РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2541938** (13) **C1**

(51) МПК
H04L9/32 (2006.01)
G09C1/00 (2006.01)

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ**

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

Статус: по данным на 27.12.2016 - действует
Пошлина: учтена за 3 год с 21.11.2015 по 20.11.2016

(21), (22) Заявка: **2013151760/08, 20.11.2013**

(24) Дата начала отсчета срока действия патента:
20.11.2013

Приоритет(ы):
(22) Дата подачи заявки: **20.11.2013**

(45) Опубликовано: **20.02.2015**

(56) Список документов, цитированных в отчете о поиске: **RU 2417410 C2, 27.04.2011. RU 2376651 C2, 20.12.2009. US 2010/0082992 A1, 01.04.2010. US 2010/0172491 A1, 08.07.2010. US 7499544 B2, 03.03.2009. US 7209555 B2, 24.04.2007**

Адрес для переписки:
195251, Санкт-Петербург, ул. Политехническая 29, ФГАОУ ВО "СПбПУ", отдел интеллектуальной собственности

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

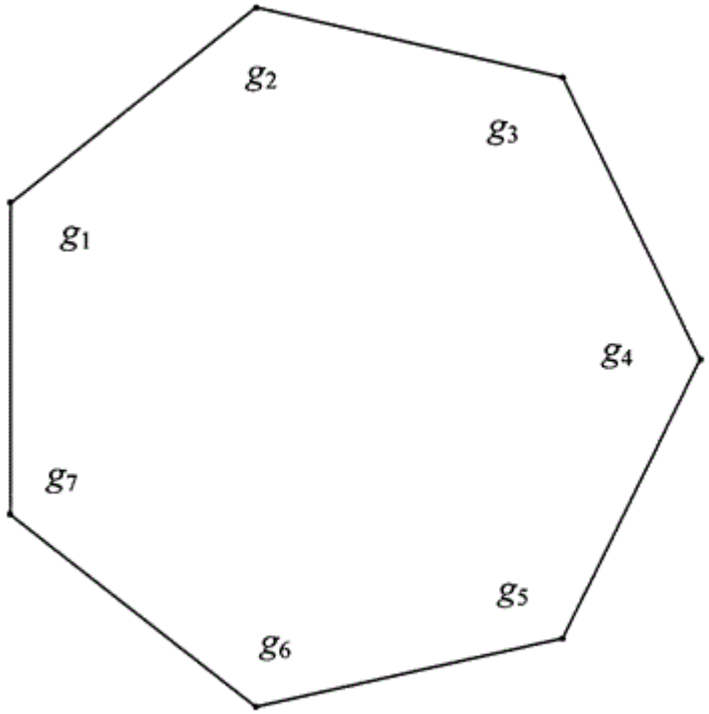
(73) Патентообладатель(и):
федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный политехнический университет" (ФГАОУ ВО "СПбПУ") (RU)

(54) СПОСОБ ШИФРОВАНИЯ С ЗАЩИТОЙ ОТ КВАНТОВЫХ АТАК НА ОСНОВЕ ЦИКЛОВ ФУНКЦИЙ ВЕБЕРА

(57) Реферат:

Изобретение относится к области криптографической защиты электронных данных, передаваемых по телекоммуникационным сетям и сетям ЭВМ. Технический результат - защита от квантовых атак. Способ шифрования с защитой от квантовых атак на основе циклов функций Вебера использует циклы функций Вебера для эллиптических кривых на число, сравнимое с 1 по модулю 8, а циклы определяются изогениями Элкиса малых степеней. Очередное значение функции Вебера находится как корень целочисленного симметрического полинома. Секретным ключом является список целых чисел ($N_1, \ldots, N_k$), где N_i - число шагов, выполняемых по циклу функций Вебера для изогении Элкиса степени l_i, открытым ключом является значение функции Вебера последней изогении. При первом вычислении функции Вебера для изогении степени l задается положительное направление на цикле. Для этого выбирается ядро изогении как делитель степени (l-1)/2 l-го полинома деления, определяющий минимальную степень расширения, в котором лежат точки ядра и по трем старшим коэффициентам полинома, задающего ядро, вычисляются

коэффициенты изогенного образа эллиптической кривой. Шаги по циклу выполняются в соответствии со знаком числа



Фиг. 1

N_i. 2 з.п. ф-лы, 2 ил.

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

Известны системы криптографической защиты - 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.]. Известен также способ криптографической защиты данных, заключающийся в шифровании с открытым ключом на основе эллиптических кривых [Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография, СПб, НПО «Профессионал», 2005, доступно с http://progbook.net/seti/kriptograf/1568-teoreticheskava_kriptografiya.html].

Известен способ шифрования данных с использованием изогений эллиптических кривых [Джао, Венкатесан. Использование изогений для разработки криптосистем, патент RU № 2376651, патент US № 7499544]. Здесь изогении рассматриваются как отображения точек одной эллиптической кривой в точки другой эллиптической кривой.

Безопасность указанных технических решений основана на сложности решения задачи дискретного логарифма на эллиптической кривой: для точек P, Q эллиптической кривой найти целое число l такое, что P=lQ. Известно, что квантовый компьютер достаточно большой разрядности (примерно 3000 кубитов) может эффективно решать такие задачи [http://en.wikipedia.org/wiki/Elliptic_curve_cryptography]. Поэтому известные способы не обеспечивают безопасность по отношению к квантовым атакам.

Другие известные криптосистемы с открытым ключом (RSA, криптосистема на группе классов квадратичного порядка, криптосистемы на гиперэллиптических кривых [A. Menezes, P. Van Oorchot, S. Vanstone. Handbook of applied cryptography, CRC press, 1996]) также уязвимы к квантовым атакам [Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография, СПб, НПО «Профессионал», 2005]. Такие криптосистемы также уязвимы к квантовым атакам, например, для разложения составного числа может использоваться алгоритм Шора [Hughes R.J. Quantum computation. Technical report LA-UR-98-288, 1998].

