УДК 681.3

АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ СЛОЖНОСТИ ИЗВЛЕЧЕНИЯ КОРНЕЙ В КОНЕЧНЫХ ГРУППАХ ИЗВЕСТНОГО ПОРЯДКА

Е. С. Дернова,
аспирант
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
В. И. Избаш,
канд. физ.-мат. наук, заведующий лабораторией
Институт математики и информатики Академии наук Молдовы
Д. Ю. Гурьянов,
инженер
Д. Н. Молдовян,
инженер
НФ ФГУП НИИ «Вектор» — специализированный центр программных систем «Спектр»

Приводится способ построения конечных групп для вычислительно эффективных алгоритмов электронной цифровой подписи и обосновывается новый криптографический примитив — сложная задача вычисления корней большой простой степени в нециклических группах, порядок циклических подгрупп которых делится на квадрат степени корня. Предложен алгоритм электронной цифровой подписи на основе новой задачи и обсуждается его стойкость.

Введение

В работе [1] в качестве нового примитива алгоритмов электронной цифровой подписи (ЭЦП) предложена задача извлечения корней большой простой степени в конечных группах известного порядка, решение которой имеет достаточно высокую трудоемкость при условии, что квадрат степени корня делит порядок группы. Предложенные алгоритмы ЭЦП на основе данной задачи представляют интерес для разработки протоколов коллективной подписи. Указанный новый примитив апробирован для случая конечных циклических групп, элементами которых являются классы вычетов по простому модулю. Однако алгоритмы на основе таких групп имеют достаточную стойкость только при использовании простого модуля, имеющего размер 1024 бит или более, что связано с тем, что задача извлечения корней произвольной степени зависит от задачи дискретного логарифмирования, а для решения последней известны алгоритмы решения, имеющие субэкспоненциальную сложность [2]. Решение первой задачи не может быть существенно сложнее, чем второй. Поскольку сложность процедур формирования и проверки ЭЦП пропорциональна квадрату длины модуля, то указанная зависимость между задачей извлечения корня и дискретного логарифмирования приводит к ограничению производительности алгоритмов ЭЦП на основе конечных числовых групп. Использование конечных групп точек эллиптической кривой, задача дискретного логарифмирования в которых имеет экспоненциальную сложность [3], для построения алгоритмов, основанных на сложности нахождения корней, является проблематичным из-за проблем генерации эллиптической кривой, число точек которой делится на квадрат большого простого числа.

В настоящей работе рассматриваются новые конечные группы с требуемым значением порядка и на их базе разрабатываются алгоритмы ЭЦП, основанные на сложности извлечения корней простой степени, имеющей размер не менее 160 бит. Использование новых групп, элементы которых имеют размер 640 бит, обеспечивает повышение производительности алгоритмов ЭЦП более чем в 2 раза по сравнению с алгоритмами на основе числовых групп.

Новые конечные группы

Рассматриваемые ниже конечные группы содержат элементы, прототипом которых являются целые числа Гаусса [4, с. 74] вида $a + bi$, где a и b —

целые числа, называемые координатами, над которыми определены операции сложения и умножения по правилу сложения и умножения многочленов, при условии, что квадрат формальной переменной i принимается равным -1, т. е. $i^2 = -1$. Для получения конечных алгебраических структур, состоящих из пар чисел вида $(a, b) = a + bi$, мы определяем операции умножения и сложения координат по модулю m. Поэтому рассматриваемые в данной статье структуры содержат не более m^2 элементов. Кроме того, мы задаем по определению $i^2 = \varepsilon$, где $\varepsilon \in \{1, ..., m-1\}$ — параметр, входящий в определение операции умножения. Выбор параметра ε, так же как и значения m, существенно влияет на свойства задаваемой конечной алгебраической структуры. Таким образом, операция сложения пар (a, b) и (c, d) выполняется как сложение одноименных координат по модулю m, т. е.

$$(a, b) + (c, d) = ((a + c) \bmod m; (b + d) \bmod m) = g + hi,$$

где $g = (a + c) \bmod m$ и $h = (b + d) \bmod m$, а умножение векторов — по правилу

$$(a, b)(c, d) = ((ac + \varepsilon bd) \bmod m; (ad + bc) \bmod m) = g' + h'i,$$

где $g' = (ac + \varepsilon bd) \bmod m$ и $h' = (ad + bc) \bmod m$. Легко проверить, что определенные таким образом операции сложения и умножения обладают свойствами ассоциативности и коммутативности. Ниже мы покажем, что среди алгебраических структур такого типа имеются конечные поля и мультипликативные группы, существенным свойством которых является наличие единицы $E = (1, 0)$ — нейтрального элемента по умножению, который определяет существование для каждой ненулевой пары A единственного обратного значения A^{-1} такого, что $AA^{-1} = E$. В полях существует также нуль $O = (0, 0)$ — нейтральный элемент по сложению, при этом каждому элементу B может быть сопоставлен в соответствие единственный противоположный элемент $-B$ такой, что $B + (-B) = O$.

