УДК 681.3.06

И.Д. ГОРБЕНКО,д-р техн. наук, Е.Г. КАЧКО, канд. техн. наук, П.В. КОЛЕСНИКОВ

ГЕНЕРАЦИЯ ПАРАМЕТРОВ И КЛЮЧЕЙ ДЛЯ ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ КОНЕЧНОГО ПРОСТОГО ПОЛЯ

Введение

Криптостойкость цифровых подписей, которые используют модульное возведение в степень, основано на разложении произведения на простые сомножители (RSA) или вычислении дискретного логарифма (DSA, ГОСТ 34.310-95). В связи с достигнутыми успехами в области теории чисел и возрастанием мощности вычислительных систем, а также использованием параллельного программирования, для обеспечения требуемой стойкости таких алгоритмов вынуждены увеличивать длину ключа. Так, для RSA, в пакете PGP уже используются ключи длиной 4096 битов. Увеличение длины ключа не только уменьшает производительность системы при выполнении операций для выработки и проверки цифровой подписи, но и увеличивает размер цифровой подписи. Так как цифровая подпись обычно добавляется к самому документу, это уменьшает полезную пропускную способность канала связи. Поэтому сейчас повсеместно осуществляется переход на новые стандарты цифровой подписи на основе эллиптических кривых, которые позволяют без увеличения длины цифровой подписи достигнуть высокой криптографической стойкости.

В работе [1] на основании чернового стандарта X9.62-1998 [2] был предложен вариант цифровой подписи на эллиптических кривых. При построении этого алгоритма использовался механизм перехода от DSA к ECDSA и параметры действующего стандарта цифровой подписи ГОСТ 34.310–95. Алгоритм, аналогичный предложенному в [1], был принят Госстандартом России в 2001 г. (ГОСТ Р34.10-2001) [3]. В ГОСТ Р34.10-2001 не определена процедура формирования параметров цифровой подписи на эллиптических кривых. Данная работа посвящена описанию этой процедуры с учетом длин ключей, используемых в [1, 3]. Описанную процедуру можно будет использовать не только при выработке – проверке цифровой подписи, но и при реализации алгоритма Диффи – Хеллмана на эллиптических кривых.

Параметры эллиптической кривой

К параметрам эллиптической кривой над простым полем GF(p) относятся следующие параметры[1]:

1. Простое число p – модуль преобразования групп точек эллиптической кривой.
2. Эллиптическая кривая E, задаваемая коэффициентами $a, в \in F_p$[2].
3. Целое число m, определяющее количество точек эллиптической кривой (порядок группы точек).
4. Простое число q, определяющее порядок циклической подгруппы группы точек эллиптической кривой E.
5. Точка P эллиптической кривой E с координатами (x_p, y_p), которая используется в качестве базисной для генерации других точек эллиптической кривой.

[1] При определении параметров использовались обозначения, принятые в. стандарте ГОСТ Р34.10-2001

[2] В стандарте ГОСТ Р34.10-2001 разрешается вместо $a, в$ использовать так называемый инвариант J(E), но так как инвариант легко вычисляется через $a, в$ и наоборот, в дальнейшем будем считать, что эллиптическая кривая задается своими коэффициентами уравнения

Способы формирования параметров

В стандарте **X9.62-1998** [2], в дальнейшем СТАНДАРТЕ, предлагается 3 способа получения параметров эллиптической кривой.

Первый способ состоит в использовании кривых, заданных в СТАНДАРТЕ (прил. J). Анализ готовых кривых показывает, что только одна (самая последняя) эллиптическая кривая удовлетворяет требуемому простому числу. Эта кривая может использоваться только в качестве тестового варианта, поэтому данный способ не пригоден.

Второй способ состоит в случайном выборе эллиптической кривой и проверке ее параметров. Это продолжается до тех пор, пока не будет найдена требуемая кривая. Экспериментальная проверка показала, что поиск эллиптических кривых с требуемым порядком в этом случае может продолжаться очень долго, процесс чисто вероятностный.