Канадская фирма D-wave освоила производство квантовых компьютеров разрядности 128 кубитов [www.dwavesys.com/en/priducts-services.html] и работает над увеличением их разрядности. Таким образом, безопасность известных способов криптографической защиты информации находится под угрозой. Возникает необходимость в новых способах криптографической защиты данных, стойких по отношению к квантовым атакам.

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. Криптографическая защита данных 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].

Эллиптическая кривая над конечным полем из p элементов, где p - простое число, состоит из точек, заданных уравнением $y^2=x^3+Ax+B \pmod p$ и точки P_∞. Точки эллиптических кривых допускают операцию сложения с нулевым элементом $P_\infty=(0, 1, 0)$. Полиномы деления $f_l(x)$ обращаются в 0 тогда и только тогда, когда x-координата точки порядка l является корнем этого полинома. Эллиптическая кривая характеризуется своим инвариантом j, дискриминантом Фробениуса Dc^2 для целого c и соответствующим числом классов (см. Приложение 1), а также значением функции Вебера g, удовлетворяющей уравнению $j=\frac{\left(g^{24}-16\right)^3}{g^{24}}$ в случае $D\equiv 1 \pmod 8$.

Изогения эллиптических кривых - отображение $E_1 \rightarrow E_2$, заданное рациональными функциями, сохраняющее неподвижным точку P_∞ и переводящее сумму точек на E_1 в сумму точек на E_2, изогения характеризуется своей степенью (взаимно простой с p). Изогении соответствует отображение функций Вебера $g(E_1) \rightarrow g(E_2)$. Если изогения $E_1 \rightarrow E_2$ существует, то эллиптические кривые E_1, E_2 обладают одинаковыми дискриминантами Фробениуса.

Существуют целочисленные симметрические модулярные полиномы $\Phi_l(U, V)$, обращающиеся в 0, если переменные принимают значение j-инвариантов эллиптических кривых, между которыми существует изогения степени l [патент US № 7623655, H04L 9/14]. Недостатком этих полиномов является большая длина коэффициентов и большое число слагаемых, что затрудняет их использование в системах защиты информации. Изогения простой нечетной степени l является изогений Элкиса, если дискриминант Фробениуса эллиптической кривой является квадратом по модулю l.

За прототип принят способ [патент RU № 2376651, G09C 1/00] «Использование изогений для разработки криптосистем», дублирующий указанный выше патент US № 7499544.

Существенные признаки прототипа.

Способ шифрования сообщений, содержащий: генерацию изогении, отображающей множество точек первой эллиптической кривой на вторую эллиптическую кривую, опубликование открытого ключа, соответствующего изогении, шифрование сообщения с использованием ключа, соответствующего изогении, и расшифрование зашифрованного сообщения при помощи ключа расшифрования, соответствующего изогении, при этом хотя бы один из ключей является секретным и является дуальной изогений к исходной изогении (п.1 формулы).

Способ расшифрования сообщений, содержащий опубликование открытого ключа, соответствующего изогении, отображающей множество точек первой эллиптической кривой на вторую эллиптическую кривую, и расшифрование зашифрованного сообщения при помощи ключа расшифрования, соответствующего изогении, при этом ключ расшифрования является дуальной изогений к упомянутой изогении (п.12 формулы).

Способ по п.1, дополнительно включающий формирование множества модулярных изогений без раскрытия промежуточных кривых, (п.9 формулы). При этом модулярная изогения определяется авторами на основе модулярной кривой $X_0(l)$.

Идентификационное шифрование (IBE) с использованием изогений, в котором открытым ключом является точка $T \in E_2$ второй эллиптической кривой, а секретным ключом - точка $S = \hat{\varphi}(T)$ первой эллиптической кривой для дуальной изогении $\hat{\varphi}$.

Прототип рассматривает изогению как отображение точек первой эллиптической кривой на вторую эллиптическую кривую. Здесь изогения используется для ускорения известных способов криптографической защиты данных - шифрования с открытым ключом на эллиптической кривой и вычисления спаривания Вейля/Тейта. Эти известные способы основаны на задаче вычисления дискретного логарифма на эллиптической кривой и поэтому уязвимы к квантовым атакам, следовательно, и прототип, как их ускоренная версия, не обеспечивает безопасность по отношению к квантовым атакам. Это обстоятельство является недостатком прототипа, который устраняется в заявленном способе.

Технической задачей заявляемого решения является разработка способа шифрования с открытым ключом, обеспечивающего защиту от квантовых атак.

Поставленная задача достигается тем, что обрабатываемые данные представлены функциями Вебера изогенных эллиптических кривых над конечным полем, а обработка данных заключается в отображении функций Вебера путем движения по циклам функций Вебера, при этом дискриминант Фробениуса эллиптической кривой равен произведению квадрата целого числа на число, сравнимое с 1 по модулю 8.

На фиг.1 представлен цикл функций Вебера для изогении степени l_1 на фиг.2 представлен цикл функций Вебера для изогении другой степени l_2.

В заявленном способе рассматривается отображение функций Вебера, которое определяется изогениями малых простых степеней l и целочисленными симметрическими полиномами W_l для функции Вебера, являющихся аналогами классических модулярных полиномов Φ_l для функции j. Объем памяти для хранения полинома W_l примерно в 1000 раз меньше, чем для хранения полинома Φ_l, за счет сокращения числа ненулевых коэффициентов и их длины. Время обработки информации с использованием полинома Φ_l, W_l пропорционально квадрату его длины. Поэтому скорость обработки данных с использованием функций Вебера в миллионы раз больше, чем при использовании классических модулярных полиномов.

Ниже перечислены существенные признаки предлагаемого способа.

