров системы ЭЦП. Благодаря равенству (U,V,W)= (cU,cV,cW) для любого $c \neq 0$, хотя бы одна из координат точки P' может равняться 1.

2. Находят три координаты точки kP' на ЭКГ методом сложений и удвоений.

3. Выполняют обратное линейное преобразование и по трем координатам полученной точки kP' на ЭКГ находят две координаты (X,Z) соответствующей точки на ЭКВ, вычисляют $x=XZ^{-1} \pmod{p}$, $r \equiv x \pmod{q}$.

4. Вычисляют оставшиеся параметры цифровой подписи известным способом.

Умножение точки P' на число k выполняется известным способом. Например, число k записывают в двоичном виде $k=k_0+2k_1+\ldots+2^n k_n$, $k_n=1$. Полагают $T_n=P'$. Для i от n-1 до 0 полагают $T_i=2T_{i+1}+k_i P'$. Результат: T_0.

Проверка подписи (r, s) для значения хэш-функции e по ГОСТ Р 34.10-2001 требует проверки условий $0<r, s<q$, нахождения значений $z_1 \equiv se^{-1} \pmod{q}$, $z_2 \equiv -re^{-1} \pmod{q}$,

нахождения точки z_1P+z_2Q, вычисления ее x-координаты и сравнения x (mod q) с r. При совпадении подпись верна.

Проверка подписи (r, s) для значения хэш-функции e по ECDSA требует проверки условий 0<r, s<q, нахождения значений $z_1 \equiv es^{-1} (\mathrm{mod}\ q)$, $z_2 \equiv rs^{-1} (\mathrm{mod}\ q)$, нахождения точки z_1P+z_2Q, вычисления ее x-координаты и сравнения x (mod q) с r. При совпадении подпись верна.

Для проверки подписи по заявленному способу выполняют следующие расчеты на эллиптической кривой.

1. Точки P, Q на ЭКВ преобразуют в точки P', Q' на ЭКГ. Это может быть сделано на этапе генерации параметров системы ЭЦП. Благодаря равенству (U,V,W)= (cU,cV,cW) для любого $c \neq 0$, хотя бы одна из координат каждой из точек P', Q' может равняться 1. Это преобразование координат может быть выполнено при генерации параметров системы ЭЦП.

2. Находят значения z_1, z_2 по соответствующему стандарту подписи.

3. Находят точку $z_1P'+z_2Q'$ на ЭКГ методом сложений и удвоений.

4. Выполняют обратное линейное преобразование и по трем координатам полученной точки на ЭКГ находят две координаты (X,Z) соответствующей точки на ЭКВ, вычисляют значение $x=XZ^{-1} (\mathrm{mod}\ p)$, проверяют условие $r \equiv x (\mathrm{mod}\ q)$. При совпадении подпись верна.

Наиболее трудоемкой операцией при формировании и проверке подписи является операция умножения точки на число, которая выполняется путем сложений и удвоений точек. Удвоение точки на ЭКГ выполняется в $\frac{13}{9} \approx 1{,}44$ раза быстрее чем на ЭКВ, а сложение двух точек, если у одной из них третья координата (Z или W) единичная, выполняется в 1,2 раза быстрее, при этом число удвоений примерно в два раза больше, чем число сложений. Поэтому в среднем умножение точки на число заявленным способом выполняется в 1,35 раза быстрее, чем в прототипе. Поскольку сложение точек ЭКГ описывается симметрическими функциями, можно сделать единичной любую из ненулевых координат одного из слагаемых.

Заявленный способ корректен, если система (I) имеет решение по модулю p. Предлагается два варианта выбора параметров криптосистемы. Первый вариант: выбрать $p \equiv 5 (\mathrm{mod}\ 6)$, а число точек ЭКВ, задаваемое параметрами *a*, b, выбирать кратным 3 так, чтобы при этом выполнялись требования, предписанные стандартами подписи ГОСТ Р 34.10-2001 и ECDSA. Второй вариант: выбрать $p \equiv 1 (\mathrm{mod}\ 6)$, а число точек ЭКВ, задаваемое параметрами *a*, b, выбирать кратным 9 так, чтобы при этом выполнялись требования, предписанные стандартами подписи ГОСТ Р 34.10-2001 и ECDSA. Оба варианта выбора эллиптических кривых допускаются указанными стандартами.