Группа — это алгебраическая структура с ассоциативной операцией, для которой существует обратная операция [5, 6], т. е. уравнения $AX = B$ и $YA = B$ имеют единственное решение для любых элементов A и B. Поскольку определенная выше операция умножения является коммутативной, то указанные уравнения являются эквивалентными, и можно рассматривать только одно из них. Легко показать, что однозначность решения указанных уравнений выполняется, если для каждого элемента A существует единственное обратное значение A^{-1}, поэтому интересно рассмотреть решение уравнений вида $AX = E$, которое можно представить таким образом:

$$(a + bi)(x + yi) = ((ax + \varepsilon by) \bmod m) + (ay + bx) \bmod m)i = 1 + 0i.$$

Из этой записи вытекает, что для определения обратных значений следует решать следующую систему из двух линейных сравнений с двумя неизвестными:

$$\begin{cases} ax + \varepsilon by \equiv 1 \bmod m \\ bx + ay \equiv 0 \bmod m \end{cases}.$$

Рассмотрим существование решений этой системы для случая использования в качестве модуля простого значения p. Приравнивая нулю главный определитель этой системы, получаем характеристическое уравнение

$$a^2 - \varepsilon b^2 \equiv 0 \bmod p.$$

Значение $(a, b) = (0, 0)$ является решением характеристического уравнения для любых значений модуля, поэтому для этой пары не существует обратного значения. Значения p и ε можно выбрать таким образом, что характеристическое уравнение не имеет других решений, а значит, рассматриваемая система сравнений имеет единственное решение для любой пары $(a, b) \neq (0, 0)$. Рассмотрим несколько важных частных случаев.

Случай 1. Значительный интерес представляет выбор в качестве параметра ε значения, которое является квадратичным невычетом по модулю p. В этом случае получаем структуру, являющуюся конечным полем $GF(p^2)$, мультипликативная группа которого имеет порядок

$$\Omega = p^2 - 1 = (p - 1)(p + 1).$$

Задавая различные значения модуля p и параметра ε, получаем разнообразные варианты конечного поля. Для заданного значения p имеем $(p - 1)/2$ разных вариантов поля $GF(p^2)$, включающих одно и то же множество элементов, но отличающихся видом операции умножения, соответственно числу различных квадратичных невычетов по модулю p.

Случай 2. Пусть в определении операции умножения используется параметр ε, который является квадратичным вычетом по модулю p. При этих условиях характеристическое уравнение имеет, кроме $(a, b) = (0, 0)$, еще $2(p - 1)$ следующих решений вида

$$(\varepsilon^{1/2} b \bmod p, b) \text{ и } (-\varepsilon^{1/2} b \bmod p, b),$$

где $b \in \{1, 2, ..., p - 1\}$. Для пар такого вида не существует решений системы сравнений, которые определяют значение обратных элементов. Следовательно, количество элементов, для которых существуют единственные обратные значения, равно

$$\Omega = p^2 - 2(p - 1) - 1 = (p - 1)^2.$$

Эти элементы составляют мультипликативную группу, поскольку результат умножения любых

двух элементов из этого множества является элементом этого же множества.

Ниже будет использоваться также случай построения группы, заданной по модулю, который не является простым. При этом общий анализ условий существования групп и определение их порядка является более сложным. Однако интересующий нас следующий частный случай составного модуля p^2, где p — простое число, позволяет получить формулы для расчета порядка группы при произвольных p.

Случай 3. Пусть используется значение p^2, где p — простое число, в качестве модуля, а параметр ε делится на p. При этих условиях для элементов (a, b) таких, что a не делится на p, характеристическое уравнение не имеет решений, поскольку $p \mid \varepsilon$, а определитель системы сравнений является взаимно простым с модулем p^2, т. е. для каждого из указанных элементов имеются обратные значения. При этом операция умножения двух элементов дает третий элемент, в котором первая координата также не делится на p, т. е. операция умножения является замкнутой на указанном множестве пар (a, b). Следовательно, это множество является группой, порядок которой можно определить из того факта, что число возможных значений первой координаты равно функции Эйлера от модуля $\varphi(p^2) = p(p-1)$, число возможных значений второй координаты равно p^2. Получаем следующую формулу для значения порядка построенной мультипликативной группы:

