XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V: С.144-145, 2005.

УДК 50.41.00, 50.37.23

Д.П.Рыкованов (4 курс, каф ИБКС), Е.Б.Маховенко, к.т.н., доц.

ВЫБОР ПАРАМЕТРОВ СХЕМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Безопасность российского стандарта электронной цифровой подписи ГОСТ Р 34.10–2001 основана на сложности задачи дискретного логарифмирования на эллиптических кривых над конечными полями. Основными этапами, предусмотренными стандартом, являются: генерация параметров, формирование подписи и проверка подписи. Порядок выполнения первого этапа стандартом не регламентирован. Поэтому для практического применения ГОСТ Р 34.10–2001 необходимо разработать алгоритмы генерации эллиптических кривых.

Случайная эллиптическая кривая $E(\mathbf{F}_p)$ для требуемого поля $\mathbf{F}_p$, полученная с помощью алгоритма Чуфа [1], с большой вероятностью не будет удовлетворять требованиям ГОСТ Р 34.10–2001 к числу точек. Согласно закону распределения простых чисел лишь одно число из $\ln p$ случайных чисел, не превышающих p, будет простым. Поэтому сложность генерации эллиптической кривой алгоритмом Чуфа составляет $O(\log^9 p)$.

Основным недостатком криптосистем на эллиптических кривых является низкая скорость вычислений. Кривые, обладающие комплексным умножением на $\sqrt{-2}$, позволяют ускорить вычисления примерно в 1,6 раза [2]. Поэтому для использования в схеме подписи целесообразно выбирать кривые, обладающие комплексным умножением.

Согласно стандарту, характеристика поля p и порядок группы q должны быть простыми числами. При выборе характеристики поля в виде $p = c^2 + 2d^2$ (кривые над полями такой характеристики обладают указанным комплексным умножением) число точек эллиптической кривой равно $2q$, где $q = p + 1 \pm 2c$. Для удобства вычисления квадратного корня желательно, чтобы выполнялось условие $p \equiv 3 \pmod 4$. Для этого параметры c и d должны удовлетворять сравнениям $c \equiv \pm 1 \pmod 6$, $d \equiv 3 \pmod 6$. Простоту чисел p и q можно проверять алгоритмом Миллера–Рабина [3]. Эллиптические кривые с параметрами p и q, вырабатываемыми предлагаемым алгоритмом, удовлетворяют требованиям стандарта и обладают комплексным умножением на $\sqrt{-2}$. Исходя из перечисленного, алгоритм генерации имеет следующий вид:

1. Выбрать случайное целое число c, $2^{119} \le c < 2^{120}$, такое, что $c \equiv 1 \pmod 6$ или $c \equiv 5 \pmod 6$.
2. Положить $d_1 = (2^{256} - 2^{200} - c^2)/2$.
3. Положить $d = \{$старшие 128 битов числа $d_1\}$.
4. Пока $d \neq 3 \pmod 6$, полагать $d = d + 1$.
5. Положить $p = c^2 + 2d^2$.
6. Если число p составное, то вернуться на шаг 1.
7. Положить $q = (p + 1 + 2 \cdot c)/2$.
8. Если число q простое, то перейти на шаг 10, иначе положить $q = (p + 1 - 2 \cdot c)/2$.
9. Если число q составное, то вернуться на шаг 1.
10. Для $i = 1, 2, \ldots, 31$ проверить, что $p^i \neq 1 \pmod q$. Если хотя бы для одного i неравенство не выполняется, вернуться на шаг 1.
11. Результат: p, q.

В диапазоне характеристик $2^{255} < p < 2^{256}$ существует более чем 10^{70} эллиптических кривых, которые удовлетворяют требованию стандарта ГОСТ Р 34.10–2001 и могут быть выработаны предлагаемым алгоритмом.

ЛИТЕРАТУРА:

1. Schoof R. Counting points on elliptic curves over finite fields // Journal de Théorie des Nombres de Bordeaux. 1995. Vol. 7. P. 219–254.
2. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом. СПб.: Мир и Семья, 2001.
3. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1997.