Предложенный способ позволяет повысить защищенность системы ЭЦП от атак по внешнему каналу (см. Приложение 1). Известно, что однократное вскрытие случайного числа k при формировании подписи ведет к вскрытию конфиденциального ключа формирования подписи [Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография, СПб, НПО «Профессионал», 2005, доступно с http: //progbook.net/seti/kriptograf/1568-teoreticheskaya_kriptografiya.html]. На практике вычисление точки kP при формировании подписи выполняется методом удвоений и сложений в соответствии с двоичным кодом k. Анализ мгновенной потребляемой мощности (например, если ЭЦП формируется смарт-картой, которая получает

электропитание от терминала, контролируемого нарушителем) позволяет скрытно получить двоичные цифры числа k и, следовательно, получить конфиденциальный ключ [Zhou Y., Feng D. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing // Cryptology e-print archive, technical report 205-388, http://eprint.iacr.org/2005/388.pdf]. Известно, что использование ЭКГ позволяет заменить удвоение точки сложением двух точек [Joye M., Quisquater J.-J. Hessian elliptic curves and side channel attacks // Cryptographic hardware and embedded systems (CHES 2001), Lecture Notes in Computer Science, v.2162, 2001, pp.402-410], см. также Приложение 1. Это позволяет сделать операции сложения и удвоения точек практически неразличимыми при анализе потребляемой мощности и за счет этого повысить защищенность системы ЭЦП к атакам по внешнему каналу.

Рассмотрим примеры реализации заявленного способа для поля небольшого размера.

Пример 1. Выбор эллиптической кривой и расчет параметров линейного преобразования. Для p=83 (случай p≡5(mod 6)) возможны лишь ЭКВ, для которых число точек N, кратное 3, равно 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96, 99, 102. Для каждой из эллиптических кривых с указанным числом точек существует эквивалентная ЭКГ, связанная с исходной ЭКВ с помощью параметров (m,u), как показано в таблице 1. Каждая пара (m,u) задает линейную эквивалентность между ЭКВ и ЭКГ с указанным числом точек N.

Таблица 1
Параметры линейно эквивалентных эллиптических кривых в форме Вейерштрасса и Гессе

N	66	69	72	75	78	81	84	87	90	93	96	99	102
a	5	1	1	1	1	3	1	1	1	1	1	4	6
b	16	21	6	20	3	3	27	32	1	17	13	2	6
m	30	73	19	7	61	54	40	59	26	23	49	46	24
u	±33	±28	±1	±19	±37	±10	±16	±36	±37	±26	±6	±2	±19

Для p=71 (случай p≡1 (mod 6)) возможны лишь ЭКВ, для которых число точек N, кратное 3, равно 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90. Эквивалентная ЭКГ над полем из p элементов, связанная с исходной ЭКВ уравнениями (I), существует лишь для N=63, 72, 75, 81, 90 (это числа, кратные 9).

Пример 2. Формирование подписи по ГОСТ Р 34.10-2001. Параметры криптосистемы: p=83, число точек N=93, q=N/3=31. Уравнение ЭКВ (см. пример 1):

$Y^2Z=X^3+XZ^2+17Z^3 (\mathrm{mod}\ p)$.

Точка порядка q на ЭКВ: P=(0,10,1). Пусть k=9.

Известный способ умножения точки на число дает на ЭКВ точку 9P=(29,45,1). Получаем r=29.

Предложенный способ. Линейное преобразование точки P на ЭКГ по формулам (II) дает точку P'=(34,19,21)=(53,76,1)=(28,1,71)=(1,3,47), единичные значения координат получены с учетом проективной эквивалентности. Для k=9 находим 9P'=(37,38,10). Обратное линейное преобразование трех координат (U,V,W) точки 9P' в две координаты точки 9P ЭКВ по формулам (III) дает X=36, Z=27, $XZ^{-1}=29 (\mathrm{mod}\ 83)$, то есть r=29, как и в известном способе. На вычисление параметра s подписи заявленный способ не влияет.