1. Способ шифрования с защитой от квантовых атак на основе циклов функций Вебера, в котором сообщение зашифровывают с использованием открытого ключа и зашифрованное сообщение расшифровывают при помощи секретного ключа, содержащий первую эллиптическую кривую и вторую эллиптическую кривую с одинаковыми дискриминантами Фробениуса, соответствующими открытому ключу, и отображение первой эллиптической кривой во вторую эллиптическую кривую, соответствующее секретному ключу, отличающийся тем, что эллиптические кривые задают значениями функции Вебера, причем секретный ключ определяют как цепочку отображений функций Вебера,

соответствующих изогениям Элкиса степеней $l_1, \ldots, l_k$, заданную набором целых чисел $N_1, \ldots, N_k$, где N_i - число шагов по циклу функций Вебера для изогении степени, при этом очередное значение функции Вебера g_{i+1} определяют как корень симметрического полинома двух переменных при замене одной переменной на предыдущее значение функции Вебера g_i, а при переходе к изогении очередной степени задают положительное направление на цикле, для этого находят полином, задающий ядро изогении, а шаги по циклу выполняют в направлении, соответствующем знаку числа N_i.

2. Способ по п.1, отличающийся тем, что дискриминант Фробениуса выбирают равным произведению квадрата целого числа на число, сравнимое с 1 по модулю 8.

3. Способ по п.1, отличающийся тем, что ядро изогении задают полиномом, для которого точки ядра лежат в расширении минимальной степени, и по его коэффициентам находят функцию Вебера, соответствующую положительному направлению.

Принципиальное различие между прототипом и заявленным способом заключается в следующем.

- Прототип уязвим к квантовым атакам, а для заявленного способа эффективные квантовые атаки не найдены.

- В прототипе шифруемые данные представлены координатами точки эллиптической кривой, что затрудняет шифрование произвольного текста, а в заявленном способе - произвольным ненулевым элементом.

- Безопасность прототипа основана на задаче дискретного логарифмирования на эллиптической кривой, для решения которой есть эффективный квантовый алгоритм, а безопасность заявленного способа основана на задаче вычисления изогении между эллиптическими кривыми, которая в настоящее время не может быть решена на квантовом компьютере.

Указанные существенные признаки данного способа позволяют строить криптосистемы с открытым ключом по аналогии с известной криптосистемой Диффи-Хеллмана и Эль-Гамаля (см. [A. Menezes, P. Van Oorchot, S. Vanstone. Handbook of applied cryptography, CRC press, 1996]). На сегодняшний день не созданы эффективные алгоритмы для обычного или квантового компьютера, нарушающие безопасность предлагаемой криптосистемы. Это позволяет говорить о том, что предлагаемый способ обеспечивает стойкость по отношению к квантовым атакам.

Основой заявленного способа является процедура вычисления цепочки из $N \neq 0$ отображений простой нечетной степени l функции Вебера для первоначальной эллиптической кривой $E(F_p)$ (целое число N может быть положительным и отрицательным), которая выполняется следующим образом.

- Для эллиптической кривой $E(F_p)$ вычисляют значение функции Вебера g_0 по модулю p. Присваивают переменной g индекс i=0 и значение g.

- Для выбора положительного направления выполняют следующие действия.

- Определяют наименьшую степень расширения n_l поля F_p, в котором лежит ядро изогении степени l кривой $E(F_p)$ и наименьшую степень расширения m_l, поля, в котором лежит ядро изогении скрученной кривой.

- Находят делители полинома деления $f_l(x)$, степень которых является делителем числа $\frac{l-1}{2}$, и находят ядро изогении.

- По найденному ядру изогении вычисляют функцию Вебера g^r изогенной эллиптической кривой, задающую положительное направление.

- Если N=1, то результат: g^r. Если N=-1, то выбирают тот из двух корней полинома $W_l(U, g)$, который отличен от g^r.

- Если $N=\pm 1$, то находятся корни g_0, g_2 полинома $W_l(U, g_1) \pmod p$ и переменной g присваивается индекс 2 и значение g_2.

- Если $N=\pm 2$, то результат g_2, иначе п.4 рекуррентно повторяется, при этом переменной g присваивается очередной индекс и вычисляется корень g_i полинома $W_l(U, g_{i-1}) \pmod p$, пока не будет получено i=N. Результат: g_N.

Если нужно вычислить цепочку отображений функций Вебера для изогений нескольких степеней $l_1, l_2, \ldots, l_k$, состоящую из N_i изогений l_i, то для каждой изогении выполняются указанные выше вычисления, причем в качестве начального значения g_0 используется значение, найденное на предыдущем этапе.

Поскольку произведение изогений коммутативно и ассоциативно, то очередность их вычислений не влияет на результат. Например, если нужно вычислить цепочку отображений функций Вебера, заданную тремя изогениями

степени l_1 и двумя изогениями степени l_2 , то последовательности (l_1, l_1, l_1, l_2, l_2), (l_2, l_1, l_1, l_2, l_1), (l_1, l_2, l_2, l_1, l_1) и т.п. дадут одинаковый результат.

При использовании изогений степени l_1 функции Вебера образуют цикл, длина которого является делителем числа классов, например для h=7 (см. фиг.1).

Зададим положительное направление $g_1 \rightarrow g_2$ по часовой стрелке, тогда отрицательное направление $g_1 \rightarrow g_7$ соответствует дуальной изогении.

При использовании изогении другой степени l_2 функции Вебера тоже образуют цикл, но вершины соединяются в другом порядке (см. фиг.2).

Зададим положительное направление отображением $g_1 \rightarrow g_4$. Тогда один шаг изогении степени l_2 соответствует трем шагам изогении степени l_1, а один шаг изогении степени l_1 - пяти шагам изогении степени l_2. При совмещении циклов, задаваемых изогениями степенями l_1 и l_2, получаем звезду.

