Math-Net.Ru

Общероссийский математический портал

М. А. Черепнев, О связи сложностей задач дискретного логарифмирования и Диффи–Хеллмана, *Дискрет. матем.*, 1996, том 8, выпуск 3, 22–30

DOI: <https://doi.org/10.4213/dm528>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.205.225.156

26 апреля 2023 г., 13:25:25

О связи сложностей задач дискретного логарифмирования и Диффи–Хеллмана

© 1996 г. М. А. Черепнев

Доказывается, что при некоторых допущениях теоретического характера в достаточно общем случае сложность L задачи дискретного логарифмирования в произвольной циклической группе порядка m оценивается через сложность D задачи Диффи–Хеллмана по формуле

$$L \leq \exp \left\{ \frac{\log D \log m}{\log \log m \log \log \log m} \right\},$$

что в случае полиномиальной оценки для D дает субэкспоненциальную оценку для L .

Задачи дискретного логарифмирования и Диффи–Хеллмана являются типовыми при рассмотрении криптографических протоколов [1].

Введем следующие обозначения. Пусть $G(t, m)$ — произвольная коммутативная циклическая группа порядка m с операцией, которую будем в дальнейшем обозначать $+$, требующей для своего выполнения t битовых операций, и пусть $L(t, m)$ обозначает минимальное количество битовых операций, необходимых для решения задачи дискретного логарифмирования в группе $G(t, m)$: при известных $a, b \in G(t, m)$ найти $n \in \mathbb{N}$ такое, что

$$a = nb; \tag{1}$$

здесь nb есть $b + \dots + b$, где элемент b повторен n раз.

Не ограничивая общности дальнейших рассуждений, будем считать b образующим группы $G(t, m)$. Заметим, что число n при таком определении nb можно считать вычетом по модулю m .

Пусть $D(t, m)$ обозначает минимальное количество битовых операций, необходимых для решения задачи, которую в дальнейшем будем называть задачей Диффи–Хеллмана:

при известных a_1, a_2 и b таких, что $a_1 = n_1 b, a_2 = n_2 b$, найти

$$a_3 = (n_1 n_2) b. \tag{2}$$

Эта задача возникает при анализе стойкости известной схемы генерации ключей Диффи–Хеллмана [2].

Пусть $D^*(t, m)$ — минимальное количество битовых операций, необходимых для решения той же задачи при помощи алгоритмов, количество битовых операций в которых удовлетворяет неравенству

$$D^*(t, m) \leq tD^*(C, m),$$

для некоторой абсолютной константы C (например, таких, которые используют только групповую операцию).

Прежде чем сформулировать теорему, сделаем несколько замечаний. Пусть

$$p - 1 = \prod_{i=1}^r p_i^{\alpha_i}.$$

Замечание 1. Маккарли в [3] доказал, что в случае $r = 2$ и $\alpha_1 = \alpha_2 = 1$, количество битовых операций, необходимых для разложения на простые множители числа $p - 1$, есть $O(D(t, p - 1) + \log^2(p - 1))$ и не превосходит

$$D(t, p - 1) \log^2(p - 1),$$

если константу из O так же, как и все абсолютные константы в дальнейшем, считать учтенной в основании логарифма. Принимая во внимание тот факт, что для всех известных алгоритмов разложения на множители этот случай представляется наиболее трудоемким, эта оценка кажется правдоподобной и для $p - 1$, разлагающихся на большее число простых сомножителей.

Замечание 2. Поиск первообразного корня по модулю p можно осуществить следующим образом. Количество первообразных корней по модулю p равно $\varphi(p - 1)$, где φ — функция Эйлера. Поэтому, принимая во внимание известную оценку

$$\varphi(n) \geq C \frac{n}{\log \log n},$$

где C — некоторая абсолютная константа, можно считать эффективной случайную выборку из всех натуральных чисел, не превосходящих $p - 1$, с последующей проверкой выполнения неравенств

$$g^{(p-1)/p_i} \not\equiv 1 \pmod{p}, \quad i = 1, \dots, r. \quad (3)$$

В случае успеха число g является первообразным корнем по модулю p . Количество битовых операций, необходимых для проверки соотношений (3), не превосходит $u(p)\nu(p - 1) \log p$, где $\nu(p - 1)$ — количество различных простых делителей числа $p - 1$, а $u(p)$ — количество битовых операций, необходимых для умножения по модулю p . Несложные вычисления показывают, что, действуя таким способом, за $(\log \log p)u(p)\nu(p - 1) \log p$ битовых операций мы найдем первообразный корень по модулю p с вероятностью $1 - e^{-C} + o(1)$. Повторяя эту процедуру конечное, но большое число раз, получим вероятность, близкую к единице. Кроме того, применяя преобразование Абеля, находим, что

$$\log(2 \cdot 3 \cdot 5 \cdots p_s) = s \log s + o(s \log s),$$

где p_s — s -е простое число, поэтому

$$\nu(p-1) = \nu(P) = O(\log p / \log \log p),$$

где

$$P = \prod_{i=1}^{\nu(p-1)} p_i.$$

Таким образом, первообразный корень по модулю p можно найти за $u(p) \log^2 p$ шагов с вероятностью, близкой к единице.

