Эллиптические кривые

Лекция 9. Выбор кривой для криптографии

Семён Новосёлов

БФУ им. И. Канта

2023

Как выбрать кривую, подходящую для криптографии?

Требования:

1. Безопасность:
   - для параметра безопасности λ сложность наилучшей известной атаки должна быть $\approx 2^\lambda$
   - на данный момент $\lambda \approx 128$.
2. Эффективность:
   - групповой закон должен вычисляться быстро.

I. Безопасность

$$E/\mathbb{F}_q : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- $N = \#E(\mathbb{F}_q)$, вычисляем с помощью SEA за $O(\log^4 q)$
- $N = O(q)$ (граница Хассе-Вейля)
- $G = \langle P \rangle$ для $P \in E(\mathbb{F}_q)$
- для эффективности: $\#G = \operatorname{ord} P \approx \#E(\mathbb{F}_q)$

DLOG: $Q = [\ell]P, \quad (P, Q) \mapsto \ell$

Каждая известная атака накладывает ограничения по безопасности на (N, q, ℓ).

Атака BSGS или ρ—методом Полларда

Алгоритм BSGS нахождения порядка точки из лекции по подсчёту точек можно адаптировать для поиска **DLOG**.

Сложность: $\widetilde{\mathrm{O}}(\sqrt{\#\mathrm{G}}) = \widetilde{\mathrm{O}}(\sqrt{\mathrm{q}})$ по времени и по памяти.

- ρ-метод Полларда: сложность по памяти $\mathrm{O}(\mathrm{polylog}\,\mathrm{q})$.

Вывод:

- для уровня безопасности $\lambda = 128$ требуется кривая с подгруппой G порядка $\approx 2^{256}$
- т.е. над полем $\mathbb{F}_\mathrm{q}$ размера $\mathrm{q} \approx 2^{256}$

Атака Полига-Хеллмана

Идея: решить задачу DLOG в подгруппах G с помощью ρ-метода Полларда и восстановить искомый DLOG в G по КТО.

$$\#G = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m} \implies G \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_m^{e_m}\mathbb{Z}$$

т.е. $G \simeq G_1 \oplus ... \oplus G_m$, где $\#G_1 = p_1^{e_1}, \ldots, \#G = p_m^{e_m}$.

Сложность: $\widetilde{O}(\sum e_i(\log \#G + \sqrt{p_i}))$

$$\Downarrow$$

Вывод: для безопасности $\#G = cr$, где r – большое простое число, c – малое число.

Комбинируя условия двух атак получаем, что группа точек кривой должна как минимум:

- содержать подгруппу **простого** порядка размера 256-бит для уровня безопасности 128-бит.
- соответственно, размер поля $q \approx 2^{256}$.

Атака спуском Вейля

При $q = p^n$ можно определить ограничение Вейля:

$$W/\mathbb{F}_p := W_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\mathbb{F}_p) = E(\mathbb{F}_{p^n}).$$

- Это абелево многообразие размерности n, т.е. проективное многообразие, обладающее структурой группы.
- Поэтому DLOG на $E/\mathbb{F}_{p^n}$ можно свести к $W/\mathbb{F}_p$.

Если $W \subseteq \mathrm{Jac}_D$ для некоторой кривой $D/\mathbb{F}_p$ рода $g \geq n$, то получаем изменение сложности DLOG:

- $g \geq \log_g p$, D – гиперэллиптическая,

  $$\widetilde{O}(p^{n/2}) \text{ (Pollard) } \Longrightarrow L_{p^g}(1/2, 2.732) \text{ (Enge–Gaudry)}$$

  получаем переход к субэкспоненциальной сложности при $g \approx n$.

- $g < \log_g p$, D – гиперэллиптическая,

  $$\widetilde{O}(p^{n/2}) \text{ (Pollard) } \Longrightarrow \widetilde{O}(p^{2-2/g}) \text{ (GTTD).}$$

  Например, при $n = 8$, $g = 4$ получаем переход от $\widetilde{O}(p^4)$ к $\widetilde{O}(p^{1.5})$.

- Кривая D не всегда существует для кривой $E(\mathbb{F}_{q^n})$ и заданного рода $g \geq n$.
- В общем случае найти кривую D не просто.
- Условия при которых $\exists\, D$ не до конца ясны.

В общем случае, работать с абелевыми многообразиями сложнее, чем с эллиптическими кривыми.

Консервативный выбор размера поля для криптографии с учётом существования атаки спуском Вейля: $q = p$.

Атака с помощью билинейных спариваний

Пусть $r = \#G$, $G \subseteq E(\mathbb{F}_q)$ и $\mu_r = \{x \in \overline{\mathbb{F}}_q | x^r = 1\}$.
Атака использует следующее отображение на $E[r]$.

Теорема (спаривание Вейля)

$\exists$ отображение $e_n : E[r] \times E[r] \to \mu_r$ со свойствами:

1. $e_r(T, T) = 1$
2. $e_r(T, S) = e_r(S, T)^{-1}$
3. $e_r(S_1 + S_2, T) = e_r(S_1, T)e_r(S_2, T)$ *(билинейность)*
   $e_r(S, T_1 + T_2) = e_r(S, T_1)e_r(S, T_2)$
4. $e_r(S, T) = 1, \forall T \implies S = \mathcal{O}$ *(невырожденность)*
   $e_n(S, T) = 1, \forall S \implies T = \mathcal{O}$

Другие билинейные отображения: спаривание Тейта, эта-спаривание.