Пусть значение хэш-функции для подписываемого сообщения e=10, конфиденциальный ключ проверки подписи d=19. Второй параметр подписи определяется так: s≡(rd+ke)(mod q), s=21. Подпись равна (r,s)=(29,21).

Пример 3. Проверка подписи по ГОСТ Р 34.10-2001. Параметры криптосистемы те

же, что в примере 2. Открытый ключ проверки подписи (точка на ЭКВ) равен Q=dP=(73,70,1). Подпись равна (r,s)=(29,21), e=10. Условия 0<r, s>q выполнены.

Находим $z_1 \equiv se^{-1} (\mathrm{mod}\ q)=30$, $z_2 \equiv -re^{-1} (\mathrm{mod}\ q)=25$.

Проверка подписи известным способом на ЭКВ дает: $z_1P=(0,73,1)$, $z_2Q=(22,35,1)$. Точка z_1P+z_2Q имеет x-координату 29, что совпадает с r (mod q). Подпись верна.

Предложенный способ. Линейное преобразование точек P, Q на ЭКГ по формулам (II) имеет вид P'=(34,19,21)=(53,76,1)=(28,1,71)=(1,3,47),Q=(58,36,12)=(74,3,1)=(80,1,28)=(1,55,46). Находим на ЭКГ $z_1P'=(19,34,21)$, $z_2Q'=(45,34,74)$, $R'=z_1P'+z_2Q'=(73,66,13)$. Обратное линейное преобразование трех координат точки R' ЭКГ в две координаты точки R ЭКВ по формулам (III) дает значения: X=80, Z=60, $XZ^{-1}=29 (\mathrm{mod}\ 83)$, что совпадает с r (mod q). Подпись верна.

Таким образом, предлагаемый способ обеспечивает возможность ускорения формирования и проверки электронной цифровой подписи во вновь разрабатываемых и существующих системах ЭЦП, в том числе построенных на основе ESDSA, ГОСТ Р 34.10-2001, а также повысить защищенность от атак по внешнему каналу.

Приложение 1

Объяснение терминов, используемых в описании и формуле изобретения.

Запись $a \equiv b (\mathrm{mod}\ p)$ означает, что a-b делится на p.

Конечное поле F_p из простого числа p элементов - множество {0, 1, …, p-1}. Сложение и умножение в конечном поле выполняются по модулю p и обозначается $a+b (\mathrm{mod}\ p)$, $ab (\mathrm{mod}\ p)$ (см. [Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. - М.: Гелиос-АРВ, 2003]), например $3+4 \equiv 0 (\mathrm{mod}\ 7)$, $3 \cdot 4 \equiv 5 (\mathrm{mod}\ 7)$. Для любого ненулевого элемента a существует обратный элемент a^{-1} такой, что $aa^{-1}=1$. Элемент a^{-1} может быть найден расширенным алгоритмом Евклида. Если p>3, то выполняется одно из двух условий $p \equiv 1 (\mathrm{mod}\ 6)$ или $p \equiv 5 (\mathrm{mod}\ 6)$.

Проективная плоскость - множество точек, представленных ненулевыми тройками (X,Y,Z), $X,Y,Z \in F_p$, с учетом эквивалентности (X,Y,Z)=(cX,cY,cZ) для любого $c \neq 0$. Множество точек проективной плоскости вида (X,Y,0) определяет бесконечно удаленную прямую. Остальные точки проективной плоскости с учетом эквивалентности однозначно представимы в виде пар (x,y)=(x,y,1), где $x=XZ^{-1}$, $y=YZ^{-1}$.

Поскольку хотя бы одна из координат любой точки проективной плоскости отлична от 0, эта точка эквивалентна точке, у которой соответствующая ненулевая координата равна 1.