Оба эти замечания касаются случая несертифицированной задачи дискретного логарифмирования. В случае же сертифицированной задачи разложение $p-1$, p_i-1 , $i=1, \dots, r$, на простые множители, а также первообразные корни по модулям p , p_i , $i=1, \dots, r$, считаются известными.

Пусть

$$m = \prod_{i=1}^r p_i^{\alpha_i}.$$

Рассмотрим разложения на простые множители чисел p_i-1 , $i=1, \dots, r$. Получившееся разветвление назовем деревом числа m , а встречающиеся простые числа его узлами. Обозначим $s = s(m)$ длину наибольшей ветви дерева m .

Теорема 1. Для сертифицированной задачи дискретного логарифмирования

$$L(t, m) \leq s \log^2 m D(\dots D(D(t, m), m) \dots), \quad (4)$$

где справа стоит s -кратная итерация функции $D(t, m)$,

$$L(t, m) \leq s \log^2 m (D^*(C, m))^s. \quad (5)$$

Теорема 2. В случае, если оценка из замечания 1 выполняется для любого простого p , то утверждение теоремы 1 останется верным и без условия сертифицированности, но для вероятностных алгоритмов дискретного логарифмирования.

Подобная оценка с $s=1$, но только для простых p , удовлетворяющих условию гладкости (т.е. $p_i \leq C$, $i=1, \dots, r$, для некоторой абсолютной константы C) была получена в [4] (см. также [5]).

Доказательство теоремы 1. Для простоты рассмотрим сначала случай, когда m — простое число, $m=p$. Без ограничения общности можно считать, что в уравнении (1) $n \not\equiv 0 \pmod{p}$, а b — не единичный элемент группы $G(t, p)$. Введем на множестве элементов $\{nb \mid n \not\equiv 0 \pmod{p}\}$ новую групповую операцию, заданную равенством

$$n_1 b \oplus n_2 b = (n_1 n_2) b.$$

Количество битовых операций, необходимых для выполнения этой операции, равно, очевидно, $D(t, p)$. Так как отличные от нуля вычеты по простому модулю образуют циклическую группу по умножению, мы получаем циклическую группу порядка

$$\varphi(p) = p-1 = \prod_{i=1}^r p_i^{\alpha_i}$$

с аддитивной операцией $\oplus$, где p_i , $i = 1, \dots, r$, — различные простые числа, а $r = \nu(p-1)$. Обозначим эту группу $G(D(t, p), p-1)$. Ясно, что b — единичный элемент этой группы.

Пусть g — первообразный корень по модулю p , тогда gb — образующий группы $G(D(t, p), p-1)$. Эта группа, очевидно, является прямой суммой примарных циклических групп порядка $p_i^{\alpha_i}$ с образующими соответственно $g_i b$, где

$$g_i \equiv g^{(p-1)/p_i^{\alpha_i}} \pmod{p}, \quad i = 1, \dots, r.$$

Пусть $n = g^v \pmod{p}$. Уравнение (1) можно переписать в виде

$$a = \bigoplus_i g_i^{n_i} b = g_1^{n_1} b \oplus \dots \oplus g_r^{n_r} b,$$

где

$$1 \leq n_i \leq p_i^{\alpha_i}, \quad v \equiv \frac{p-1}{p_i^{\alpha_i}} n_i \pmod{p_i^{\alpha_i}}, \quad i = 1, \dots, r,$$

или

$$a = n_1 \cdot (g_1 b) \oplus \dots \oplus n_r \cdot (g_r b),$$

где операция $\cdot$ (операция умножения на натуральные числа элементов группы $G(D(t, p), p-1)$ определена для операции $\oplus$ так же, как для $+$, а именно,

$$n \cdot (kb) = kb \oplus \dots \oplus kb = k^n b,$$

где операция $\oplus$ берется n раз. Заметим, что n при этом можно считать вычетом по модулю $p-1$. Количество битовых операций, необходимых для такого умножения с применением квадратичного алгоритма, очевидно, не превосходит $\log n D(t, p)$. Теперь, чтобы определить число n в выражении (1) будем искать числа n_i , а затем найдем n по формуле

$$n \equiv \prod_{i=1}^r g_i^{n_i} \pmod{p}.$$

Для каждого $i = 1, \dots, r$ с помощью квадратичного алгоритма найдем

$$a_i = \frac{p-1}{p_i^{\alpha_i}} \cdot a = \frac{p-1}{p_i^{\alpha_i}} \cdot n_i \cdot (g_i b).$$

