Лекция #9
Эллиптические кривые для криптографии.

Как выбрать кривую, подходящую для криптографии?

Кривая должна удовлетворять следующим требованиям:

1. Эффективность: закон "+" / "·k" обладает быстрым алгоритмом
2. Безопасность: для заданного параметра безопасности λ, вычисление дискр. логарифма на кривой наиболее быстрым из известных алгоритмов занимает $\sim 2^{\lambda}$ операций. Сегодня $\lambda \sim 128$ бит.

I. Эффективность

(1) Выбор поля $\mathbb{F}_p$: p выбирается большим простым числом с разряженным бинарным представлением. Например $p = 2^{221} - 3$, $p = 2^{251} - 9$. Для p вида $p = 2^n - c$ (небольшое целое) вычисление $\bmod p$ эффективно: Если $z = z_1 2^n + z_0$. Тогда

(z_0 — младшие n бит z)

$$z \bmod p = z_1 \cdot 2^n + z_0 \bmod p \underset{2^n = c+p}{=} z_1(c+p) + z_0 \equiv z_1 c + z_0 \bmod p$$

Т.о. Процедура повторяется для z_1 пока $z_1 \geq p$.

⇒ взятие $\bmod p$ сводится к умножению на c.

Число p выбирается порядка 256 бит для обеспечения ур-ня безопасности в 128 бит. По т-ме Хассе, $\#E(\mathbb{F}_p) \sim O(p)$ ⇒ мы ожидаем найти кривую $E(\mathbb{F}_p)$ с подгруппой простого порядка в 256 бит. Безопасность задачи dlog оценивается (как минимум!) алгоритмом ρ-Полларда, работающего за время $\tilde{O}(\sqrt{p})$.

(2) Выбор кривой $E(\mathbb{F}_p)$:

Существует 3 типа эффективных эл. кривых:

- В короткой форме Вейерштрасса: $E(\mathbb{F}_p): y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0 \bmod p)$
- Кривые Монтгомери E: $By^2 = x^3 + Ax^2 + x$, где $B(A^2-4) \neq 0 \bmod p$

Замена $(x \to Bu - A/3,\ y = Bv)$ переводит кривую Монтгомери в кривую в короткой ф-ме Вейерштрасса $v^2 = u^3 + au + b$ $\left(a = (3-A^2)/(3B^2),\ b = (2A^3 - 9A)/(27B^3)\right)$

• КРИВЫЕ ЭДВАРДА: $E: x^2+y^2 = 1 + d\cdot x^2\cdot y^2$, где $d(1-d) \neq 0 \bmod p$. Замена $(X \to u/v,\ y \to \frac{u-1}{u+1})$ переводит кривую Эдварда в кривую Монтгомери $Bv^2 = u^3 + Au^2 + u$, где $A = 2(1+d)/(1-d)$, $B = 4/(1-d)$

Такие кривые обладают эффективными алг-ми "+", "x2" (= P+P).

	P+Q	2P
– Кривая Вейерштрасса:		
• проект. координаты	12M+2S	5M+2S+1D (=1M)
• координаты Якоби	11M+5S	1M+8S+1D
Если a = -3	— " —	3M+5S
– Кривая Эдварда	10M+1S	3M+4S
– Кривая Монтгомери	?	4M

M – сложность операции "·" в $\mathbb{F}_p$

S – ——— " ——— "+" в $\mathbb{F}_p$

II Безопасность

Выбранная кривая $E(\mathbb{F}_p)$ должна содержать большую подгруппу простого порядка, а именно, p

$m = \#E(\mathbb{F}_p)$ – порядок группы $\mathbb{F}_p$-рац. точек E (вычислен с помощью алг-на Схофа)

$m = n \cdot q$, q – большое простое число.

По Т-ме Хассе $m \sim O(p)$ и если n – мало (например, $n \geq 4$ для кривых Монтгомери), то $q \sim O(p)$ ⇒ мы нашли большую подгруппу порядка q, $G \subseteq E$ $\forall P \neq O$ из этой подгруппы будет образующей G, $\langle P \rangle = G$.

Один из способов задать образующую G: выбрать случайную точку P на E; Возможные порядки $P \in \{q, 2q, \dots, iq, \dots, nq\}$, где $i \mid n$.

Если n – мало, $\langle P \rangle \overset{?}{=} G$ находится эффективно перебором. Для кривой, сгенерированных на стороне, все делители m

Обязательна проверка $ord(P) = q$, $P \in E$.