Эллиптическая кривая в форме Вейерштрасса (ЭКВ) над полем F_p - подмножество точек проективной плоскости для $p \geq 5$, удовлетворяющих уравнению $Y^2Z \equiv X^3+aXZ^2+bZ^3 (\mathrm{mod}\ p)$, $4a^3+27b^2 \neq 0 (\mathrm{mod}\ p)$. Эта кривая содержит единственную бесконечно удаленную точку (0, 1, 0). Число точек N эллиптической кривой лежит в пределах $p+1-2\sqrt{p} < N < p+1+2\sqrt{p}$. Точки ЭКВ допускают операцию сложения, при этом для любых точек P_1, P_2, P_3 выполняются условия $P_1+P_2=P_2+P_1$, $(P_1+P_2)+P_3=P_1+(P_2+P_3)$. Нулем по сложению является точка (0,1,0), при этом -(X,Y,Z)=(X,-Y,Z). Сложение точек $(X_1,Y_1,Z_1)+(X_2,Y_2,Z_2)=(X_3,Y_3,Z_3)$ задается формулами [Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография, СПб., НПО «Профессионал», 2005, доступно с http://progbook.net/seti/kriptograf/1568-teoreticheskaya_kriptografiya.html].

$$X_3 \equiv 2Y_1Z_1\left(\left(3X_1^2 + aZ_1^2\right)^2 - 8X_1Y_1^2Z_1\right)(\mathrm{mod}\, p),$$

$$Y_3 \equiv 4Y_1^2Z_1\left(3X_1\left(3X_1^2 + aZ_1^2\right) - 2Y_1^2Z_1\right) - \left(3X_1^2 + aZ_1^2\right)^3 \pmod p,$$

$$Z_3 \equiv 8Y_1^3Z_1^3 \pmod p,$$

если $(X_1,Y_1,Z_1)=(X_2,Y_2,Z_2)$ (случай удвоения точек) или

$X_3\equiv(X_2Z_1-X_1Z_2)(Z_1Z_2(Y_2Z_1-Y_1Z_2)^2-(X_2Z_1+X_1Z_2)(X_2Z_1-X_1Z_2)^2)(\mathrm{mod}p)$,

$Y_3\equiv(X_2Z_1-X_1Z_2)^2(Y_2Z_1(X_2Z_1+2X_1Z_2)-Y_1Z_2(X_1Z_2+2X_2Z_1))-Z_1Z_2(Y_2Z_1-Y_1Z_2)^3$ (mod p), $Z_3\equiv Z_1Z_2(X_2Z_1-X_1Z_2)^3$(mod p),

если $(X_1,Y_1,Z_1)\neq(X_2,Y_2,Z_2)$. Наименьшее натуральное число q такое, что $q*(X_1,Y_1,Z_1)=(0,1,0)$ называется порядком точки (X_1,Y_1,Z_1). ЭКВ допускает эквивалентное преобразование координат и коэффициентов (X,Y,Z,*a*,b) в (X',Y',Z',*a*',b'), где $X'=u^2X(\mathrm{mod}\ p)$, $Y'=u^3Y(\mathrm{mod}\ p)$, $Z'=Z(\mathrm{mod}\ p)$, $a'=u^4a(\mathrm{mod}\ p)$, $b'=u^6b(\mathrm{mod}\ p)$ для любого и $u\neq0$.

Эллиптическая кривая в форме Гессе (ЭКГ) над полем F_p - подмножество точек проективной плоскости для $p\geq5$, удовлетворяющих уравнению $U^3+V^3+W^3\equiv3mUVW(\mathrm{mod}\ p)$, где $m^3\neq1$ (mod p). Если $p\equiv5$ (mod 6), то ЭКГ содержит единственную бесконечно удаленную точку (1,-1,0). Точки ЭКГ допускают операцию сложения. Нулевым элементом по сложению является бесконечно удаленная точка (1,-1,0), при этом -(U,V,W)=(V,U,W).