$$\Omega = p(p-1) \cdot p^2 = p^3(p-1).$$

Согласно теореме Силова [7], в этой группе содержатся подгруппы порядка p, p^2 и p^3, причем известна теорема, что любая подгруппа простого порядка является циклической, т. е. в построенной группе существуют циклические группы порядка p. Однако для поставленной конструктивной криптографической задачи требуется использовать циклические группы, порядок которых делится на квадрат простого числа. Поэтому для нас важно выяснить вопрос существования циклических подгрупп порядка p^2 и p^3. Ответ на него из теоретических рассмотрений получить достаточно трудно, поскольку для этого в настоящее время не предложены соответствующие подходы. Вопрос был выяснен экспериментально с помощью специально разработанной программы для ЭВМ. Опыт показал, что в построенной группе содержится циклическая группа порядка

$$\Omega' = p^2(p-1),$$

которая подходит для решения нашей задачи синтеза алгоритмов ЭЦП, основанных на вычислительной сложности нахождения корней большой простой степени в конечных мультипликативных группах.

Приведем некоторые примеры алгебраических структур, соответствующих рассмотренным случаям 1, 2 и 3 (в реальных применениях для построения алгоритмов ЭЦП требуется задать конечные группы при использовании модуля размером до 100 десятичных знаков, однако в этом месте дается только иллюстрация трех типов построенных выше конечных групп небольшими конкретными примерами).

Пример 1. Пусть $m = p = 10301$ — простое число и $\varepsilon = 10001$ — квадратичный невычет по модулю 10301. Элемент (17, 11) имеет порядок $\omega(17, 11) = 106110600 = 10300 \cdot 10302 = (p-1)(p+1)$ и является генератором мультипликативной группы конечного поля $GF(10301^2)$. Для криптографических приложений требуется выбирать такие простые значения модуля p, чтобы либо число $p-1$, либо число $p+1$ содержало большой простой делитель q, размер которого должен составлять 160 бит и более. В этом примере в качестве делителя q можно указать число 103. Циклическую подгруппу такого порядка генерирует элемент (6230, 0).

Пример 2. Пусть $m = p = 10301$ — простое число и $\varepsilon = 10002$ — квадратичный вычет по модулю 10301. Элемент (17, 11) имеет порядок $\omega(17, 11) = 10300 = (p-1)$, который является максимально возможным в рассматриваемой группе. Последнее означает, что циклических групп, порядок которых превышает значение $p-1$, не существует. Эксперимент показывает, что такая ситуация имеет место и для других значений простого числа p и квадратичного вычета $\varepsilon \pmod p$. Поэтому для построения алгоритмов ЭЦП, основанных на вычислительной сложности нахождения корней простой степени $q \mid p-1$, требуется использовать такие значения p, что $q^2 \mid p-1$, хотя порядок группы имеет значение $\Omega = (p-1)^2$, а следовательно, делится на квадрат любого делителя числа $p-1$.

Пример 3. Пусть $m = p^2 = 10201$, где $p = 101$ — простое число, и $\varepsilon = 101$. Элемент (7, 11) имеет порядок $\omega(7, 11) = 1020100$ и является генератором циклической группы порядка $p^2(p-1)$. Элемент (1718, 7660) имеет порядок $\omega(7, 11) = 10201$ и является генератором циклической группы порядка p^2. При рассмотрении алгоритмов ЭЦП будут использованы группы такого типа при больших значениях простого числа p.

Генерация простых чисел вида $p = Nk^2 + 1$ и $p = Nk^2 - 1$

В рассмотренных выше случаях 1 и 2 для синтеза алгоритмов ЭЦП, основанных на сложности вычисления корней большой простой степени, требуется использование простых чисел p, имеющих структуру $p = Nk^2 + 1$ или $p = Nk^2 - 1$. При разработке алгоритмов генерации чисел такого вида следует учитывать, что не для всех значений N могут быть найдены простые k, при которых значение $Nk^2 + 1$ также является простым. Такая же ситуация имеет место и для случая $p = Nk^2 - 1$. Для по-

вышения производительности процедуры генерации простых чисел указанного вида следует учитывать эти случаи.

Предложение 1. Простых чисел вида $Nk^2 + 1$, где k — простое нечетное число и $N \equiv 2 \bmod 6$, не существует, кроме числа 19.

Доказательство. Пусть $Nk^2 + 1 = p$. При $k = 3$ и $N = 2$ получаем $p = 19$ — простое число. Известно, что любое нечетное простое число имеет вид $6t \pm 1$ для некоторого целого положительного t. Пусть $k > 3$ — простое, тогда при $N = 6g + 2$ и некоторых целых g и G имеем

$$p = (6g + 2)(6t \pm 1)^2 + 1 = 6G + 3 = 3(2G + 1),$$

следовательно, число p делится на 3, т. е. не является простым. Предложение доказано.

