ИССЛЕДОВАНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ ИЗ ЗАРУБЕЖНЫХ СТАНДАРТОВ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ГОСТ Р 34.10–2012

С.С. Малахов
НИУ ВШЭ,
департамент прикладной математики
МИЭМ НИУ ВШЭ

Аннотация

Работа отражает исследование некоторых эллиптических кривых из зарубежных стандартов на соответствие требованиям ГОСТ Р 34.10–2012. При этом для рассмотрения были выбраны эллиптические кривые над полем простого порядка, поддерживаемые криптографической библиотекой OpenSSL 1.0.2.

Введение

В настоящее время широкое распространение получили криптографические алгоритмы, стойкость которых основана на сложности задачи дискретного логарифмирования в группе точек эллиптической кривой (например, российский стандарт ГОСТ Р 34.10–2012 [1] на вычисление электронной подписи и его зарубежный аналог ECDSA [2,3]). Интерес к эллиптической криптографии обусловлен тем, что заданный уровень стойкости обеспечивается меньшей битовой длиной ключевой информации по сравнению с алгоритмами, основанными на дискретном логарифмировании в конечном поле или задаче факторизации [4]. На сегодняшний день не известен алгоритм, вычисляющий в общем случае дискретный логарифм в группе точек эллиптической кривой с менее чем экспоненциальной сложностью. Тем не менее, стойкость криптосистем, эксплуатирующих эллиптические кривые, существенно зависит от параметров выбранной кривой. Использование некоторых эллиптических кривых позволяет снизить сложность вычисления дискретного логарифма [3].

Одной криптографической библиотекой, поддерживающей эллиптическую криптографию, является OpenSSL — библиотека с открытым исходным текстом, которая используется во многих программных продуктах, в том числе и российского производства. В частности, в ней реализованы эллиптические кривые, рекомендованные стандартами [2,5,6], которые могут быть использованы для вычисления электронной подписи. По этой причине представляет интерес исследование реализованных эллиптических кривых на соответствие требованиям, накладываемым ГОСТ Р 34.10–2012.

Требования ГОСТ Р 34.10–2012

В соответствии с [1] под эллиптической кривой E над полем $\mathrm{GF}(p)$ простого порядка $p > 3$ в аффинной форме будем понимать множество точек $(x; y) \in \left(\mathrm{GF}(p)\right)^2$, удовлетворяющих уравнению

$$y^2 = x^3 + ax + b (\mathrm{mod}\, p), \quad (1)$$

вместе с бесконечно удаленной точкой O. Здесь $a, b \in \mathrm{GF}(p)$ и $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, p)$. Далее, определим следующие параметры схемы электронной подписи:

– натуральное число m — порядок группы точек эллиптической кривой E;

– простое число q — порядок подгруппы группы точек эллиптической кривой E;

– образующий элемент $P = (x_p; y_p)$ подгруппы группы точек эллиптической кривой, $\mathrm{ord}\, P = q$.

На обозначенные выше параметры в соответствии с ГОСТ Р 34.10–2012 накладываются ограничения:

$$\begin{gathered} p \text{ и } q \text{ простые числа}, q \in (2^{254}, 2^{256}) \cup (2^{508}, 2^{512}); \\ p^t \neq 1 (\mathrm{mod}\, q), t \in \{1, \dots, B\}; \\ B = 31, \text{если } q \in (2^{254}, 2^{256}); \\ B = 131, \text{если } q \in (2^{508}, 2^{512}); \\ m \neq p; \\ J(E) = 1728 \times 4a^3(4a^3 + 27b^2)^{-1} (\mathrm{mod}\, p) \notin \{0{,}1728\}. \end{gathered} \quad (2)$$

Будем говорить, что эллиптическая кривая удовлетворяет требованиям ГОСТ 34.10–2012, если ее параметры, удовлетворяют ограничениям (2), накладываемым на параметры схемы электронной подписи.

Выбор эллиптических кривых для исследования

Покажем, что удовлетворять соотношениям (2) могут только эллиптические кривые, определенные над полями 254–257- или 508–513-разрядного порядка p (в двоичном представлении). Результат теоремы Хассе [7] приводит к следующей оценке числа точек эллиптической кривой:

$$p + 1 - 2\sqrt{p} \leq |E| = m \leq p + 1 + 2\sqrt{p}. \quad (3)$$

Учитывая, что для всех кривых, определенных в стандартах [2,5,6] над простыми полями, порядок подгруппы $\langle P \rangle$ совпадает с порядком группы точек эллиптической кривой, т.е. $m = q$, получим ограничение на простое число p.

$$\begin{gathered} \begin{cases} p + 1 - 2\sqrt{p} \leq q \leq p + 1 + 2\sqrt{p}; \\ \begin{bmatrix} 2^{254} < q < 2^{256}; \\ 2^{508} < q < 2^{512}, \end{bmatrix} \end{cases} \Rightarrow \\ \Rightarrow \begin{cases} p + 1 + 2\sqrt{p} > 2^{254}; \\ p + 1 - 2\sqrt{p} < 2^{256}; \\ 2^{254} < q < 2^{256}, \end{cases} \text{ или } \begin{cases} p + 1 + 2\sqrt{p} > 2^{508}; \\ p + 1 - 2\sqrt{p} < 2^{512}; \\ 2^{508} < q < 2^{512}, \end{cases} \Leftrightarrow \\ \Leftrightarrow \begin{bmatrix} \begin{cases} 2^{254} - 2^{128} + 1 < p < 2^{256} + 2^{129} + 1; \\ 2^{254} < q < 2^{256}; \end{cases} \\ \begin{cases} 2^{508} - 2^{255} + 1 < p < 2^{512} + 2^{257} + 1; \\ 2^{508} < q < 2^{512}. \end{cases} \end{bmatrix} \end{gathered} \quad (4)$$

Итак, среди кривых, приведенных в стандартах [2,5,6], условию (4) удовлетворяют только кривые, определенные над 256- и 512-разрядными простыми полями. Заметим также, что российский стандарт не допускает эксплуатацию эллиптических кривых над составными полями.