Сложение точек $(U_1,V_1,W_1)+(U_2,V_2,W_2)=(U_3,V_3,W_3)$ задается соотношениями $U_3=V_1(W_1^3-U_1^3)(\mathrm{mod}\ p)$, $V_3=U_1(V_1^3-W_1^3)(\mathrm{mod}\ p)$,

$W_3=W_1(U_1^3-V_1^3)(\mathrm{mod}\ p)$, если $(U_1,V_1,W_1)=(U_2,V_2,W_2)$ (удвоение точки), и

$U_3=U_1W_1V_2^2-U_2W_2V_1^2(\mathrm{mod}\ p)$, $V_3=V_1W_1V_2^2-V_2W_2U_1^2(\mathrm{mod}\ p)$,

$W_3=U_1V_1W_2^2-U_2V_2W_1^2$ (mod p), если $(U_1,V_1,W_1)\neq(U_2,V_2,W_2)$.

ЭКГ всегда содержит точку (0,-1,1) порядка 3. Поэтому число точек ЭКГ всегда делится на 3. Если $p\equiv1$ (mod 6), то ЭКГ содержит 9 точек порядка 3, в этом случае число точек ЭКГ делится на 9. Любая точка ЭКГ имеет хотя бы две ненулевых координаты и эквивалентна точке, у которой одна из ненулевых координат равна 1. Например, точка (U,V,W) при $U\neq0$ эквивалентна точке $(1,VU^{-1},WU^{-1})$, при $V\neq0$ она эквивалентна точке $(UV^{-1},1,WV^{-1})$, при $W\neq0$ она эквивалентна точке $(UW^{-1},VW^{-1},1)$.

Известно [Joye M., Quisquater J.-J. Hessian elliptic curves and side channel attacks // Cryptographic hardware and embedded systems (CHES 2001), Lecture Notes in Computer Science, v.2162, 2001, pp.402-410;

http://www.gemplus.com/smart/rd/publications/pdf/JQ01hess.pdf], что точку (X,Y,Z) ЭКВ можно преобразовать в точку (U,V,W) ЭКГ и обратно с помощью нелинейных выражений

$$\frac{U}{W} = \frac{6\left(m^3-1\right)\left(YZ^{-1} - 9m^2 - 3mXZ^{-1} - 36\right)}{\left(XZ^{-1} + 9m^2\right)^3 + \left(3m^3 - mXZ^{-1} - 12\right)^3}\left(XZ^{-1} + 9m^2\right),$$

$$\frac{V}{W} = -1 + \frac{6\left(m^3-1\right)\left(YZ^{-1} - 9m^2 - 3mXZ^{-1} - 36\right)}{\left(XZ^{-1} + 9m^2\right)^3 + \left(3m^3 - mXZ^{-1} - 12\right)^3}\left(3m^3 - mXZ^{-1} - 12\right),$$

$$\frac{X}{Z} = -9m^2 + \frac{12\left(m^3-1\right)UW^{-1}}{mUW^{-1} + VW^{-1} + 1}, \frac{Y}{Z} = \frac{36\left(m^3-1\right)\left(VW^{-1}-1\right)}{mUW^{-1} + VW^{-1} + 1}.$$

Нарушитель - человек или техническое средство, ставящее целью вскрыть секретный ключ в системе электронной цифровой подписи.

Атака со стороны нарушителя по внешнему каналу (side channel attack) основана на измерении времени, затрачиваемого на формирование подписи, мгновенной потребляемой мощности и других физических величин и позволяет получить информацию о числе k, так как сложение и удвоение точек эллиптической кривой требуют различного времени и различного мгновенного энергопотребления. Однократное нахождение числа k ведет к вскрытию секретного ключа формирования подписи. ЭКГ затрудняет указанную атаку за счет замены операции удвоения точки операцией сложения двух различных точек [Joye M., Quisquater J.-J. Hessian elliptic curves and side channel attacks // Cryptographic hardware and embedded systems (CHES 2001), Lecture Notes in Computer Science, v.2162, 2001, pp.402-410; http: //www.gemplus.com/smart/rd/publications/pdf/JQ01hess.pdf]:

$2(U_1,V_1,W_1)=(W_1,U_1,V_1)+(V_1,W_1,U_1)$.