Таким образом, используемые циклы функций Вебера задают звезду. Если число классов очень велико (что имеет место в криптографии), то число вершин звезды оказывается необозримым. При этом длина шага на звезде для изогении одной степени по сравнению с другой степенью является трудновычислимой.

Ключевой обмен при использовании изогении строится по аналогии с системой Диффи-Хеллмана. Два пользователя A, B договариваются об использовании первоначальной эллиптической кривой $E(F_p)$, для которой число классов дискриминанта Фробениуса велико. Кроме того, оба пользователя имеют библиотеку модулярных полиномов $\{W_1, \ldots, W_k\}$ для функции Вебера, состоящую из полиномов W_l для простых нечетных l, по модулю которых дискриминант Фробениуса D является квадратом, библиотеку полиномов деления f_l для тех же l для каждой из k изогении, при этом для изогении каждой степени определена степень полинома, задающего ядро. Если в разложении полинома деления есть несколько полиномов одинаковой степени, то положительное направление задается тем ядром, для которого y-координата лежит в поле минимальной степени расширения.

Для установления сеансового ключа пользователь A выбирает малые целые случайные числа $\{N_l, \ldots, N_k\}$ по числу модулярных полиномов своей библиотеки. В качестве первоначального значения пользователь A использует значение функции Вебера g_0 исходной эллиптической кривой. Он вычисляет цепочку описанным выше способом и посылает результат g_A пользователю B.

Пользователь B выбирает независимо случайные числа $\{M_1, \ldots, M_k\}$, вычисляет цепочку изогений для начального значения g_0 и результат g_B посылает пользователю A.

Пользователь A, используя в качестве начального значения g_B, вычисляет цепочку изогений длин $\{N_1, \ldots, N_k\}$, эквивалентную цепочке $\{M_1+N_1, \ldots, M_k+N_k\}$ для начального значения g_0 и получает результат g_{AB}. Пользователь B, используя в качестве начального значения g_A, вычисляет цепочку изогений длин $\{M_1, \ldots, M_k\}$, эквивалентную цепочке $\{N_1+M_1, \ldots, N_k+M_k\}$ для начального значения g_0 и получает тот же результат g_{AB}. Оба пользователя используют найденное значение g_{AB} в качестве сеансового ключа.

Шифрование с открытым ключом выполняется следующим образом. Открытым ключом являются эллиптическая кривая $E(F_p)$ со значением функции Вебера g_0 , набор изогений $\{l_1, \ldots, l_k\}$, значение функции Вебера $\underline{\underline{g}}_A$, полученное применением к эллиптической кривой цепочки изогений длин $\{N_1, \ldots, N_k\}$. Секретным ключом является набор длин $\{N_1, \ldots, N_k\}$.

Для зашифрования текста m с помощью открытого ключа отправитель генерирует случайную цепочку длин изогений $\{M_1, \ldots, M_k\}$, вычисляет цепочку этих изогений для начального значения g_0, получает значение g_B, вычисляет цепочку этих же изогений для начального значения g_A , получает результат g_{AB}, вычисляет значение $s \equiv m*g_{AB} \pmod p$. Зашифрованным текстом является пара (g_B, s).

Для расшифрования зашифрованного текста владелец секретного ключа вычисляет цепочку изогений степеней $\{N_1, \ldots, N_k\}$ для начального значения g_B и получает g_{AB}. Затем он вычисляет $m \equiv s*g_{AB}^{-1} \pmod p$.

Заявленный способ позволяет выполнять аутентификацию сообщений по схеме без диалоговых доказательств с нулевым разглашением знаний.

Для вычисления коэффициентов изогенного образа эллиптической кривой можно использовать многочисленные известные алгоритмы разложения на множители. Например, произведение линейных делителей полинома F(U) равно наибольшему общему делителю полиномов: GCD(F(U), U^p-U) и быстро вычисляется алгоритмом Евклида [A. Menezes, P. Van Oorchot, S. Vanstone. Handbook of applied cryptography, CRC press, 1996].

Полиномы деления f_l (x) и модулярные полиномы $W_l(U, V)$ для функций Вебера вычислимы, например, [math.mit.edu/~drew/WeberModPolys.htm]. Так, модулярные полиномы W_l для изогений степени l=5, 7, 11, 13, 17, 29 имеют вид:

$W_5=U^6+V^6-U^5V^5+4UV$;

$W_7=U^8+V^8-U^7V^7+7U^4V^4-8UV$;

$W_{11}=U^{12}+V^{12}-U^{11}V^{11}+11U^9V^9-44U^7V^7+88U^5V^5-88U^3V^3+32UV$;

$W_{13}=U^{14}+V^{14}-U^{13}V^{13}+13U^{12}V^2+13U^2V^{12}+52U^{10}V^4+52U^4V^{10}+78U^8V^6+78U^6V^8+64UV$;

$W_{17}=U^{18}+V^{18}-U^{17}V^{17}+17U^{16}V^{10}+17U^{10}V^{16}-34U^{15}V^3-34U^3V^{15}+34U^{13}V^{13}+119U^{12}V^6+119U^6V^{12}+340U^9V^9+272U^8V^2+272U^2V^8+544U^5V^5-256UV$;

$W_{29}=U^{30}+V^{30}-U^{29}V^{29}+29U^{29}V^5+29U^5V^{29}+261U^{28}V^{10}+261U^{10}V^{28}+783U^{27}V^{15}+783U^{15}V^{27}+667U^{27}V^{20}+667U^{20}V^{27}-116U^{25}V-116UV^2+203U^{25}V^{25}+5365U^{24}V^6+5365U^6V^{24}-5713U^{22}V^{16}-5713U^{16}V^{22}-1334U^{21}V^{21}+4716U^{20}V^2+4716U^2V^{20}+37642U^{18}V^{12}+37642U^{12}V^{18}+12470U^{17}V^{17}-50112U^{15}V^3-50112U^3V^{15}-91408U^{14}V^8-91408U^8V^{14}-49880U^{13}V^{13}+170752U^{10}V^4+170752U^4V^{10}+85376U^9V^9-207872U^5V^5+16384UV$