для заданного ур-ня безопасности λ

① q должен удовлетворять: $\sqrt{\frac{\pi}{4}} \cdot \sqrt{q} > 2^{\lambda}$.

Асимптотически, ρ-метод Полларда: $\mathcal{O}(\sqrt{q})$, более точный анализ: $\sqrt{\frac{\pi}{4} \cdot q}$ (Bernstein-Lange-Schwabe "on the correct use of the negation map in the Pollard rho method")

этот анализ не принимает во внимание параллельную версию ρ-метода (van Oorschot-Wiener)

② Противостояние MOV атаке (Menezes-Okamoto-Vanstone)

задача дискретного логарифма в $G = \langle P \rangle$ в $\mathbb{F}_{p^t}^*$ где $p^t \equiv 1 \bmod q$. Так как dlog в $\mathbb{F}_{p^t}^*$ решается намного быстрее, чем в G (наиболее быстрый алг-м на сегодня: GNFS - тип алг-ма исчисления индексов) Number Field Sieve, то мы требуем, чтобы t было большим. А именно $t \geq \frac{p-1}{\text{const}}$, const - малая константа. t называется степенью вложения кривой.

③ Мы требуем, чтобы $q \neq p$. Кривые, у которых $q = p$, называются аномальными. Задача дискр. логарифма в таких кривых решается за время $O(\text{poly}(\lg p))$ (N. Smart "The discrete log. problem on elliptic curves of trace 1") (q - число $\mathbb{F}_p$-рац. точек)

④ Дискриминант CM-поля ("complex multiplication")

$\#E_p = m = p + 1 - t$, где t - след кривой E, $|t| \leq 2\sqrt{p}$

Пусть s^2 - наибольший квадрат, делящий $t^2 - 4p$.

Тогда $\frac{t^2-4p}{s^2} < 0$ - свободно от квадрата,

Положим $D = \begin{cases} \frac{t^2-4p}{s^2}, & \text{если } \frac{t^2-4p}{s^2} \equiv 1 \bmod 4 \\ \frac{4\cdot(t^2-4p)}{s^2}, & \text{иначе.} \end{cases}$

Если D - мало, существуют методы ускорения ρ-алг-ма Полларда. (Wiener-Zuccherato). Эти же методы используются для ускорения операций "+", "x2". "Faster attacks on Elliptic Curve Cryptosystems"

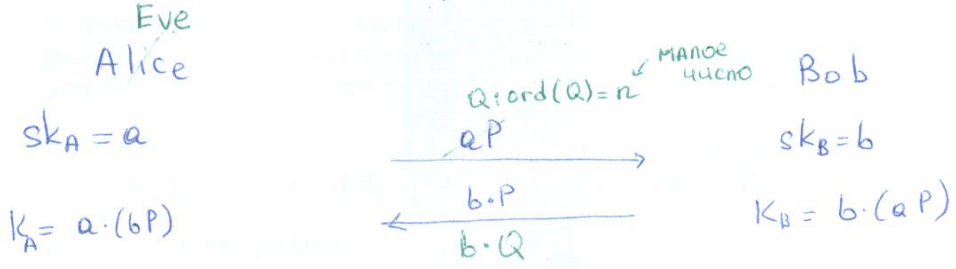
(5) Параметры кривой должны сопровождаться детальным объяснением, откуда они взялись:
- сиды всех псевдослучайных ф-ий
- выбор псевдослуч. ф-ий / хэш ф-ий
(если $a = Hash(seed)$, $b = Hash(seed')$)

Док-во / сертификаты простоты p и q должны быть приложены)

Все выше указанные правила лишь "гарантируют" безопасность (т.е. сложность) задачи dlog на $E(\mathbb{F}_p)$, но не "гарантируют" безопасное использование $E(\mathbb{F}_p)$ в криптогр. протоколах.

Например, в протоколе DH

$$E(\mathbb{F}_p), \quad \langle P \rangle = G$$



$bQ \in \langle Q \rangle$

Т.к. Q имеет малый порядок ($= n$), вычисл. dlg в $\langle Q \rangle$ эффективно: мы вычисляем $b \bmod n$, перебирая n разл. значений.

Более подробно: safecurves.cr.yp.to

Существующие стандарты: (задают модуль p, коэф-ты ур-ия кривой и коор-ты образующей P)
- IEEE P1363 (2000)
- SEC 2 (2000)
- NIST FIPS 186-2 (2000)
- NSA Suite B (2005)

ГОСТ не специфицирует кривую.