Для этого, очевидно, потребуется не более, чем $\nu(p-1) \log(p-1) D(t, p)$ битовых операций. Еще $\nu(p-1) \log(p-1)(u(p) + t)$ битовых операций необходимо для вычисления g_i , $g_i b$ при известных g и b для всех $i = 1, \dots, r$. Затем, решая задачу дискретного логарифмирования в циклической подгруппе порядка $p_i^{\alpha_i}$ группы $G(D(t, p), p-1)$, порожденной элементом $g_i b$, найдем такое t_i , что

$$a_i = t_i \cdot (g_i b) = g_i b \oplus \dots \oplus g_i b, \quad (6)$$

где операция $\oplus$ берется t_i раз. Для этого потребуется $L(D(t, p), p_i^{\alpha_i})$ битовых операций. Причем, очевидно,

$$n_i \frac{p-1}{p_i^{\alpha_i}} \equiv t_i \pmod{p_i^{\alpha_i}}.$$

С помощью алгоритма Евклида элемент $(p-1)/p_i^{\alpha_i}$ по модулю $p_i^{\alpha_i}$ можно обратить за $u(p) \log p_i^{\alpha_i}$ битовых операций, поэтому количество битовых операций, необходимых для нахождения каждого n_i при известных $a_i, g_i b$, не превосходит

$$L(D(t, p), p_i^{\alpha_i}) + u(p) \log p_i^{\alpha_i}. \quad (7)$$

Уравнение (6) можно решать и по другому, а именно, домножая его на $p_i^{\alpha_i}$, не более, чем за $L(D(t, p), p_i)$ битовых операций, получим t_i по модулю p_i .

Пусть

$$t_i = t_{i0} + p_i t_{i1}, \quad 0 \leq t_{i0} < p_i,$$

тогда

$$a_i = (t_{i0} + p_i t_{i1}) \cdot (g_i b),$$

а так как при перемножении показатели складываются,

$$a_i \oplus (p_i - t_{i0}) \cdot (g_i b) = (t_{i1} + 1) \cdot (g_i^{p_i} b).$$

Число t_{i1} по модулю $p_i^{\alpha_i}$, очевидно, определяется не более, чем за $L(D(t, p), p_i^{\alpha_i})$ битовых операций. Таким образом, в равенстве (7) можно заменить $L(D(t, p), p_i^{\alpha_i})$ на

$$\alpha_i (\log p_i D(t, p) + L(D(t, p), p_i)).$$

Суммируя сказанное, получим следующую рекуррентную формулу для оценки сложности сертифицированной задачи дискретного логарифмирования:

$$L(t, p) \leq D(t, p) \log^2 p + \sum_{p_i^{\alpha_i} \parallel p-1} \alpha_i L(D(t, p), p_i) \quad (8)$$

(считаем, что $D(t, p) \geq \max\{t, u(p)\}$).

Повторяя те же рассуждения с заменой p на p_i и т.д., мы в конечном счете придем к задаче дискретного логарифмирования в группе порядка 2, которая может быть решена перебором.

Утверждение теоремы докажем индукцией по s . Основание индукции очевидно следует из неравенства (8) и тривиальной оценки

$$L(t, p) \leq tp. \quad (9)$$

При рассмотрении шага индукции, воспользуемся неравенством (8) и неравенством (4) с заменой s на $s-1$. Тогда получим, что

$$\begin{aligned} L(t, p) &\leq D(t, p) \log^2 p + \sum_{p_i^{\alpha_i} \parallel p-1} \alpha_i (s-1) \log^2 p_i D(\dots D(D(t, p), p), p) \dots) \\ &\leq D(\dots D(D(t, p), p), p) \dots \left(\log^2 p + (s-1) \log p_i \sum_{p_i^{\alpha_i} \parallel p-1} \alpha_i \log p_i \right) \\ &\leq s \log^2 p D(\dots D(D(t, p), p), p) \dots), \end{aligned}$$

где в формулах стоят s -кратные итерации функции $D(t, p)$, причем считаем, что $D(x, y)$ не убывает по y .