Направление на цикле изогении задается следующим упрощением формул Велу. Пусть исходная эллиптическая кривая задана уравнением $y^2=x^3+Ax+B$, а ее образ для изогении степени l задан уравнением $y^2=x^3+A_1x+B_1$. x-координаты точек ядра изогении степени l - задаются делителем степени $d=\frac{l-1}{2}$ полинома деления $f_l(x)$. Обозначим этот делитель

$h_l(x)=x^d+c_1x^{d-1}+c_2x^{d-2}+c_3x^{d-3}+\ldots+c_d$

Коэффициенты A_1, B_1 изогенного образа эллиптической кривой равны:

$A_1\equiv -A(10d-1)-30(c_1^2+2c_2) \pmod p$;

$B_1\equiv -B(28d-1)+70(c_1^3+3c_1c_2+3c_3)+42Ac_1 \pmod p$.

Положительное направление на цикле изогении можно задавать иначе, например, выбором одного из двух возможных значений отображения Фробениуса для заданного ядра изогении [Elkies N. Elliptic and modular curves over finite fields and related computational issues. Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.; AMS/International Press, 1998), p.21-76]. Эти значения одинаковы для всех изогенных эллиптических кривых и могут быть определены заранее (входить в состав программного обеспечения, реализующего криптосистему).

Для практических приложений число классов h должно быть достаточно большим, чтобы перебор всех изогенных эллиптических кривых был невозможен, например $h>2^{256}$. Для этого числа p, D должны иметь длину примерно 500-550 бит.

Число используемых изогении k и максимальная длина N_{max} изогений каждой длины оценивается из условия, что почти каждое значение функции Вебера из h возможных значений можно получить, меняя длины цепочек. Если число используемых степеней изогении k=1, то $N_{max}=h/2$, если k=2, то $N_{max}\sqrt{h/4}$, в общем случае $N_{max}=(h*2^{-k})^{1/k}$. Если $h\approx 2^{256}$, то при k=50 получаем $N_{max}\approx 18$, если K=80, то $N_{max}\approx 5$. Поскольку случайный дискриминант является квадратом по модулю l_i примерно для половины простых чисел l_i, а случайное число l является простым с

вероятностью $\frac{1}{\ln 1}$, то при использовании 50 малых простых l_i получаем максимальную степень используемой степени изогении $l_{max} \approx 547$. Соответствующий симметрический полином W_l (U, V) имеет длину 869 килобайт.

Рассмотрим примеры реализации заявленного способа для небольших чисел p.

Пример 1. Циклы функций Вебера. Исходная эллиптическая кривая задана уравнением $y^2=x^3+x+3$ (mod 971) и имеет параметры D=-2588, j=42,число классов h=23, функция Вебера равна g=466.

Дискриминант D является ненулевым квадратом по модулю l=7, 13, 17. Используем полиномы W_7 , W_{13}, W_{17}.

Для изогении степени 7 модулярный полином W_7(U, g) имеет два корня по модулю p: 92 и 881. Подставляем значение 881, полином W_7(U, 881) имеет два корня: 466, соответствующий предыдущему значению, и 701 - новый элемент цикла. Продолжаем эту процедуру далее и получаем цикл функций Вебера степени 7 длины h для направления, заданного корнем 881: (466, 881, 701, 120, 300, 397, 952, 108, 697, 140, 411, 839, 812, 903, 171, 374, 639, 963, 459, 613, 545, 71, 92).

Для изогении степени 13 модулярный полином W_{13}(U, g) имеет два корня по модулю p: 300 и 613. Строим цикл функций Вебера длины h для направления, заданного корнем 613. Получаем цикл (466, 613, 374, 839, 108, 120, 92, 459, 171, 411, 952, 701, 71, 963, 903, 140, 397, 881, 545, 639, 812, 697, 300).

Для изогении степени 17 модулярный полином W_{17}(U, g) имеет два корня по модулю p: 545 и 120. Строим цикл изогений степени 17 длины h для направления, заданного корнем 545. Получаем (466, 545, 963, 171, 839, 697, 397, 701, 92, 613, 639, 903, 411, 108, 300, 881, 71, 459, 374, 812, 140, 952, 120).

Пример 2. Определение положительного направления на цикле изогений. Исходная эллиптическая кривая задана уравнением $y^2=x^3+x+1$ (mod 1187), имеет значение следа T=-12, дискриминант отображения Фробениуса D_π =4D где D=-1151, значение функции Вебера g_0 =123. Дискриминант D является квадратом по модулю простых чисел l_1=5, l_2=7, l_3=11, l_4 =29. Эти простые числа задают степени используемых изогений.

Уравнение отображения Фробениуса π^2-Tπ +p=0 имеет корни $\alpha = -6 + \sqrt{D}$, $\bar{\alpha} = -6 - \sqrt{D}$. Находим, для каких наименьших степеней расширения d число точек эллиптической кривой над полем из p^d элементов, равное $p^d + 1 + \alpha^d + \bar{\alpha}^d$, делится на l_i. Получаем для l_1=5 степень d=1; для l_2=7 степень d=1; для l_3 =11 степень d=5; для l_4=29 степень d=7.

Задаем положительное направление на цикле изогении. Для изогении степени 5 модулярный полином W_5(U, g_0) имеет два корня: 487 и 486. Находим $h_2(x)=GCD(x^p-x, f_5(x))=645+74x+x^2$ (это произведение двух линейных полиномов), отсюда A_1=223, B_1 =348, функция Вебера имеет два противоположных значения 487 и 700, первое из них совпадает с одним из корней полинома W_5(U, g_0). Положительное направление на цикле изогений для изогении степени 5 задается значением g=487, а отрицательное направление - другим корнем полинома W_5(U, g_0): g=486.