Третий способ заключается в выборе требуемых параметров и построении кривой по этим параметрам. Последний способ сразу дает одну или несколько эллиптических кривых с заданным порядком.

В данной работе рассматривается процедура генерации параметров с использованием третьего способа, приводятся рекомендации по ходу выполнения отдельных этапов процедуры.

Выбор простого числа

Простое число p должно удовлетворять неравенству $p>2^{255}$. Верхняя граница этого числа определяется конкретными реализациями. Для получения цифровой подписи длиной 512 бит, как это было для стандарта ГОСТ 34.310-95, число p должно удовлетворять неравенству $p<2^{256}$. В дальнейшем предполагается, что число $2^{255}<p<2^{256}$. Для генерации простого числа можно использовать:

1. Процедуру генерации числа q в стандарте ГОСТ 34.310-95;
2. Генерацию случайного простого числа длиной 256 бит.
3. Генерацию сильного простого числа.

Первый способ не гарантирует 256-битное число. Длина числа может быть 254-256 битов. Наиболее надежным мы считаем третий способ, так как криптографические преобразования, в которых используются сильные простые числа, обладают большей стойкостью.

В контрольном примере к ГОСТ Р 34.1—2001 предлагается простое число p[3]:
57896044618658097711785492504343953926
634992332820282019728792003956564821041

Вычисление параметров кривой

Определяется минимальное значение порядка эллиптической кривой (число m_{min}). В соответствии с рекомендациями СТАНДАРТА, для обеспечения требуемого уровня безопасности по отношению к проблеме дискретного логарифма, m_{min} должно удовлетворять неравенству:

$$m_{min} > 2^{200}. \qquad (1)$$

При заданном значении p

$$mmin \le (p+1-2\sqrt{p}) \qquad (2)$$

Проверим, что значение m_{min}, вычисляемое по формуле $m_{min} = (p-2\sqrt{p})$ удовлетворяет формулам (1) и (2). Так как $p>2^{255}$ то $m_{min}>2^{254}$, т.е. условие (1) выполняется с запасом. Выполнимость условия (2) очевидна.

---

[3] Все числа в данной статье представляются в 10-ой системе счисления, начиная со старшей цифры

Для контрольного примера к стандарту ГОСТ Р 34.1—2001 получаем значение m_{min}, равное

m_{min}=57896044618658097711785492504343953926

153760394484272996638724459001314707187.

Известно, что порядок эллиптической кривой m зависит от размера поля, определяемого простым числом p, и удовлетворяет неравенству:

$$p+1-2\sqrt{p} \le m \le p+1+2\sqrt{p}. \qquad (3)$$

Из формулы (3) следует, что $4p-(p+1-m)^2 \ge 0$, целое. Обозначим это значение через Z. Любое положительное целое число может быть представлено как произведение сомножителей, которые встречаются четное и нечетное число раз. Тогда $Z = D * V^2$, где D - произведение сомножителей, не содержащих квадратов. Значение D называется дискриминантом эллиптической кривой.

С учетом (3) параметры эллиптической кривой связаны соотношениями:

$$\begin{aligned} m &= p+1 \pm W, \\ 4p &= W^2 + D*V^2, \end{aligned} \qquad (4)$$

где $W = \sqrt{p} + 1$.

Задача состоит в решении системы уравнений (4) относительно неизвестных m, V и D при заданном значении p. Так как в системе (4) два уравнения и три неизвестных, для ее решения выбирается значение дискриминанта D, требования к которому определены ниже. Как показывает практика, решения системы могут быть найдены при небольших значениях D.