Формула изобретения

1. Способ электронной цифровой подписи на основе эллиптической кривой в форме Вейерштрасса, заданной уравнением $Y^2Z\equiv X^3+aXZ^2+bZ^3(\mathrm{mod}p)$, где простое число p, коэффициенты a, b и координаты точек (X, Y, Z) заданы битовыми строками, в котором генерируют параметры системы электронной цифровой подписи: a, b, p, число точек эллиптической кривой, имеющее большой простой делитель q, точку P порядка q и точку Q=dP для конфиденциального ключа d, а также формируют и проверяют подпись, причем при формировании и проверке подписи находят результирующую точку путем удвоений и сложений точек эллиптической кривой, заданных проективными координатами (X, Y, Z), находят битовую строку, представляющую значение $XZ^{-1}(\mathrm{mod}p)$ координат результирующей точки, отличающийся тем, что выполняют линейное преобразование координат (X, Y, Z) точки эллиптической кривой в форме Вейерштрасса в координаты (U, V, W) точки эллиптической кривой в форме Гессе, заданной уравнением $U^3+V^3+W^3\equiv 3mUVW(\mathrm{mod}p)$,

операции сложения и удвоения точек выполняют на эллиптической кривой в форме Гессе, после чего выполняют линейное преобразование координат (U, V, W) результирующей точки эллиптической кривой в форме Гессе в координаты (X, Z) точки эллиптической кривой в форме Вейерштрасса, при этом в ходе генерации параметров системы электронной цифровой подписи находят два параметра (u, m) указанного линейного преобразования, для которых выполняются условия

$$u^4a\equiv-\frac{m\left(8+m^3\right)}{3}(\mathrm{mod}p),\ u^6b\equiv\frac{2\left(-8-20m^3+m^6\right)}{27}(\mathrm{mod}p).$$

2. Способ по п.1, отличающийся тем, что линейное преобразование координат (X, Y, Z) точки эллиптической кривой в форме Вейерштрасса в координаты (U, V, W) точки эллиптической кривой в форме Гессе выполняют по формулам

$U\equiv u^2mX+u^3Y+3^{-1}(4-m^3)Z(\mathrm{mod}p)$,

$V\equiv u^2mX-u^3Y+3^{-1}(4-m^3)Z(\mathrm{mod}p)$,

$W\equiv-2(u^2X+m^2Z)(\mathrm{mod}p)$.

3. Способ по п.1, отличающийся тем, что линейное преобразование координат (U, V, W) результирующей точки эллиптической кривой в форме Гессе в координаты (X, Z) точки эллиптической кривой в форме Вейерштрасса выполняют по формулам

$X\equiv m^2(U+V)+3^{-1}(4-m^3)W(\mathrm{mod}p)$,

$Z\equiv-u^2(U+V+mW)(\mathrm{mod}p)$.

4. Способ по п.1, отличающийся тем, что при генерации параметров системы электронной цифровой подписи выбирают $p \equiv 5 \pmod 6$, а число точек эллиптической кривой в форме Вейерштрасса выбирают кратным 3.

5. Способ по п.1, отличающийся тем, что при генерации параметров системы электронной цифровой подписи выбирают $p \equiv 1 \pmod 6$, а число точек эллиптической кривой в форме Вейерштрасса выбирают кратным 9.

6. Способ по п.1, отличающийся тем, что при генерации параметров системы электронной цифровой подписи для каждой из точек P, Q находят координаты (U, V, W), затем заменяют ее координаты на $(1, VU^{-1}(\mathrm{mod}p), WU^{-1}(\mathrm{mod}p))$ при $U \neq 0$, или на $(UV^{-1}(\mathrm{mod}p), 1, WV^{-1}(\mathrm{mod}p))$ при $V \neq 0$, или на $(UW^{-1}(\mathrm{mod}p), VW^{-1}(\mathrm{mod}p), 1)$ при $W \neq 0$.