Для изогении степени 7 полином W_7(U, g_0) имеет два корня: 529 и 576. Для задания положительного направления находим $h_3(x)=GCD(x^p-x, f_5(x))=63+374x+1121x^2+x^3$ (это произведение трех линейных полиномов), отсюда A_1 =935, B_1=568, функция Вебера имеет два противоположных значения 576 и 611, первое из них совпадает с одним из корней полинома Вебера. Положительное направление на цикле изогении для изогении степени 5 задается значением g=576, а отрицательное направление - другим корнем полинома Вебера g=529.

Для изогении степени 11 полином W_{11}(U, g_0) имеет два корня: 227 и 84. Полином деления $f_{11}(x)$ имеет два неприводимых делителя степени 5, найденные как $GCD\left(x^{p^5}-x, f_{11}(x)\right): 1146+922x+178x^2+446x^3+39x^4+x^5$ и $100+523x+943x^2+1158x^3+1184x^4+x^5$, задающие расширение степени 5. Расширенное поле K можно задавать любым неприводимым полиномом степени 5. Зададим поле K первым полиномом и обозначим t - корень первого полинома, y - координата точки ядра при x=t равна $\sqrt{t^3+t+1} \in K$ - обе координаты точки ядра лежат в поле степени расширения 5. Зададим поле K вторым полиномом и обозначим s - корень второго полинома, y - координата точки ядра при x=s равна $\sqrt{s^3+s+1} \notin K$ (она лежит в поле степени расширения 10). Для задания положительного направления выбираем первый делитель: h_5 (x)=1146+922x+178x^2+446x^3+39x^4 +x^5, отсюда A_1=73, B_1=758, функция Вебера имеет два противоположных значения 227 и 960, первое из них совпадает с одним из корней полинома Вебера.

Положительное направление на цикле изогений для изогении степени 5 задается значением g=227, а отрицательное направление - другим корнем полинома Вебера g=84.

Для изогении степени 29 полином $W_{29}(U, g_0)$ имеет два корня: 314 и 165. Для задания положительного направления находим делитель степени 14 полинома $f_{29}(x):h_{14}(x)=668+657x+1140x^2+256x^3+131x^4+841x^5+483x^6+484x^7+667x^8+987x^9+48x^{10}+743x^{11}+978x^{12}+1079x^{13}+x^{14}$ (это произведение двух неприводимых полиномов степени 7), отсюда $A_1=623$, $B_1=1128$, функция Вебера имеет два противоположных значения 165 и 1022, первое из них совпадает с одним из корней полинома Вебера.

Объяснение терминов, используемых в описании и формуле изобретения.

Запись $a\equiv b \pmod p$ означает, что a-b делится на p.

Конечное поле F_p из p элементов, где число p - простое множество {0, 1, ..., p-1}. Сложение и умножение в конечном поле 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, $3+4\equiv 0 \pmod 7$, $3\cdot 4\equiv 5 \pmod 7$. Для любого ненулевого элемента a существует обратный элемент a^{-1} такой, что $aa^{-1}=1$. Элемент a^{-1} может быть найден расширенным алгоритмом Евклида. Конечное поле F_p допускает конечные расширения, получаемые присоединением корней неприводимых полиномов. Степень расширения равна степени неприводимого полинома, корень которого присоединяется. Если t - корень неприводимого полинома f степени d, то остальные корни равны $t^p \pmod{f(t)}$, $t^{p^2} \pmod{f(t)}$, ..., $t^{p^{d-1}} \pmod{f(t)}$. Присоединение корней всех неприводимых полиномов дает алгебраическое замыкание поля F_p.

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 $E(F_p)$ над полем из $p>3$ элементов состоит из точек проективной плоскости, удовлетворяющих однородному кубическому уравнению $f(X, Y, Z)=0$, причем ни в одной точке кривой все три частных производных полинома f не обращаются в 0 одновременно. Например, уравнение в форме Вейерштрасса $Y^2Z=X^3+AXZ^2+BZ^3$, где $A, B\in F_p$, $4A^3+27B^2\neq 0 \pmod p$.

Точки эллиптической кривой допускают сложение: $P_1+P_2=P_3$ для любых P_1 P_2, причем $P_1+P_2=P_2+P_1$, $P_1+(P_2+P_3)=(P_1+P_2)+P_3$ для любых P_1, P, P_3. Если эллиптическая кривая задана уравнением в форме Вейерштрасса, то нулевым элементом по сложению является точка $P_\infty=(0, 1, 0)$. Все остальные точки удовлетворяют уравнению $y^2=x^3+Ax+B$, $x=X/Z$, $y=Y/Z$. Противоположной к точке (x, y) является точка (x, -y).

На эллиптической кривой $E(F_p)$ действует отображение Фробениуса π $(X, Y, Z)=(X^p, Y^p, Z^p)$, отображающее кривую в себя, при этом $\pi(P_1+P_2)=\pi(P_1)+\pi(P_2)$. Отображение Фробениуса удовлетворяет уравнению $\pi^2-T\pi+p=0$ с дискриминантом $D_\pi=T^2-4p<0$, где $|T|<2\sqrt{p}$ - целое число. Число точек r эллиптической кривой $E(F_p)$ равно $r=p+1-T$. При переходе к конечным расширениям поля F_p число точек остается конечным. Скрученные эллиптические кривые обладают противоположными значениями T, одинаковым значением дискриминанта D_π , но различными числами точек. Дискриминант отображения Фробениуса может допускать разложение вида $D_\pi=Dc^2$ для целого c.

Число приведенных квадратичных форм (a, b, c), $0<a\leq c$, $-a<b\leq a$, $b>0$ при $a=c$, называется числом классов.

Если α , $\overline{\alpha}$ - комплексные корни уравнения Фробениуса, то число точек эллиптической кривой над расширением степени n исходного поля F_p равно $p^n+1-\alpha^n-\overline{\alpha^n}$.