Требования к выбору дискриминанта *D*

Кроме того, что D - положительное и не содержит квадратов, оно должно обладать следующими свойствами:

1.

$$D = \begin{cases} 2,3,7 \bmod 8, & \text{если } p \equiv 3 \bmod 8, \\ \text{нечетное, если } p \equiv 5 \bmod 8, \\ 3,6,7 \bmod 8, \text{если } p \equiv 7 \bmod 8, \\ 3 \bmod 8, \text{если } K = 1, \\ \neq 7 \bmod 8, \text{если } K = 2,3. \end{cases}, \qquad (5)$$

Здесь переменная K определяет отношение между максимально и минимально возможным порядком кривой и определяется по формуле:

$$K = \frac{W^2}{m_{min}}. \qquad (6)$$

При рассмотренных выше значениях W, m_{min} значение K всегда равно 1 и формула (5) для проверки дискриминанта превращается в:

$$D = 3 \bmod 8, \qquad (7)$$

т.е. в качестве дискриминанта можно использовать значения: 3,11,19,27,...

2. Должен существовать корень:

$$\left(\overline{(-D)}\right) mod\ P, \qquad (8)$$

т.е. символ Якоби для *P-D* и *P* должен быть равен 1.

Для контрольного примера, минимальное значение D, удовлетворяющее (7) и (8) равно 915.

Чем меньше число *D*, используемое для построения эллиптической кривой, тем быстрее эта кривая может быть построена. В работе выполнено исследование возможности построения эллиптических кривых для первых 1000 простых чисел длиной 256 бит. Если для данного простого числа не удавалось построить эллиптическую кривую при значении дискриминанта меньше 1000, такое простое число отвергалось. Как показали исследования, при максимальном значении дискриминанта, равном 995, найдено 114 эллиптических кривых, из них 15 эллиптических кривых вырождено, т.к. имеют коэффициент $a = 0$. Проверялись различные выборки простых чисел, характер зависимости количества эллиптических кривых от значения дискриминанта в этом случае не изменяется. Авторы считают, что достаточно использовать дискриминанты до 1000.

Рассмотрим построение кривой по заданным значениям размера поля *p*, порядка кривой *u*, ее дискриминанта *D* и значений констант *V, W*.

Значению дискриминанта D соответствует матрица: $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$, для которой *D* - определитель.

Элементы матрицы *A, B, C* должны обладать свойствам:

A, B, C - целые;

$$íîä\ (A,\ 2*B,\ C) = 1. \qquad (9)$$

Если $A=|2*B|$ или $A = C$, то $B \geq 0$.

Таблица 1

Диапазон значений дискриминанта	Значение дискриминанта		Количество матриц	
	Минимум	Максимум	Минимум	Максимум
0..99	3	59	3	9
100..199	163	131	3	15
200..299	235	299	6	24
300..399	307	371	9	24
400..499	403	419	6	27
500..599	547	563	9	27
600..699	643	659	9	33
700..799	715	731	12	36
800..899	883	899	9	42
900..999	907	971	9	45
1000..1099	1003	1091	12	51
1100..1199	1123	1139	15	48
1200..1299	1227	1259	12	45
1300..1399	1387	1379	12	48
1400..1499	1411	1427	12	45
1500..1599	1507	1571	12	51
1600..1699	1603	1691	18	54
1700..1799	1723	1739	15	60
1800..1899	1867	1811	15	69
1900..1999	1915	1979	18	69

Эти свойства обеспечивают положительность *D* и отсутствие в его разложении сомножителей с четным показателем.

Одному значению определителя соответствует группа матриц, причем, если ему соответствует матрица *(A, B, C)* при $B \neq 0$, то определителю соответствует матрица *(A, -B, C)*. Все матрицы, соответствующие данному значению определителя, образуют группу, которой

может быть поставлен в соответствие полином, степень полинома равна количеству матриц, а коэффициенты определяются по самим матрицам и являются целыми числами по модулю *D*. Зависимость количества матриц от значения дискриминанта D, удовлетворяющего (7), представлено в таблице 1. Количество матриц и сами матрицы определяются по алгоритму Е2.2 СТАНДАРТА.

Как следует из таблицы, количество матриц растет при увеличении значения дискриминанта. В соответствии с таблицей можно подобрать значение дискриминанта из любого из приведенных диапазонов, при котором количество матриц минимально. Почему необходимо стремиться к небольшому числу матриц? Чем меньше количество матриц, тем меньше порядок образующего полинома, тем быстрее его можно разложить на множители для выделения уравнения третьего порядка для эллиптической кривой, т.е. далее полином должен быть разложен на полиномы третьей степени.

