О возможности применения одного алгоритма дискретного логарифмирования

Сергей Гребнев

МИЭМ НИУ ВШЭ

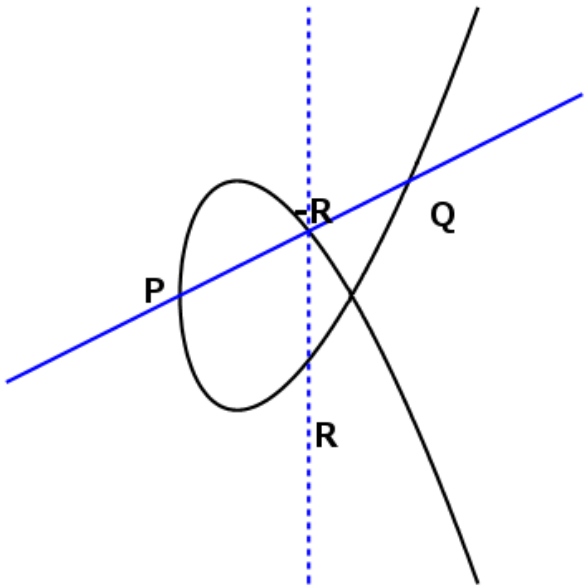
Москва, 21.03.2018

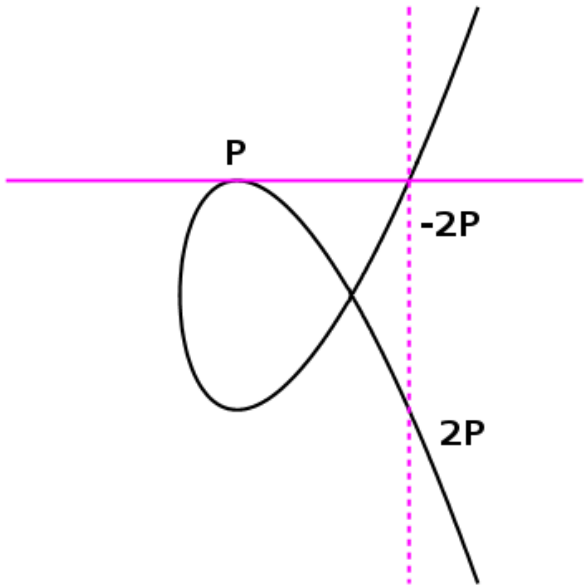
Intro

Пусть эллиптическая кривая E задана над полем $GF(p)$ уравнением

$$y^2 = x^3 + ax + b, \tag{1}$$

Закон сложения





ECDLP

Определим *задачу дискретного логарифирования*: для заданных $P, Q \in E(GF(p))$, найти

$$x : 0 \leq x \leq \#E(GF(p)) \text{ т.ч. } Q = xP, \tag{2}$$

если такой существует.

Вычислительно сложная: ρ-метод Полларда с асимптотической трудоемкостью $O(\#E(GF(p))^{1/2})$

Определяет стойкость многих криптографических приложений.

Алгоритм

CTCrypt'2015: А. Ю. Нестеренко предложил алгоритм, использующий свойства мультипликативной группы по модулю q, где q — простой порядок подгруппы группы точек эллиптической кривой, для ускорения решения задачи дискретного логарифирования в случае, когда x обладает малым ультипликативным порядком по модулю $\#E(GF(p))$.

Мультипликативный порядок и логарифмирование

Пусть $\#E(GF(p)) = q$, где q простое.
Для целого x, взаимно простого с простым числом q, его *порядок* по модулю q равен целому r такому, что

$$x^r \equiv 1 \pmod{q} \quad \text{and} \quad x^l \not\equiv 1 \pmod{q}, \quad \text{для каждого} \quad 1 \leq l < r.$$

Имеем, что $r|(q-1)$. Следовательно, существуют α и n т.ч.

$$\alpha^n \equiv x \pmod{q}, \quad 0 \leq n < r. \tag{3}$$

Имеем $\alpha \equiv g^{\frac{q-1}{r}} \pmod{q}$, где g – первообразный вычет по модулю q.

Используем уравнение (3) и перепишем (2) как

$$\alpha^n P = Q, \tag{4}$$

и, найдя n, определим x.
Положим $h = \lceil \sqrt{r} \rceil$ и запишем n как $n_1 h - n_0$, где $0 \leq n_0 < h$, $0 < n_1 \leq h$. Тогда для (4) имеем

$$(\alpha^h)^{n_1} P = \alpha^{n_0} Q;$$

и теперь методом Хеллмана находим n_0, n_1, а затем n и x.
Требуется не более $2h$ вычислений кратной точки и $O(\sqrt{q})$ ячеек памяти.

Зафиксируем $s = \lceil \log_2 r \rceil$, выберем случайное $\xi_0, \ldots, \xi_{s-1}$ т.ч. $0 < \xi_i < r$, $i = 0, \ldots, s-1$, и определим отображение $f : E \to E$ следующим образом. Для точки $R = (x_R, y_R) \in E$ положим

$$f(R) = \zeta_i R, \quad \text{где} \quad i \equiv x_R \pmod{s}, \quad \zeta_i \equiv a^{\xi_i} \pmod{q}. \tag{5}$$

Можем считать, что f – случайное отображение.

На I этапе алгоритма находим целое β и строим орбиту точки P под действием отображения f, т.е. конечную последовательность

$$R_{k+1} = f(R_k), \quad R_0 = P, \quad k = 0, 1 \ldots, \beta. \tag{6}$$

Имеем, что

$$R_{k+1} = \zeta_k R_k = \zeta_k \zeta_{k-1} R_{k-1} = \cdots = \mu_{k+1} P,$$

где $\mu_{k+1} \equiv \prod_{j=0}^{k} \zeta_j \pmod q$, и ζ_j – псевдослучайные значения, выбранные из (5).
Начиная с индекса k_0, храним множество S точек $R_{k_0+1}, \ldots, R_{k_0+\beta}$ и соответствующие значения $\mu_{k_0+1}, \ldots, \mu_{k_0+\beta}$. Назовем эти точки *выделенными*.