Предложение 2. Простых чисел вида $Nk^2 - 1$, где $k > 3$ — простое число и $N \equiv 4 \bmod 6$, не существует.

Доказательство. Пусть $Nk^2 - 1 = p$ и $k > 3$. Пусть $k > 3$ — простое число, тогда при $N = 6g + 4$ и некоторых целых g и G' имеем

$$p = (6g + 4)(6t \pm 1)^2 - 1 = 6G' + 3 = 3(2G' + 1),$$

следовательно, число p делится на 3, т. е. не является простым. Предложение доказано.

Эксперимент показал, что для случаев $N \equiv 0 \bmod 6$ и $N \equiv 4 \bmod 6$ сравнительно легко можно найти простое k, такое, что $Nk^2 + 1$ — тоже простое. Также для случаев $N \equiv 0 \bmod 6$ и $N \equiv 2 \bmod 6$ сравнительно легко можно найти простое k, такое, что $Nk^2 - 1$ — тоже простое. В обоих случаях это можно сделать для любых длин числа k в интервале $8 < |k| < 512$ бит, который представляет практический интерес для разработки алгоритмов ЭЦП.

Процедура генерации простых чисел со структурой $p = Nk^2 + 1$ ранее рассматривалась в работе [8], где также показано, что для различных значений размера числа p и k могут быть достаточно легко сгенерированы. Это можно сделать двумя путями:

1) генерируется простое число k требуемого размера, а затем подбирается 16-битовое число N, при котором значение $p = Nk^2 + 1$ является простым;

2) фиксируется значение N, например $N = 6$, и генерируются случайные простые числа k до тех пор, пока не будет получено простое число $p = Nk^2 + 1$. Кроме того, значения p и k являются долговременными элементами алгоритма ЭЦП, поэтому требуемые для генерации несколько секунд не являются критичными на практике. В рассмотренном выше случае 3 на структуру простого числа никаких новых дополнительных требований не накладывается.

Синтез алгоритмов ЭЦП

Группы, относящиеся к случаям 1, 2 и 3, могут быть использованы для построения алгоритмов ЭЦП, основанных на сложности задачи нахождения корней большой простой степени k в конечных мультипликативных группах. При этом следует учитывать особенности этих групп, связанные с необходимостью использования подгрупп, порядок которых делится на квадрат степени корня. В первом случае следует найти такое простое число p, что либо $k^2 \mid p - 1$, либо $k^2 \mid p + 1$. Во втором случае для выбора простого модуля p имеется только один вариант, а именно $k^2 \mid p - 1$. В третьем случае в качестве степени k выбирается значение p и на структуру выбираемого простого модуля ограничений не накладывается. Во всех трех случаях рекомендуется обеспечить выполнение условия $|k| \geq 160$ бит.

Рассмотрим общую схему построения алгоритмов ЭЦП. В качестве секретного ключа используется элемент X группы Г порядка Ω такой, что $\omega(X) \geq k^2$. Открытый ключ генерируется по формуле $Y = X^k$. Процедура генерации ЭЦП состоит в следующем.

1. Выбирается случайный элемент T группы Г, такой, что $\omega(T) \geq k^2$.

2. Вычисляется значение $R = T^k$.

3. Вычисляется значение хэш-функции F_H от подписываемого документа M, к которому предварительно присоединяются координаты r_1 и r_2 элемента R: $E = F_H(M \| r_1 \| r_2)$, где $\|$ — операция конкатенации. Значение E является первым элементом ЭЦП.

4. Вычисляется второй элемент ЭЦП: $S = TX^E$.

Сформированная ЭЦП (E, S) включает два элемента, первый из которых является числом, а второй — элементом группы Г. Проверка подлинности ЭЦП осуществляется следующим образом.

1. Вычисляется значение $R' = Y^{\Omega - E} S^k$.

2. Вычисляется значение хэш-функции $E' = F_H(M \| r'_1 \| r'_2)$, где r'_1 и r'_2 — координаты элемента $R' \in \Gamma$.

3. Сравниваются значения E и E'. Если $E = E'$, то ЭЦП признается подлинной.

Рассмотренная схема построения алгоритма ЭЦП может быть реализована с использованием конкретной циклической группы Г, порядок которой делится на k^2. В качестве такой группы могут быть использованы группы, относящиеся к трем рассмотренным выше типам. Приведем конкретный пример, относящийся к использованию группы, порядок которой выражается формулой $\Omega = p^3(p - 1)$ (см. случай 3). Как было показано выше, в этой группе существуют элементы порядка $\omega = p^2(p - 1)$, т. е. в качестве степени корня следует взять значение p. Возьмем значение $p = 926\,181373187296779285466463658388731804980\,85133$. Тогда имеем значение модуля $m = p^2 = 85\,781193603910670542926266004387089\,657469649971461826592989643313157\,889560091089546797156276 89$.