Случай произвольного

$$m = \prod_{i=1}^r q_i^{\alpha_i}$$

сводится к рассмотренному выше умножением равенства (1) на m/q_i и т. д. аналогично приведенному выше решению уравнения (6).

Доказательство неравенства (5) очевидно. Теорема 1 доказана.

Доказательство теоремы 2 очевидным образом следует из оценки (8) и замечания 2.

Отметим, что в качестве $D(x, y)$ в неравенство (4) (или $D^*(t, m)$ в неравенство (5)) может быть подставлена оценка количества битовых операций любого массового алгоритма (т.е. такого, который может быть применен к любой циклической группе простого порядка y с групповой операцией, требующей x битовых операций для своего выполнения).

Для числа s тривиальная оценка $s(m) \leq \log m$ для подстановки в полученные неравенства не подходит, так как при этом, пренебрегая, как и выше, изменением оснований используемых логарифмов, получим оценку

$$L(t, m) \leq (D^*(C, m))^{\log m} \log^3 m = e^{\log(D^*(C, m)) \log m} \log^3 m = m^{\log(D^*(C, m))} \log^3 m.$$

Эта оценка, очевидно, хуже тривиальной оценки (9), где p заменено на m .

Из теоремы Линника (см. [6] с. 411) следует, что для некоторой абсолютной константы C и любого простого числа p наименьшее простое число вида $1 + pn$ не превосходит p^C . Поэтому, существует бесконечная последовательность натуральных чисел m , для которых

$$s(m) \geq \log \log m.$$

При

$$\begin{aligned} s(m) &\leq \alpha(m) \frac{\log m}{\log \log m}, \\ D^*(C, m) &\leq \log m \end{aligned} \quad (10)$$

из оценки (5) получим, что

$$L(t, m) \leq m^{\alpha(m)} \log^3 m, \quad (11)$$

где

$$\frac{\log \log m}{\log m} \ll \alpha(m) \ll \log \log m,$$

что при $\alpha(m) = o(1)$ дает нетривиальную информацию о связи между сложностью задач дискретного логарифмирования и вскрытия схемы Диффи-Хеллмана.

По имеющейся у автора информации, нетривиальными оценками величины $s(m)$ раньше не занимались. Задача выявления классов простых чисел, для которых $\alpha(p) = o(1)$ остается открытой. Отметим также, что простые числа Ферма F_n определяются равенством $s(F_n) = 1$.

В заключение хотелось бы привести несколько соображений мощностного характера, позволяющих получить некоторые оценки вида (10) в среднем.

Рассмотрим рекуррентную последовательность следующего вида

$$p_{i+1} = a_i p_i + 1, \quad 2 \leq a_i \leq A, \quad (12)$$

для некоторой величины $A = A(p_i)$, зависящей от p_i . Пусть p_i — простое число. Будем считать, что простые числа среди всех чисел вида (12) распределены равномерно, а также, что $A(p_i) = o(p_i)$. Тривиальные арифметические преобразования позволяют получить следующую оценку частоты появления простого числа вида (12):

$$\varepsilon(p_i) = \frac{\pi(Ap_i) - \pi(2p_i)}{(A-2)p_i} = O(1/\log p_i),$$

где $\pi(x)$ — количество простых чисел, не превосходящих x . В случае, если эта величина на каком-нибудь шаге оказывается меньше $1/A$, будет естественно предположить, что все числа вида (12) составные. Таким образом, для простоты чисел (12) величина A должна быть как минимум порядка $\log p_i$. Из этих соображений естественно предположить, что при каждой редукции, описанной выше, величина простого числа уменьшается в логарифм от этого числа раз. Не вдаваясь в детали, получим следующую оценку для $s = s(p)$:

$$p/\log^s p = O(1),$$

откуда следует оценка (10), в которой $\alpha(p)$ постоянно.

Обозначим $\pi(x, p, 1)$ количество простых чисел, не превосходящих x , в арифметической прогрессии $1 + pk$, $k \in \mathbb{N}$. Тогда

$$\begin{aligned} \sum_{p \leq m} \nu(p-1) &= \sum_{p \leq m} \pi(m, p, 1) \\ &= (m/\log m + o(m/\log m)) \sum_{p \leq m} \frac{1}{p-1} = \frac{m \log \log m}{\log m} (1 + o(1)). \end{aligned}$$

Можно сделать предположение, что $\nu(p-1)$ растет в среднем как $\log \log p$. Действительно, с помощью преобразования Абеля легко находим, что

$$\sum_{p \leq m} \log \log p = \frac{m \log \log m}{\log m} + O\left(\int_2^m \frac{dt}{\log^2 t}\right) = \frac{m \log \log m}{\log m} (1 + o(1)).$$