CTCrypt'2015: А.Ю. Нестеренко

На этапе II алгоритма строим орбиту точки $U_0 = \alpha^{\xi} Q$ для случайного ξ т.ч. $0 < \xi < r$, под действием отображения f:

$$U_{k+1} = f(U_k), \quad U_0 = \alpha^{\xi} Q, \quad k = 0, 1, \ldots, \quad 0 < \xi < r. \tag{7}$$

Теперь выполняются следующие соотношения:

$$U_{k+1} = \zeta_k U_k = \zeta_k \zeta_{k-1} U_{k-1} = \cdots = \nu_{k+1} Q,$$

где $\nu_{k+1} \equiv \alpha^{\xi} \prod_{j=0}^{k} \zeta_j \pmod q$.
Теперь для каждой точки U_k проверяем, что $U_k \in S$. Если для индекса j верно, что

$$\mu_j P = P_j = U_k = \nu_k Q,$$

моем заключить, что $\mu_j \equiv \nu_k x \pmod q$, и

$$x \equiv \mu_j \nu_k^{-1} \pmod q.$$

Если среди индексов $k \leq h$ не нашлось выделенной точки, перезапускаем этап II алгоритма с новым случайным значением ξ

Анализ трудоемкости

ρ-метод Полларда:

$$\sqrt{\frac{\pi q}{2\#\mathfrak{G}}}, \tag{8}$$

сложений точек эллиптической кривой; здесь $\mathfrak{G}$ – группа эффективно вычислимых автоморфизмов.
Определим отображение f на классах эквивалентности $E(GF(p))/\mathfrak{G}$ и зафиксируем некоторого представителя класса для хранения выделенной точки.
Тогда для неизвестного x т.ч. $\mathrm{ord}_q x = r$ алгоритм имеет трудоемкость

$$T(x) = \sqrt{\frac{\pi \,\mathrm{ord}_q x}{2\#\mathfrak{G}}} \cdot \log_2 q \tag{9}$$

где множитель $\log_2 q$ is определяется средней трудоемкостью вычисления кратной точки $\alpha^{\xi_i} P$.

Анализ трудоемкости

Предположим, что группа $\mathfrak{G}$ порождена отображением $\psi : P \mapsto -P$, и $\#\mathfrak{G} = 2$ (всегда имеет место для несуперсингулярных, неаномальных кривых Вейерштрасса над $GF(p)$ при $p > 3$, где $1728\frac{4a^3}{4a^3+27b^2} \neq 0, 1728 \pmod p$)
В т.ч. ГОСТ Р 34.10-2012.
Определим среднюю трудоемкость S алгоритма:

$$S = \frac{1}{q-1} \sum_{0<x<q} T(x) \tag{10}$$

Анализ трудоемкости

Отметим, что, поскольку $(q-1)P = -P$, можно считать, что $T(q-1) = 0$.
Перепишем (10) в виде

$$S = \frac{1}{q-1} \sum_{r|\varphi(q)} (\#\{x : \operatorname{ord}_q x = r\}) T(r) = \\ = \frac{\sqrt{\pi} \log_2 q}{2(q-1)} \left(\sum_{r|\varphi(q)} \varphi(r)\sqrt{r} \right) \tag{11}$$

Отметим, что точное значение S в (11) зависит от факторизации $\varphi(q)$:

$$\varphi(q) = q - 1 = r_1^{\alpha_1} \cdot \dots \cdot r_k^{\alpha_k}.$$

Анализ трудоемкости

Однако, можно вычислить нижнюю границу (11). Пусть q простое, что выполнено в большинстве криптографически важных приложений. Рассмотрим сумму

$$\frac{\sqrt{\pi}\log_2 q}{2(q-1)}\left(\sum_{r|\varphi(q)}\varphi(r)\sqrt{r}\right). \tag{12}$$

Для простого q имеем, что $\varphi(q) = q-1$ делится на $(q-1)/2$. Тогда старший член (11), соответствующий $(q-1)/2$, равен

$$\frac{\sqrt{\pi}\log_2 q}{2(q-1)} \cdot \varphi((q-1)/2)\sqrt{(q-1)/2}.$$

Анализ трудоемкости

Для любого целого $l \geq 3$ выполнено неравенство

$$l > \varphi(l) > \frac{\ln 2}{2} \cdot \frac{l}{\ln l}, \tag{13}$$

можно оценить (12) следующим образом:

$$\begin{aligned} \frac{\sqrt{\pi}\log_2 q}{2(q-1)} \cdot \frac{\ln 2}{2} \cdot \frac{(q-1)/2}{\ln(q-1/2)} \cdot \sqrt{(q-1)/2} \geq \\ \geq \frac{\sqrt{\pi}}{4\sqrt{2}} \cdot \frac{\log_2 q}{\log_2(q-1)} \cdot \sqrt{q-1} = O(\sqrt{q}); \end{aligned} \tag{14}$$

и таким образом мы заключаем, что нижняя асимптотическая граница средней трудоемкости алгоритма совпадает с оценкой трудоемкости алгоритма Полларда.

Вывод

Для криптографически важных случаев средняя трудоемкость метода А. Ю. Нестеренко по крайней мере не меньше, чем трудоемкость оригинального метода Полларда.
Алгоритм неприменим для анализа реально используемых криптосистем, в частности, схемы ЦП ГОСТ Р 34.10-2012, где $2^{508} < q < 2^{512}$.