В качестве коэффициента ε возьмем значение $101p$, т. е. $\varepsilon = 935443186919169747078321128294972619123030659843 3$.

Выбор группы данного конкретного вида вносит определенную специфику в синтезируемый алгоритм ЭЦП. При генерации случайного секретного ключа $X = (x_1, x_2) \in \Gamma$ следует делать проверку: наибольший общий делитель НОД $(p, x_1) = 1$ и $X^{p(p-1)} \neq (1, 0)$. Первое условие обеспечивает выбор в качестве секретного ключа элемента, принадлежащего группе Г. Второе условие обеспечивает выбор в качестве секретного ключа элемента, порядок которого делится на квадрат степени корня, который равен значению p^2 (согласно выбору $k = p$). Аналогичную проверку следует выполнить и при генерации случайного элемента $T = (t_1, t_2) \in \Gamma$. Если указанное условие не выполняется (вероятность этого события мала) для случайно выбранных координат x_1 и x_2 (или для координат t_1 и t_2), то следует выбрать новые случайные значения координат $x_1 \le p^2$ и $x_2 \le p^2$ (или координат $t_1 \le p^2$ и $t_2 \le p^2$). Указанной проверке удовлетворяет значение

$$X = (162748957475865968,\ 97871643950719457493284 95).$$

Возводя элемент $X \in \Gamma$ в степень k, получаем значение открытого ключа $Y = X^k = (y_1, y_2)$, где

$$y_1 = 212287848797788405237368553490440\ 785992618321256912292473768372302645 4\ 694663820975943984437961;$$

$$y_2 = 90646893590375535174289\ 45448340085264044576\ 035216096271083871680927648 35.$$

Сформируем случайное значение

$$T = (96846596736586738292216171,\ 37586931174658693746285927),$$

которое также удовлетворяет условиям проверки. Возводя элемент $T \in \Gamma$ в степень p, получаем значение «разового» открытого ключа $R = T^k = (r_1, r_2)$, где

$$r_1 = 66765277168220183839579881 2\ 603927841861722391575858247 9\ 6142950115356680631354\ 39573548109332464;$$

$$r_2 = 34812315529241802932559681604665\ 63282460623255695990065 4\ 75962954205823291.$$

Пусть получено значение хэш-функции $E = F_H(M \| r_1 \| r_2)$, равное 75867496586968496537352193793 67391846697037563 8. Тогда получаем следующее значение элемента ЭЦП $S = TX^E = (s_1, s_2)$:

$$s_1 = 82565941055476172164239390128263022\ 37218370734284428450969373421 2\ 95221722475025012259161992826;$$

$$s_2 = 42226075478492550295968174821517 3\ 23994008397847085785550433021 20\ 12892903897205453209052939744.$$

Для проверки подписи вычислим значение $R' = Y^{\Omega - E} S^k = (r'_1, r'_2)$:

$$r'_1 = 66765277168220183839579881 2\ 603927841861722391575858247 9\ 6142950115356680631354\ 39573548109332464;$$

$$r'_2 = 34812315529241802932559681604665\ 63282460623255695990065 4\ 75962954205823291.$$

Сравнение показывает, что $R' = R$, следовательно, имеем $E' = E$, т. е. сформированная ЭЦП проходит процедуру проверки подлинности. Аналогично можно реализовать алгоритмы ЭЦП и на группах, относящихся к типам, соответствующим случаям 1 и 2.

Оценка стойкости

Особенностью приведенной выше схемы ЭЦП является вычисление хэш-функции от подписываемого документа после присоединения к нему рандомизирующего значения R. Эта особенность ранее использована в алгоритме ЭЦП Шнорра [9] и лежит в основе способа формального доказательства стойкости алгоритмов ЭЦП, предложенного в работе [10]. Этот способ доказательства состоит в сведении предполагаемой успешной атаки на алгоритм ЭЦП (т. е. успешной подделки подписи) к алгоритму решения сложной задачи, лежащей в основе схемы ЭЦП. Показывается, что алгоритм атаки может быть использован для решения указанной сложной задачи, поэтому трудоемкость атаки не ниже трудоемкости решения этой задачи. За количественную меру стойкости схемы ЭЦП принимается трудоемкость решения сложной задачи, положенной в основу схемы ЭЦП. Подробно данный подход к формальному доказательству стойкости алгоритмов ЭЦП детально обсуждается в работе [11], где показано принципиальная важность использования вычисления значения хэш-функции после генерации рандомизирующего элемента. Последнее позволяет построить общую схему доказательства, в которой используется возможность подставить для формирования подписи две разных хэш-функции в момент, когда рандомизирующий элемент уже сформирован, а подпись еще не вычислялась. Алгоритм подделки ЭЦП одинаково успешно работает в обоих случаях, поскольку генерация рандомизирующего элемента выполняется независимо от хэш-функции. В результате имеются две различные подписи, полученные при использовании одного и того же рандомизирующего значения. На завершающем этапе доказательства показывается, что по этим подписям легко решить трудную вычислительную задачу, положенную в основу схемы ЭЦП, например задачу дискретного логарифма в алгоритме ЭЦП Шнорра.