Пусть $p = p_1, p_2, \dots, p_s = 2$ — узлы наибольшей ветви дерева p (см. выше). Дальнейшие вычисления произведены в предположении, что для всех p_i

$$\nu(p_i - 1) > \log \log p_i,$$

где логарифмы берутся по некоторому фиксированному основанию, не зависящему от p и i . На каждом шаге редукции величина простого числа p_i уменьшается как минимум в $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots q_{\nu_i} = O(\nu_i^{\nu_i})$ раз, где q_l есть l -е простое число, а $\nu_i = \nu(p_i - 1)$. Поэтому

$$p_2 \leq \frac{p}{e^{f(\log p)}},$$

где

$$f(x) = \log x \log \log x, \quad f(\log p) < (\nu(p-1) - 1) \log(\nu(p-1) - 1),$$

и если

$$p_{i+1} \leq \frac{p}{e^{k_i(p)}}, \quad k_1(p) = (\log \log p) \log \log \log p < \nu(p-1) \log \nu(p-1),$$

то

$$p_{i+2} \leq \frac{p_{i+1}}{e^{f(\log p_{i+1})}} \leq pe^{-k_i(p)-f(\log p-k_i(p))}.$$

Число $s(p)$, очевидно, можно оценить сверху минимальным числом шагов, за которое рекуррентная последовательность

$$k_{i+1}(p) = k_i(p) + f(\log p - k_i(p))$$

приблизится к числу $\log p$. Для простоты будем считать, что $s \leq s_0$, где s_0 — минимальное число, для которого

$$k_{s_0}(p) \geq \log p. \quad (13)$$

Применяя формулу Тейлора при $t = k_i / \log p$, $k_i = k_i(p)$, получим, что

$$\begin{aligned} k_{i+1} &= k_i + f((1-t) \log p) \geq k_i + f(\log p) - f'(\log p)t \log p \\ &= k_i(1 - f'(\log p)) + f(\log p). \end{aligned}$$

Таким образом,

$$\begin{aligned} k_{s_0} &\geq h(p) + g(p)(h(p) + g(p)(\dots)) \\ &= h(p)(1 + g(p) + g^2(p) + \dots + g(p)^{s_0-2}k_1) \\ &\geq h(p)(1 - g^{s_0-1}(p))/(1 - g(p)), \end{aligned}$$

где

$$h(p) = f(\log p), \quad g(p) = 1 - f'(\log p).$$

Неравенство (13), таким образом, будет выполнено, если число s_0 будет удовлетворять неравенству

$$\log \log p \log \log \log p \frac{(1 - (1 - (\log \log \log p + 1)/\log p)^{s_0-1}) \log p}{\log \log \log p + 1} \geq \log p,$$

или

$$1 - \frac{\log \log \log p + 1}{\log \log p \log \log \log p} \geq \left(1 - \frac{\log \log \log p + 1}{\log p}\right)^{s_0-1},$$

откуда

$$\begin{aligned} s_0 &\geq \frac{\log(1 - (\log \log \log p + 1)/(\log \log p \log \log \log p))}{\log(1 - (\log \log \log p + 1)/\log p)} \\ &= \frac{\log p(1 + o(1))}{\log \log p \log \log \log p}. \end{aligned}$$

Взяв минимальное s_0 , удовлетворяющее этому неравенству, получим оценку вида (10) для числа $s(p)$, а значит, и для числа $s(m)$, с

$$\alpha(m) = \frac{1}{\log \log \log m}.$$

Подставляя это равенство в (11), получим, что

$$L(t, m) \leq \exp \left\{ \frac{\log m}{\log \log \log m} \right\}.$$

Список литературы

1. Pomerance C. *Cryptology and Computational Number Theory*. Amer. Math. Soc., Providence, 1990.
2. Diffie W., Hellman M. E. New directions in cryptography. *IEEE Trans. Inform. Theory* (1976) **22**, 644–654.
3. McCurley K. S. A key distribution system equivalent to factoring. *J. Cryptology* (1988) **1**, №2, 95–105.
4. Boer B. Diffie–Hellman is as strong as discrete log for certain primes. *Lect. Notes. Comp. Sci.* (1988) **403**, 530–540.
5. Maurer U. M. Towards the equivalence of breaking the Diffie–Hellman protocol and computing discrete logarithms. *Crypto'94*, 271–281.
6. К. Прахар, *Распределение простых чисел*. Мир, Москва, 1967.

Статья поступила 22.05.95.