Получение верхней оценки на сложность задачи целой факторизации, включающей сложность задачи Диффи-Хеллмэна.

Черепнёв М.А.

Работа частично поддержана грантом РФФИ 17-01-00485а

Аннотация

Построен вероятностный полиномиальный алгоритм, решающий задачу целой факторизации, с оракулом, решающим задачу Диффи-Хеллмэна.

В статье [1] был построен алгоритм, решающий задачу дискретного логарифмирования при помощи оракула, решающего задачу Диффи-Хеллмэна, на элементах той же группы, связанных некоторыми новыми групповыми операциями на основе задачи Диффи-Хеллмэна. По методам решения и оценкам сложности задача целой факторизации обычно бывает близка к задаче дискретного логарифмирования. Поэтому естественно предположить возможность построения нетривиального алгоритма целой факторизации с оракулом, решающим задачу Диффи-Хеллмэна.

Давно известно (см. например [2] теорема 4.7. стр. 148 для чисел RSA), что задача целой факторизации натурального числа n полиномиально с вероятностью эквивалентна задаче нахождения целого M, для которого

$$M \equiv 0 \pmod{L(n)}, \tag{1}$$

где $L(n)$ - функция Кармайкла.

Действительно, если мы предположим, что $n = \prod_{i=1}^{s} q_i^{\beta_i}$ нечетно, а

$$L(n) = \text{НОК}_i[q_i^{\beta_i - 1}(q_i - 1)],$$

$$L(n) \mid M, \qquad L(n) \nmid \frac{M}{2},$$

то наибольший общий делитель $(a^{\frac{M}{2}} - 1 \pmod{n}, n)$ будет нетривиальным если индексы

$$ind_{q_u^{\beta_u}} a, \qquad ind_{q_v^{\beta_v}} a$$

(в этой статье будем изображать порядок рассматриваемой группы, ввиду его громоздкости, в нижнем индексе порядков и индексов элементов, а основанием для индекса всегда будет наименьший первообразный корень по соответствующему модулю) для некоторых $u, v \in \{1, 2, \dots, s\}$ будут иметь разную четность при

$$L(q_u^{\beta_u}) \nmid \frac{M}{2}, \qquad L(q_v^{\beta_v}) \nmid \frac{M}{2},$$

и $ind_{q_u^{\beta_u}} a$ будет нечетным при

$$L(q_u^{\beta_u}) \nmid \frac{M}{2}, \qquad L(q_v^{\beta_v}) \mid \frac{M}{2}.$$

Поскольку оба эти события наступают с вероятностью $\frac{1}{2}$, то это означает наличие алгоритма факторизации, матожидание числа шагов которого полиномиально зависит от длины входа.

При этом указанное M ищется один раз. Таким образом для решения нашей задачи достаточно было бы построить такое M алгоритмом с оракулом Диффи-Хеллмэна.

Однако, M, которое можно построить при помощи применения композиции оракулов Диффи-Хеллмэна, оказывается слишком большим. Поэтому мы поступим несколько иначе.

Выберем некоторое случайное натуральное число a, и пусть $(a,n)=1, ord_n a = l$, тогда $l \mid L(n)$. На циклической группе $< a >_l \subseteq \mathbb{Z}_n^*$ рассмотрим новую групповую операцию

$$a^{\alpha} * a^{\beta} = a^{\alpha\beta} \pmod{n}, \tag{2}$$

требующую для своей реализации решения задачи Диффи-Хеллмэна. Соответствующее количество битовых операций обозначим $D(log^3 n, l)$, где $D(t,l)$ - оценка сверху на количество битовых операций, необходимых для решения задачи Диффи-Хеллмэна в группе порядка l, со сложностью групповой операции, не превосходящей t битовых операций. Будем считать эту функцию неубывающей по l.

Для простоты дальнейших рассуждений будем считать, что $n = pq$, где $p, q > 10$ - взаимнопростые натуральные числа.

Мы будем опираться на следующую элементарную Лемму

Лемма 1 *1. $HOK[L(a), L(b)] = L(HOK[a,b]), \quad a, b \in \mathbb{N}$,*

2. Пусть для некоторого натурального a выполнено $(a,p)=(a,q)=1$, тогда $ord_{HOK[p,q]}a = HOK[ord_p a, ord_q a]$ и делит $ord_n a$.

Равенство

$$a^{m^j} \equiv a \pmod{p} \tag{3}$$

эквивалентно тому, что $(ord_p a, m) = 1$ и $ord_{ord_p a} m \mid j$. По лемме $\text{НОК}[ord_{ord_p a} m, ord_{ord_q a} m] = ord_{ord_{\text{НОК}[p,q]} a} m$, который делит $L(ord_n a)$.

Допустим, что $L(ord_n a) \mid N$ и N известно, тогда чётные (с большой вероятностью) $L(ord_p a), L(ord_q a)$ его также делят. Пусть