Применительно к случаю алгоритма, описанного в предыдущем разделе, эта общая модель фор-

мального доказательства стойкости приводит к решению трудной вычислительной задачи извлечения корней большой простой степени в группах со специальным значением порядка. Действительно, пусть рандомизирующее значение $R = T^k = (r_1, r_2)$ использовано алгоритмом подделки подписи для двух различных хэш-функций F'_H и F''_H. В соответствии с рассматриваемым алгоритмом формирования и проверки ЭЦП имеем $E_1 = F'_H(M\|r_1\|r_2)$ и $E_2 = F''_H(M\|r_1\|r_2)$, причем с вероятностью, близкой к единице, $E_1 \neq E_2$. Алгоритм подделки дает два значения S_1 и S_2, удовлетворяющих соотношению

$$R = Y^{\Omega - E_1} S_1^k = Y^{\Omega - E_2} S_2^k,$$

из которого легко получить $Y^{E_2 - E_1} = S_2^k S_1^{-k} = (S_2 S_1^{-1})^k$, где значение S_1^{-1} может быть вычислено как $S_1^{-1} = S_1^{\Omega - k}$, и с высокой вероятностью НОД $(\Omega, E_1 - E_2) = 1$ (если это соотношение не выполнится, то атаку следует повторить несколько раз). Если последнее соотношение выполняется, то можно вычислить $e = (E_1 - E_2)^{-1} \bmod \Omega$ и

$$Y = [(S_2 S_1^{-1})^e]^k \Rightarrow X = Y^{1/k} = [(S_2 S_1^{-1})^e,$$

т. е. вычислен корень из значения Y. (Если требуется решить уравнение $X^k = A$, для которого существуют решения, то, предполагая, что A — это открытый ключ, и применяя атаку подделки подписи, мы решим это уравнение.) Таким образом, если существует атака подделки подписи в схеме ЭЦП, описанной в предыдущем разделе, то, применяя ее несколько раз, мы можем вычислить корень k-й степени. Это означает, что успешная атака имеет сложность одного порядка со сложностью лучшего алгоритма решения указанной сложной вычислительной задачи. Действительно, если имеется эффективный алгоритм решения этой задачи, то он непосредственно реализует успешную атаку по схеме: 1) вычисление секретного ключа X по открытому ключу $Y = X^k$ и 2) формирование подписи в соответствии со специфицированным алгоритмом ЭЦП. Если имеется эффективный алгоритм подделки подписи, то он может быть использован для нахождения корней большой простой степени k в группах, порядок которых делится на квадрат числа k.