Изоморфизм эллиптических кривых задается обратимой линейной заменой переменных. Эллиптическая кривая с точностью до изоморфизма над алгебраически замкнутым полем характеризуется своим j-инвариантом [Silverman J. The arithmetic of elliptic curves. - Springer-Verlag, 1986]. Если эллиптическая кривая задана уравнением в форме Вейерштрасса, то $j = 1728\frac{4A^3}{4A^3 + 27B^2}$. Скрученные кривые изоморфны над квадратичным расширением поля F_p.

Инвариант эллиптической кривой $E(F_p)$ с дискриминантом D_π равен приведенному по модулю p значению модулярной функции $j(\tau)$ комплексной переменной τ для некоторого значения τ, связанного с уравнением кривой.

Существует функция Вебера $g(\tau)$, связанная с функцией j соотношением $j(\tau) = \frac{(g(\tau)^{24} - 16)^3}{g(\tau)^{24}}$. Если $D=D_\pi/c^2 \equiv 1 \pmod 8$ для целого c, то по зависимость между j и g взаимно однозначная [N. Yui, D. Zagier. On the singular values of Weber modular functions // Mathematics of computation, 1997, v.66, 1645-1662].

Если две эллиптические кривые в форме Вейерштрасса $E_1(F_p)$, $E_2(F_p)$, обладающие инвариантами j_1, j_2 соответственно, имеют одинаковое число точек над полем F_p или его квадратичным расширением, то существует изогения - отображение первой кривой во вторую и обратно, заданное дробями полиномов с коэффициентами из F_p. Число неизоморфных эллиптических кривых, обладающих одинаковым числом точек, называется числом классов дискриминанта D_π и по порядку величины близко к $\sqrt{|D_\pi|}$.

Ядро изогении $\phi : E_1 \to E_2$ - точки кривой E_1, рассматриваемой над алгебраически замкнутым полем, отображающиеся в нулевой элемент кривой E_2, конечно. Изогения полностью определяется своим ядром. Число точек ядра называется также степенью изогении $\phi : E_1 \to E_2$. Дуальная изогения $\hat{\varphi} : E_2 \to E_1$ имеет такую же степень. Изогения степени l для эллиптической кривой $E(F_p)$ существует, если число точек эллиптической кривой над некоторым конечным расширением поля F_p делится на l. Поэтому для изогении степени l существует наименьшая степень расширения поля F_p такая, что число точек эллиптической кривой над этим расширением делится на l.

Изогении допускают умножение, степень произведения изогений равна произведению степеней исходных изогений, поэтому достаточно рассматривать только изогении простых степеней. Произведение изогений коммутативно и ассоциативно: $\phi_1\phi_2=\phi_2\phi_1$, $\phi_1(\phi_2\phi_3)=(\phi_1\phi_2)\phi_3$.

Изогения может быть вычислена по формулам Велу [Velu J. Isogenies entre courbes elliptiques. C.R. Acad. Sc. Paris, 273 (1971), 238-241]. Пусть $E_1(F_p): y^2=x^3+Ax+B$; $E_2(F_p): v^2=u^3+A_1u+B_1$, и $(x_R,y_R) \in E_1(F_p)$ - точка нечетного порядка l. Для точки Q из ядра изогении положим

$s_Q=4x_Q^3+4Ax_Q+4B$, $t_Q=6x_Q^2+4A$.

Кривая $E_2(F_p)$ задается коэффициентами

$$A_1 = A - 5\sum_{Q \in R} t_Q,\ B_1 = B - 7\sum_{Q \in R}(s_Q + x_Q t_Q).$$

Ядро изогении простой нечетной степени l для эллиптической кривой в форме Вейерштрасса состоит из l^2 точек порядка l, x-координаты которых являются корнями полиномов деления $f_l(x)$ степени $(l^2-1)/2$.

Полиномы деления определяются рекуррентно [J. Silverman. The arithmetic of elliptic curves. - Springer-Verlag, 1986]:

$\psi_0=0$, $\psi_1=1$, $\psi_2=2y$,

$\psi_3=3x^4+6Ax^2+12Bx-A^2$,

$\psi_4=4y(x^6+5Ax^4+20Bx^2-5A^2x^2-4ABx-8B^2-A^3)$,

$2y\psi_{2n}=\psi_n(\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n-1}^2)$, $n>2$,

$\psi_{2n+1}=\psi_{n+2}\psi_n^3-\psi_{n+1}^3\psi_{n-1}$, $n<1$,

$f_n(x)=\psi_n(x, y)$,

если n нечетное, и

$f_n(x)=\psi_n(x, y)/y$,

если n четное.

Полиномы f_l раскладываются на множители. Координаты точек ядра изогении степени l являются корнями одного и того же неприводимого делителя полинома деления $f_l(x)$.

Существует алгоритм Чуфа для вычисления числа точек эллиптической кривой над конечным полем и его улучшение Элкиса [N. Elkies. Elliptic and modular curves over finite fields and related issuses // Proceedings of a conference in honor of A.O.L. Atkin, AMS international press, 1998, pp.21-76]. Изогения Элкиса - изогения, по модулю степени которой дискриминант Фробениуса является квадратом. Для изогении Элкиса степени l характеристический полином отображения Фробениуса раскладывается на линейные множители по модулю l. Дуальные изогении соответствуют различным корням полинома отображения Фробениуса по модулю l.

Для изогении Элкиса степени l и кривой E_0 с инвариантом j_0 существует ровно два изогенных образа, соответствующие двум дуальным изогениям (для исходной и скрученной кривой). При этом существует целочисленный симметрический модулярный полином $\Phi_l(U, V)$, такой, что $\Phi_l(U, j_0)$ (mod p) имеет два корня, соответствующие двум дуальным изогениям. Обозначим один из корней через j_1. Тогда можно построить цикл изогений степени l вида $j_0 \to j_1 \to \ldots \to j_0$. Длина цикла является делителем числа классов. При изменении степени изогении цикл состоит из тех же j-инвариантов, но переставленных. Множество точек (U, V), таких, что $\Phi_l(U, V)=0$, называется классической модулярной кривой $X_0(l)$.