Степень вложения: минимальное целое k т.ч. $E[r] \subseteq E(\mathbb{F}_{q^k})$.

- Атака на DLOG: $|\langle P \rangle| = r$, $Q = \ell P$.
  1. Выбрать случайную точку R.
  2. $\alpha = e_r(P, R)$
  3. $\beta = e_r(Q, R)$ $\qquad (\beta = e_r(\ell P, R) = e_r(P, R)^\ell = \alpha^\ell)$
  4. $\ell = \mathrm{DLOG}(\alpha, \beta)$ в $\mathbb{F}_{q^k}$
- Конструктивное использование: ZCash, IBE, ~~SIKE~~.

- Сложность решения DLOG в $\mathbb{F}_{q^k}$ используя NFS (и его модификации): $L_{q^k}(1/3, c)$.
- Для уровня безопасности $\lambda = 128$ требуется поле размера 3072-бит [ECRYPT'18].

$$\Downarrow$$

Для стойкости к атаке с помощью билинейных спариваний необходимо: $k \geq 24$ ($3072/128$).

- Т.к. $\mu_r \subseteq \mathbb{F}_{q^k} \iff q^k \equiv 1 \pmod r$. Достаточно проверить, что:

$$r \nmid q^k - 1,$$

для $k = 1, \ldots, 24$.

Аномальные кривые

Кривые с $\#E(\mathbb{F}_p) = p$ называются **аномальными**.

- Если $\#G = p$ для кривой $E/\mathbb{F}_p$, то $\exists$ гомоморфизм $E[p] \to \Omega_E^0(\mathbb{F}_p)$

Здесь $\Omega_E^0(\mathbb{F}_p)$ – $\mathbb{F}_p$-векторное пространство голоморфных дифференциалов, где DLOG решается время $O(\mathrm{polylog}(p))$

- Подробнее: [Galbraith'12, §26.4.1].
- Условия легко проверяются.

Атаки на кривые с автоморфизмами

Существуют модификации методов BSGS или ρ-метода Полларда, использующие автоморфизмы.

- **Идея:** при поиске DLOG перебирать вместо точек P классы эквивалентности $(P, \psi(P), \psi^2(P), \ldots, \psi^{\alpha-1}(P))$ для $\alpha = \operatorname{ord}\psi$.
- **Сложность:** для модифицированного ρ-метода Полларда – $O(\sqrt{\frac{\pi}{2\alpha}}\sqrt{\#G})$ [Galbraith'12, Th. 14.4.3]

- Может быть обобщено на эндоморфизмы, в случае если их можно эффективно вычислить.

Пример кривой:

$$E/\mathbb{F}_p : y^2 = x^3 + a_6,$$

- Автоморфизм: $(x, y) \mapsto (\zeta_3 x, y)$ для $p \equiv 1 \pmod 3$, $\alpha = 3$.
- Эффективная арифметика, т.к. $a_4 = 0$.
- Однако нужно учитывать ускорение DLOG.

Условия безопасности для $\lambda = 128$ относительно основных атак.

$$E/\mathbb{F}_q : y^2 = x^3 + a_4x + a_6$$

1. $r = \# \langle P \rangle \subseteq E(\mathbb{F}_q)$ – простое число, $\#E(\mathbb{F}_q)/r$ – малое число (стойкость к методу Полига-Хеллмана)
2. $r \approx 2^{256}$ (стойкость к ρ-методу Полларда)
3. $q = p$ (стойкость к спуску Вейля)
4. $r \nmid q^k - 1$ для $k \leq 24$ (стойкость к атакам на спариваниях)
5. $r \neq p$ (кривая не аномальная)

Дополнительно

- Параметры кривой должны сопровождаться детальным описанием откуда они взялись.
  - сиды всех псевдослучайных функций
  - выбор псевдослучайных функций / хеш-функций (если $a_4 = hash(seed), a_6 = hash(seed)$)
- Условия только для DLOG, не гарантируется безопасное использование E в протоколах

II. Эффективность

Есть 3 основных формы кривой E.

1. Краткая форма Вейерштрасса:

$$y^2 = x^3 + ax + b$$

2. Кривые Монтгомери:

$$By^2 = x^3 + Ax^2 + x$$

3. Кривые Эдвардса:

$$x^2 + y^2 = 1 + dx^2y^2$$

Сравнение операций

Кривая/Операция	$P + Q$	$2P$
Кривая Вейерштрасса (проект. коорд.)	$12M + 2S$	$5M + 2S$
Кривая Вейерштрасса (коорд. Якоби)	$11M + 5S$	$1M + 8S$
Кривая Эдвардса	$10M + 1S$	$3M + 4S$
Кривая Монтгомери	$6M + 2S$[1]	$4M$

[1] для $2P + Q$

Литература

- D. J. Bernstein и T. Lange. SafeCurves: choosing safe curves for elliptic-curve cryptograph 2020. URL: `https://safecurves.cr.yp.to`.
- H. Cohen и др. Handbook of elliptic and hyperelliptic curve cryptography. 2005.
- S. D. Galbraith. Mathematics of public key cryptography. 2012.

Контакты

snovoselov@kantiana.ru