Приведенное выше формальное доказательство стойкости, так же как и в случае доказательства стойкости других схем ЭЦП, сводит сложность атаки к сложности решения трудной вычислительной задачи, положенной в основу схемы ЭЦП. Количественная оценка стойкости связана с нахождением лучшего известного алгоритма решения этой задачи и определением числа операций, которые требуются для его выполнения, и объема используемой памяти. Лучшим известным алгоритмом вычисления корней в рассматриваемом нами случае является алгоритм, предложенный и описанный [1] для случая мультипликативных групп кольца $\boldsymbol{Z}_p$, где $p = Nk^2 + 1$ — простое число размером более 1024 бит и N — четное число. Трудоемкость этого алгоритма имеет порядок 2^w операций возведения в степень, где $w = 0{,}5|k|$, при использовании памяти порядка 2^w байт. Алгоритм из работы [1] может быть применен практически непосредственно для случая циклических мультипликативных групп (случай 1), а в случаях нециклических групп (случаи 2 и 3) он может быть использован в качестве аналога для разработки алгоритмов специально для этих случаев. Сложность вычисления корней в случае нециклических групп значительно сложнее, поскольку алгоритм требует нахождения и использования элементов B, непредставимых в виде k-й степени некоторых других элементов, причем эти элементы B должны выбираться из циклической подгруппы, которой принадлежит элемент Y. Вероятность такого выбора составляет примерно k^{-2} (для $p = 4k^2 + 1$) и p^{-1} в случаях 2 и 3, соответственно. Рассмотрение точной спецификации алгоритмов вычисления корней в нециклических группах требует детального изучения строения таких групп и представляет самостоятельную задачу. В настоящей работе можно ограничиться тем, что алгоритм из работы [1] дает точную оценку для случая циклических групп и нижнюю границу оценки сложности для случая нециклических групп, и задать в качестве безопасного значения длину степени, равную $|k| \geq 160$ бит. Более точная оценка, видимо, позволит значительно уменьшить величину $|k|$ при построении алгоритмов ЭЦП на основе нециклических групп (случаи 2 и 3). При этом может быть уменьшен также и размер модуля, по которому ведутся вычисления, что даст дополнительный выигрыш в производительности алгоритмов ЭЦП. Однако точная оценка сложности извлечения корней в нециклических группах требует детального исследования их строения, что составляет самостоятельную задачу. Предварительное рассмотрение этого вопроса позволило сделать предположение, что размер степени корня может быть уменьшен до значений $|k| \geq 80$ бит с сохранением минимального приемлемого уровня безопасности алгоритмов ЭЦП.

Сопоставление с известными алгоритмами

В таблице представлена сравнительная оценка производительности различных алгоритмов ЭЦП в случае обеспечения минимально допустимого сегодня уровня безопасности ЭЦП, равного 2^{80} операциям возведения в степень. При этом для трех представленных вариантов реализации алгоритма ЭЦП, отличающихся использованием групп, построенных для случаев 1, 2 и 3, получена одинаковая оценка относительной производительности, поскольку в настоящее время вопрос о точной оценке безопасного размера степени корня $|k|$ для случаев применения нециклических групп остает-

Алгоритм ЭЦП	Размер ЭЦП	Размер ОК	Производительность, отн. ед.
ГОСТ Р 34.10–94	320*	1024	1
ГОСТ Р 34.10–2001	320*	320*	2,5
DSA	320	320	2,5
Предложенный в настоящей работе	640	640	4**

* В спецификации стандартов рекомендуются размеры значений ЭЦП и открытого ключа (ОК), превышающие 320 бит.
** Для случая применения нециклических групп это является нижней оценкой производительности.

ся открытым, и для этих вариантов предполагается использование завышенного значения $|k| = 160$ бит.

Обсуждение результатов

Задача дискретного логарифмирования в определенных в данной работе новых алгебраических структурах существенно зависит от значения коэффициента ε. В пользу этого утверждения, в частности, свидетельствует тот факт, что порядок группы, образуемой в указанных структурах, в широких пределах зависит от ε. При выборе значения этого коэффициента следует стремиться к предотвращению возможности разработки специальных методов дискретного логарифмирования, которые за счет использования особых свойств конкретных групп, на основе которых работают алгоритмы ЭЦП, могут обеспечить существенное снижение сложности дискретного логарифмирования по сравнению с общими методами решения этой задачи, применимыми к группам любой природы. Можно предположить, что главным в этом вопросе является выяснение возможности применения метода, подобного методу вычисления индексов. С учетом этого выбор величин растягивающих коэффициентов при задании операции умножения векторов приобретает еще одно значение — их следует выбирать таким образом, чтобы возможность разложения элементов группы в произведение некоторых неразложимых элементов, принадлежащих достаточно малочисленному их подмножеству, имела малую вероятность (разложение рассматривается в бесконечном дискретном пространстве двухкоординатных элементов, операция умножения которых включает значение ε, заданное для рассматриваемой конечной группы или конечного поля таких элементов). На данный момент предполагается, что безопасный размер конечных групп поля обеспечивается выбором модуля m размером 320 бит и более.

Особый интерес в этом плане представляют нециклические группы, в которых решение задачи извлечения корней большой простой степени принципиально затруднено отсутствием генераторов нециклических групп и заданием открытого ключа в виде $Y = X^k$, где значения Y и X не являются привязанными к какой-либо заданной циклической подгруппе нециклической группы. Пользователи произвольно выбирают секретный ключ X и тем самым произвольно задают выбор циклической подгруппы из большого числа возможных вариантов (k^2 и p вариантов в случаях 2 и 3 соответственно), причем не задается генератор этой циклической подгруппы, что *снимает проблему вычисления корней путем предварительного вычисления дискретных логарифмов*. Применение сложности вычисления корней большой простой степени k в случае порядка группы, делящегося на k^2, в сочетании с нецикличностью самой группы дает принципиально новое качество, состоящее в том, что сложность задачи извлечения корней становится независимой от сложности задачи дискретного логарифмирования, т.е. первая вычислительно сложная задача становится в таких применениях самостоятельным криптографическим примитивом, какими являются хорошо известные задачи дискретного логарифмирования и факторизации.