$$L(ord_p a) \mid \frac{N}{2}, \qquad L(ord_q a) \nmid \frac{N}{2}. \tag{4}$$

Будем рассматривать только такие m, для которых $(m, ord_n a) = 1$. Тогда по лемме будет выполняться $(m, ord_p a) = (m, ord_q a) = 1$. Тогда $a^{m^{\frac{N}{2}}} \equiv a \pmod{p}$ при любом m взаимнопростом с $ord_p a$, а $a^{m^{\frac{N}{2}}} \not\equiv a \pmod{q}$ тогда и только тогда, когда при $(m, ord_q a) = 1$ выполняется $ord_{ord_q a} m \nmid \frac{N}{2}$, что в данном случае равносильно тому, что степени вхождения двойки удовлетворяют равенству $\gamma_2(ord_{ord_q a} m) = \gamma_2(L(ord_q a))$. При случайном выборе m, такого, что $(m, ord_q a) = 1$, это произойдет с вероятностью не меньше $\frac{1}{2}$, так как для этого достаточно, чтобы индекс элемента $m \in \mathbb{Z}_{ord_q a}^*$, отвечающий примарной компоненте, порядок которой равен степени двойки, был нечетным (если таких примарных компонент в разложении $\mathbb{Z}_{ord_q a}^*$ две, достаточно нечетности одного из индексов). Таким образом с вероятностью не меньше $\frac{1}{2}$ для m, таких, что $(m, ord_n a) = 1$, мы получаем

$$\text{НОД}(a^{m^j} - a, n) = p.$$

Если

$$L(ord_p a) \nmid \frac{N}{2}, \qquad L(ord_q a) \nmid \frac{N}{2}, \tag{5}$$

то при условии случайности и независимости индексов случайного m по модулю $ord_p a$ и $ord_q a$ (напомним, что $(p,q)=1$) с вероятностью не меньше $\frac{1}{16}$ (грубо), мы получим

$$\text{НОД}(a^{m^j} - a, n) \in \{p, q\}. \tag{6}$$

По [4] (теорема 5.1, стр. 32) вероятность того, что $(m, ord_n a) = 1$ при $ord_n a > 2$ не меньше $\frac{c}{\ln\ln ord_n a}$ для некоторой абсолютной константы c. Поэтому общая оценка вероятности будет $O(\frac{1}{\ln\ln ord_n a})$.

При последовательном делении на 2 одно из условий (4, 5) обязательно наступит, о чем будет сигнализировать проверка (6). Таким образом, при известном $L(ord_n a) \geq 2$, его можно применить в качестве N в описанном выше вероятностном алгоритме и разложить n на два взаимнопростых множителя за время, матожидание которого равно

$$O(D(\log^3 n, t) \log L(ord_n a) \ln\ln ord_n a).$$

Аналогично вместо равенства (3) можно работать с равенством

$$a^{b^{\cdot^{\cdot^{\cdot^{c^{d^j}}}}}} = a^{b^{\cdot^{\cdot^{\cdot^{c}}}}} \pmod p, \tag{7}$$

где многоточие скрывает $(t-3)$ возведения в степень и выполняются условия взаимной простоты:

$$(b, ord_n a) = \dots = (d, ord_{\left(\ddots_{ord_{ord_n a} b}\right)} c) = 1. \tag{8}$$

Тогда, если известно $L(ord_{\left(\ddots_{ord_{ord_n a} b}\right)} c) \geq 2$, то сложность задачи разложения n на два взаимнопростых множителя не превосходит $O(\underbrace{D(\dots D(D}_{t}(\log^3 n, n), n)\dots) \log L(ord_{\left(\ddots\right)} c) \ln\ln ord_{\left(\ddots\right)} c)$.

Количество взаимнопростых множителей в разложении n не превосходит $\log n$. Кроме того, для некоторого $k = k(n) \leq \log n$ выполнено $\underbrace{L(L\dots L}_{k}(n)\dots) = 2$. Если выбрать $a = b = \dots = c = d$ простым, большим n, то условия взаимной простоты (8) будут выполнены и для некоторого $t \leq k$ с большой вероятностью число $ord_{\left(\ddots_{ord_{ord_n a} b}\right)} c$ будет больше единицы и будет раскладываться на «маленькие» простые множители (меньше некоторой константы), которые также можно перебрать. Действительно, если $ord_{ord_{\left(\ddots\right)} e} c = 1$, а $ord_{\left(\ddots\right)} e$ не раскладывается на маленькие простые, то $c \equiv 1 \pmod{ord_{\left(\ddots\right)} e}$, вероятность чего мала.

Степени простых чисел можно разложить, извлекая последовательно корни как из вещественного числа с округлением и последующей проверкой, от второй до $\log n$-й степени в совокупности. Таким образом выполнена следующая теорема

Теорема 1 *Сложность задачи разложения n на множители не превосходит* $\log n \log\log n \underbrace{D(\ldots D(D}_{k(n)}(\log^3 n, n), n)\ldots)$.

Замечание 1 *Если обозначить за D^* оценку сверху на число битовых операций для алгоритмов решения задачи Диффи-Хеллмэна, количество битовых операций в которых удовлетворяет неравенству*

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

для некоторой константы C (например таких, которые используют операции не сложнее групповых), то в условиях теоремы сложность задачи разложения n на множители не превосходит $\log^5 n(D^*(C, n))^{k(n)}$.

Заметим также, что использованная здесь функция $k(n)$ удовлетворяет неравенству $k(n) \geq s(n)$ для функции величины наибольшей ветви дерева Пратта $s(n)$, введённой в [1], хотя в среднем, по-видимому, значения этих функций близки.

Список литературы

[1] Черепнёв М.А. О связи сложностей задач дискретного логарифмирования и Диффи-Хеллмэна.// Дискретная математика.-1996.-т.8-вып.3-с.22-30.

[2] Гашков С.Б., Применко Э.А., Черепнёв М.А. Криптографические методы защиты информации. Учебное пособие, «Академия», 2010.-298 с.

[3] Василенко О.Н. Теоретико-числовые алгоритмы в криптографии.-М.:МЦНМО,2006.-325с.

[4] Прахар К. Распределение простых чисел.-М.,Мир,1967.-511с.