Алгоритм проверки эллиптических кривых

Для проверки соответствия эллиптических кривых требованиям ГОСТ Р 34.10–2012 была написана программа в системе компьютерной алгебры Wolfram Mathematica 11.2, реализующая следующий алгоритм.

Шаг 1. Проверить, что число p простое. Если p составное, то перейти на Шаг 9.

Шаг 2. Проверить, что число q простое. Если q составное, то перейти на Шаг 9.

Шаг 3. Проверить, что $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, p)$. Если равенство выполняется, то перейти на Шаг 9.

Шаг 4. Проверить, что точка P принадлежит кривой E. В противном случае перейти на Шаг 9.

Шаг 5. Проверить, что точка $qP = O$. Если равенство не выполняется, то перейти на Шаг 9.

Шаг 6. Проверить, что $q \in (2^{254}, 2^{256}) \cup (2^{508}, 2^{512})$. В противном случае перейти на Шаг 9.

Шаг 7. Проверить, что $p^t \neq 1 (\mathrm{mod}\, q), t \in \{1, \dots, B\}$, где выбор B определен в соотношениях (2). Если равенство выполняется для некоторого t, то перейти на Шаг 9.

Шаг 8. Проверить, что $J(E) \notin \{0{,}1728\}$. Если $J(E)$ принимает значение 0 или 1728, то перейти на Шаг 9.

Шаг 9. Завершить выполнение программы и заключить, что кривая удовлетворяет требованиям ГОСТ Р 34.10–2012.

Шаг 10. Завершить выполнение программы и заключить, что кривая не удовлетворяет требованиям ГОСТ Р 34.10–2012.

Результат проверки эллиптических кривых

Ниже, в таблице 1, приводится перечень исследованных эллиптических кривых и метки их соответствия требованиям ГОСТ Р 34.10–2012.

Таблица 1. Перечень эллиптических кривых и метки их соответствия ГОСТ Р 34.10–2012

Идентификатор кривой	Документ	Метка соответствия
P-256	[2], раздел D.1.2.3	соответствует
Secp256k1	[5], раздел 2.4.1	не соответствует, $J(E) = 0$
Secp256r1	[5], раздел 2.4.1	соответствует
BrainpoolP256r1	[6], раздел 3.4	соответствует
BrainpoolP256t1	[6], раздел 3.4	соответствует, скрученная кривая
BrainpoolP512r1	[6], раздел 3.7	соответствует
BrainpoolP512t1	[6], раздел 3.7	соответствует, скрученная кривая

Под скрученной кривой в таблице 1 понимается следующее ([8]). Пусть найдется значение $u \in \mathrm{GF}(p)\backslash\{0\}$ такое, что $a' = au^{-4}$ и $b' = bu^{-6}$. Тогда эллиптическая кривая $E'\colon y^2 = x^3 + a'x + b' (\mathrm{mod}\, p)$ изоморфна эллиптической кривой E, имеет ту же структуру и порядок. Так определенную кривую E' будем называть скрученной.

Заключение

Итак, данная работа содержит результаты исследования эллиптических кривых, определенных в иностранных стандартах, на соответствие требованиям ГОСТ Р 34.10–2012. Для рассмотрения были выбраны кривые, определенные над полями 256- и 512-разрядного простого порядка и поддерживаемые криптографической библиотекой OpenSSL. Для исследования была разработана программа, реализующая приведенный в работе алгоритм проверки эллиптических кривых.

Список литературы:

1. ГОСТ Р 34.10–2012. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. — Взамен ГОСТ Р 34.10–2001; введ. 2012–08–07. — Москва: Стандартинформ, 2012. — 33 с.

2. National Institute of Standards and Technology (NIST) FIPS PUB 186-4 (Federal Information Processing Standards Publication): Digital Signature Standard (DSS). July. 2013.

3. American National Standard Institute. ANSI X9.62-1998, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm. Sep. 1998.

4. National Institute of Standards and Technology (NIST). NIST Special Publication 800-57: Recommendation for Key Management. Jan. 2016.

5. Standards for Efficient Cryptography — SEC 2: Recommended Elliptic Curve Domain Parameters. Version 2.0. — Certicom Research. Jan. 2010.

6. The Internet Society. RFC 5639 (Request for Comments). Elliptic Cryptography (ECC) Brainpool Standard Curves and Curve Generation. Mar. 2010.

7. Hankerson D., Menezes A., Vanstone S. Guide to elliptic curve cryptography. — New York: Springer-Verlag, 2003.

8. Brier E., Joyce M. Fast Point Multiplication on Elliptic Curves through Isogenies. Applied Algebra Algebraic Algorithms and Error-Correcting Codes // Lecture notes in Computer Science, 2003, Vol. 2643, P. 43–50.