Значение дискриминанта D используется для определения порядка базовой точки эллиптической кривой. Для определения порядка m используется алгоритм Е.3.2.с СТАНДАРТА. Для контрольного примера получаем значение порядка m, удовлетворяющего $m > m_{min}$:

m= 57896044618658097711785492504343953927082934583725450622380973592137631069619.

Построение и разложение полинома

Для построения полинома по заданным коэффициентам матриц (Ai, Bi, Ci) используется алгоритм Е2.3 СТАНДАРТА.

Для контрольного примера получаем полином порядка 24:

x^24 - 72114*x^23 + 2126408*x^22 - 5895642*x^21 - 5532022*x^20 - 60792018*x^19 - 70125360*x^18 + 97965798*x^17 + 35668303*x^16 - 72288692*x^15 + 129495040*x^14 - 78718468*x^13 + 30977772*x^12 + 72917852*x^11 - 15938320*x^10 - 29367412*x^9 + 51609743*x^8 - 23991322*x^7 + 10115960*x^6 - 3523618*x^5 + 2550698*x^4 - 669962*x^3 + 73088*x^2 - 114*x + 1.

Для получения параметров уравнения эллиптической кривой строятся их начальные значения, которые определяются из разложения полинома, полученного на предыдущем шаге на множители, в их числе множитель с полиномом степени 3. Один и тот же полином может иметь несколько сомножителей требуемого порядка, например, если количество матриц 6, то может быть 2 полинома, при числе матриц 24 может быть до 8 полиномов третьего порядка, т.е по одному полиному можно построить сразу несколько эллиптических кривых, имеющих одинаковые модули и порядки базовой точки. Для разложения полинома на множители используется постепенное выделение сомножителя третьего порядка по алгоритму Е1.4 СТАНДАРТА.

В результате факторизации для контрольного примера получаем такой трехчлен:

x^3 + 28122443055414125650524061560182863399889457803909307045456633293834119814058*x^2 - 1115785347824070460927661595348732319109250450282595459175303778348205830367 3*x – 1.

Для полученного полинома третьей степени строится эллиптическая кривая, которая имеет заданное значение дискриминанта D, но пока не гарантируется ее порядок. Значения коэффициентов a_0, b_0 такой кривой определяется по алгоритму Е.3.4.1. Для контрольного примера

A0=40418041243272845574322042644730969642132756176440874349302870804884135919179,
B0=34699716189756471699896117326078024952181449703850381273077498683297306383262.

По полученным начальным значениям a_0, b_0 формируются значения коэффициентов эллиптической кривой a, b. При формировании коэффициентов используется алгоритм, описанный в Е3.4.2 СТАНДАРТА. На этом же шаге получаем базовую точку эллиптической кривой с заданным значением порядка.

Для контрольного примера коэффициенты эллиптической кривой равны:

$$a = 7,$$

$$b = 43308876546767276905765904595650931995$$

$$942111794451039583252968842033849580414.$$

Порядок циклической подгруппы группы точек эллиптической кривой равен

$$q = 57896044618658097711785492504343953927082934583725450622380973592137631069619.$$

Заключение

В работе приведен практический алгоритм формирования параметров эллиптической кривой для схемы электронной цифровой подписи в соответствии с [1, 2]. Для иллюстрации достоверности приведенного алгоритма используется контрольный пример из [2]. В статье приведены промежуточные данные при выполнении каждого шага алгоритма, что существенно упрощает практическую реализацию вычислений параметров.

Список литературы: 1. *ГОСТ 34.310 – 95* Стандарт цифровой подписи на эллиптических кривых. 2. X9.62-1998 [2]. Public Key Cryptography For The Financial Services Industry. Public Key Cryptography For The Financial Services Industry 3. *ГОСТ Р34.10-2001.* Информационная технология. Криптографическая защита информации. Процессы формирования и проверки цифровой подписи// Госстандарт России, М.: 2001.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 30.04.2002