Возникающая при анализе безопасности предложенных алгоритмов ЭЦП задача дискретного логарифмирования требует разработки новых решений, поэтому предложенные группы представляют интерес для развития направления разработки алгоритмов ЭЦП, взлом которых требует решения двух вычислительно трудных задач. Подход к построению таких алгоритмов, предложенный в работе [12], может быть расширен применением рассмотренных выше групп. В частности, способ, использованный в работе [12], может быть применен для синтеза алгоритмов ЭЦП, базирующихся на сложности решения задачи логарифмирования в рассмотренных выше группах и одной из следующих трудных математических задач: дискретного логарифмирования в конечном числовом поле, дискретного логарифмирования на эллиптической кривой и факторизации больших натуральных чисел специального вида.

По аналогии с работой [13] на основе рассмотренного в данной статье алгоритма ЭЦП можно реализовать более производительные протоколы коллективной и композиционной ЭЦП, позволяющих решить ряд нестандартных проблем придания юридической силы электронным документам, например задачу одновременного удаленного подписания контракта несколькими пользователями и задачу одновременного удаленного подписания пакета контрактов различными группами подписывающих.

Заключение

Для синтеза алгоритмов ЭЦП, основанных на вычислительной сложности задачи нахождения корней большой простой степени в конечных группах известного порядка, предложены новые типы

алгебраических структур. Составлены алгоритмы ЭЦП, которые примерно в 1,5 раза производительнее по сравнению с известными. Показано, что определенные параметры задания алгебраических структур при их выборе представляют собой нециклические конечные группы, порядок циклических подгрупп которых делится на квадрат большого простого числа, которое может быть использовано в качестве степени корня. В этом случае возрастает сложность вычисления корней по известным алгоритмам, причем эта сложная вычислительная задача приобретает характер самостоятельного криптографического примитива.

Отмечена возможность применения построенных алгоритмов для реализации протоколов коллективной и композиционной подписей, а также синтеза алгоритмов ЭЦП, взлом которых требует одновременного решения двух трудных вычислительных задач различного вида. Самостоятельность задачи вычисления корней в нециклических группах расширяет область поисков схем ЭЦП, взлом которых требует одновременного решения двух вычислительно трудных задач.

Данная работа поддержана грантом РФФИ № 08-07-90100-Мол_а и грантом АН Молдовы № 08.820.08.08 РФ.

Литература

1. **Молдовян Н. А.** Извлечение корней по простому модулю как криптографический примитив // Вестник СПбГУ. Сер. 10. 2008. Вып. 1. С. 100–105.
2. **Menezes A. J., van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, 1997. 780 p.
3. **Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А.** Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2006. 270 с.
4. **Ван дер Варден Б. Л.** Алгебра. СПб.; М.; Краснодар: Лань, 2004. 623 с.
5. **Курош А. Г.** Курс высшей алгебры. М.: Наука, 1971. 431 с.
6. **Кострикин А. И.** Введение в алгебру. Основы алгебры. М.: Физматлит, 1994. 320 с.
7. **Каргаполов М. И., Мерзляков Ю. И.** Основы теории групп. М.: Физматлит, 1996. 287 с.
8. **Moldovyan N. A.** Digital Signature Scheme Based on a New Hard Problem // Computer Science Journal of Moldova. 2008. Vol. 16. N 2. P. 192–208.
9. **Schnorr C. P.** Efficient signature generation by smart cards // J. Cryptology. 1991. Vol. 4. P. 161–174.
10. **Koblitz N., Menezes A. J.** Another Look at Provable Security // J. Cryptology. 2007. Vol. 20. P. 3–38.
11. **Pointcheval D., Stern J.** Security Arguments for Digital Signatures and Blind Signatures // J. Cryptology. 2000. Vol. 13. P. 361–396.
12. **Дернова Е. С., Костин А. А., Молдовян Н. А.** Построение схем ЭЦП, раскрытие которых требует одновременного решения двух трудных задач // Инновационная деятельность в Вооруженных силах Российской Федерации: Тр. всеармейской науч.-практ. конф. 23–24 ноября 2006. Санкт-Петербург. СПб.: ВАС, 2006. С. 190–194.
13. **Ананьев М. Ю., Гортинская Л. В., Молдовян Н. А.** Протоколы коллективной подписи на основе свертки индивидуальных параметров // Информационно-управляющие системы. 2008. № 2. С. 34–36.