На практике если $D \equiv 1 \pmod 8$, то вместо полиномов Φ_l удобнее рассматривать полиномы W_l для функции Вебера g,

$$j=\frac{(g^{24}-16)^3}{g^{24}}$$

удовлетворяющей уравнению . Это полиномы тоже симметрические, разреженные, имеют меньшие коэффициенты и позволяют строить аналогичные циклы для функции Вебера.

Квантовая атака основана на вычислении секретного ключа с помощью квантового компьютера.

Формула изобретения

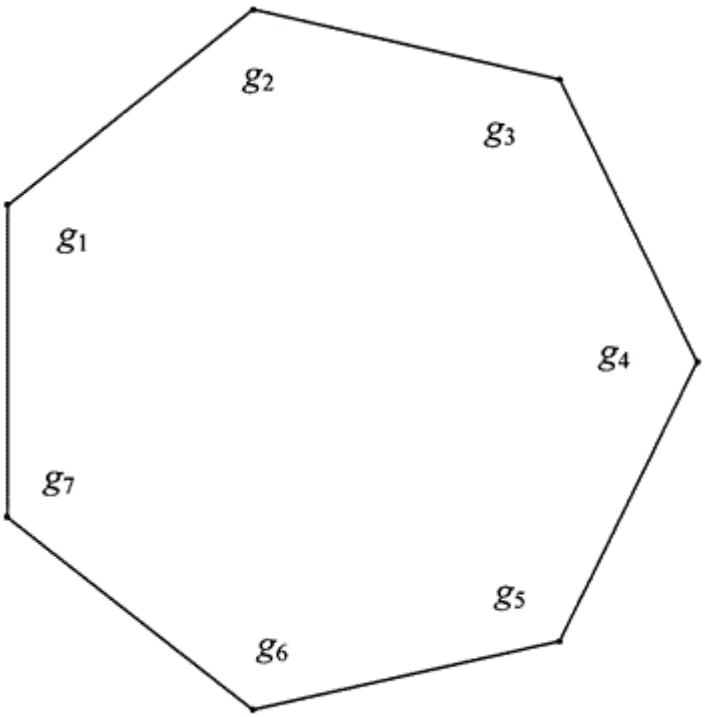
1. Способ шифрования с защитой от квантовых атак на основе циклов функций Вебера, в котором сообщение зашифровывают с использованием открытого ключа и зашифрованное сообщение расшифровывают при помощи секретного ключа, содержащий первую эллиптическую кривую и вторую эллиптическую кривую с одинаковыми дискриминантами Фробениуса, соответствующие открытому ключу, и отображение первой эллиптической кривой во вторую эллиптическую кривую, соответствующее секретному ключу, отличающийся тем, что эллиптические кривые задают значениями функции Вебера, причем секретный ключ определяют как цепочку отображений функций Вебера, соответствующих изогениям Элкиса степеней $l_1, \ldots, l_k$, заданную набором целых чисел $N_1, \ldots, N_k$, где N_i - число шагов по циклу функций Вебера для изогении степени l_i, при этом очередное значение функции Вебера g_{i+1} определяют как корень симметрического полинома двух переменных при замене одной переменной на предыдущее значение функции Вебера g_i, а при переходе к изогении очередной степени задают положительное направление на цикле, для этого находят полином, задающий ядро изогении, а шаги по циклу выполняют в направлении, соответствующем знаку числа N_i.

2. Способ по п.1, отличающийся тем, что дискриминант Фробениуса выбирают равным произведению квадрата целого числа на число, сравнимое с 1 по модулю 8.

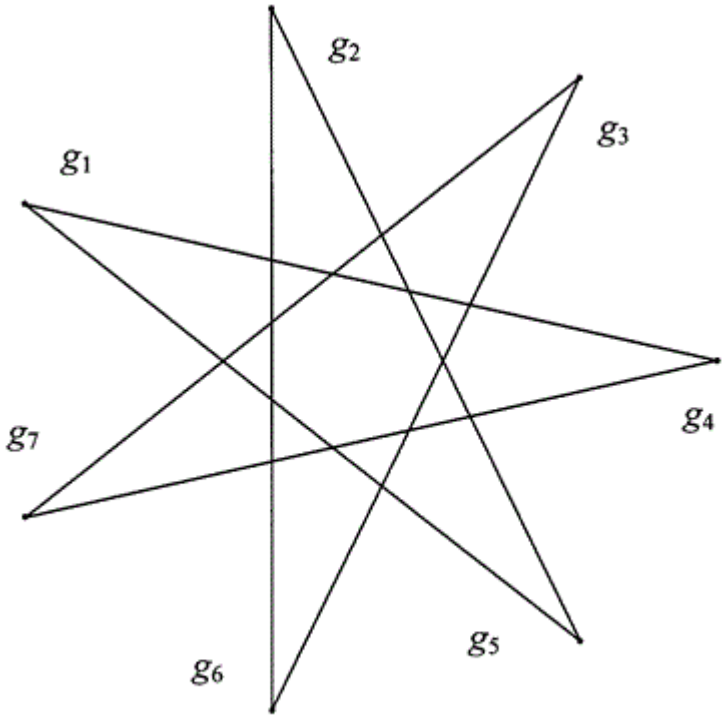
3. Способ по п.1, отличающийся тем, что ядро изогении задают полиномом, для которого точки ядра которого лежат в расширении минимальной степени, и по его коэффициентам

находят функцию Вебера, соответствующую положительному направлению.

РИСУНКИ



Фиг. 1



Фиг. 2