1 Электронная подпись Эль Гамаля с возвратом сообщения – схема Nyberg-Rueppel

Проверки цифровой подписи *с возвратом сообщения* основана на возможности извлечения «отпечатка» $h(m)$ сообщения m из цифровой подписи $\mathrm{Sign}(m,k)$, полученной на ключе подписи k, и состоит в проверке условия

$$h'(m) = h(m'),$$

где m' сообщение, подпись под которым проверяется, а $h'(m)$ – хеш-значение подписанного сообщения, извлеченное из цифровой подписи $\mathrm{Sign}(h(m),k)$ на заданном ключе проверки $k',\ k' \in K'$.

Пусть $\mathcal{E}(F)$ группа точек эллиптической кривой, P – базовая точка открытого ключа, N – порядок этой точки, k – секретный ключ подписывающего документ участника. Открытым ключом последнего является точка

$$Q = kP. \tag{1}$$

Пусть $e = h(m)$ - значение хеш-функции h для документа m.

Алгоритм генерации подписи следующий.

1) Взять случайное число $r,\ 0 < r < N$, такое, что x-компонента точки

$$R = rP = (x,y) \tag{2}$$

не равна 0.

2) Используя x-компоненту точки R как целое число, вычислить

$$c = (x+e) \bmod N, \tag{3}$$

$$d = (r - kc) \bmod N. \tag{4}$$

Если $c = 0$ или $d = 0$, то вернуться к шагу 1.

Пара (c,d) является подписью для документа m, такого, что $h(m) = e$.

Для проверки, что $h(m)$ является корректным хеш-значением, выполняются следующие действия.

1) Проверить, что $1 < c < N-1,\ 1 < d < N-1$.

2) Вычислить

$$R' = dP + cQ. \tag{5}$$

3) Интерпретируя x-компоненту точки R' как двоичную запись целого числа, вычислить

$$e' = (c - x') \bmod n. \tag{6}$$

3) Если полученное значение e' совпадает с хеш-значением $h(m')$, вычисленным для полученного сообщения m', то последнее удостоверяется.

Поясним этот протокол следующим примером (при заведомо малых значениях параметров).

Пример 1.1 Выберем несуперсингулярную кривую $Y^2 + XY = X^3 + X^2 + 1$ над полем $GF(2^5) = GF(2)(\lambda)$, где λ – корень неприводимого многочлена $1 + X^2 + X^5$, и базовую точку $P = (00101, 10110)$ этой кривой. Непосредственной проверкой убедимся, что порядок N этой точки равен 22. Пусть значение хеш-функции[1]сообщения m есть $e = h(m) = (1011) = 13$. Допустим, что секретным ключом является двоичный код $k = (111) = 7$, тогда открытым ключом является точка

$$Q = kP = 7(00101, 10110) = (10011, 10111).$$

Для получения подписи сначала базовая точка P умножается на случайно выбираемый рандомизатор r, пусть $r = 5$, и получается точка

$$R = 5P = (10111, 11011);$$

x-компонента (10111)=29 этой точки R также является случайным числом.

Прибавление по формуле (3) этой точки к хеш-значению $e = h(m) = 13$ по модулю $N = 22$ (порядка точки P) эффективно маскирует это хеш-значение,в результате получается первое число кода цифровой подписи

$$c = (x + e) \bmod N = 29 + 13 \bmod 22 = 20.$$

Второе число d кода цифровой подписи получается по (4) с использованием секретного ключа k :

$$d = (r - kc) \bmod N = (5 - 7 \cdot 20) \bmod 22 = 19.$$

Цифровая подпись под значением $e = h(m)$ на ключе подписи $k = 7$ есть пара чисел $(c, d) = (20, 19)$.

[1]Элементы двоичных кодов располагаются в порядке возрастания степеней или весовых эквивалентов

Этап проверки подписи по (5) позволяет восстановить точку R и, следом, по (6) получить замаскированное хеш-значение e : Если подпись корректна, то получится $R' = R$:

$$R' = dP + cQ = dP + ckP = (d + ck)P == (r - ck + ck)P = rP = R.$$

В нашем примере $R' == dP + cQ =$

$$= 19(00101, 1011) + 20(10011, 10111) = (10111, 11011) = R.$$

Используя x-координату $x' = (10111 = 29)$ точки R, восстановим хеш-значение

$$e' = c - x' = 20 - 29 \bmod 22 = 13.$$

Если это восстановленное значение e' совпадает с хеш-значением $h(m')$, вычисленным по полученному сообщению m', то можно считать, что последнее мог подписать только обладатель секретного ключа s и что ни сообщение, ни его хеш-значение не было изменено активным криптоаналитиком или вследствие ошибок при передаче или хранении.

Заметим, что при проверке подписи операции умножения модульной арифметики не используются.

2 Особенности российского стандарта цифровой подписи с возвратом сообщения

В российском стандарте цифровой подписи с возвратом сообщения используется другая схема генерации и проверки подписи:

Цифровой подписью под сообщением m со значением хеш-функции $e = h(m)$ на ключе подписи k является пара чисел (c, d), где c есть отличное от нуля число, определяемое x-координатой точки $R = rP$, а число d вычисляется как

$$d = (xk + re) \bmod N.$$

Для проверки цифровой подписи восстанавливают точку R, используя операции арифметики эллиптической кривой и модульной арифметики:

$$R' = z_1 P + z_2 Q, \tag{7}$$

где

$$z_1 = d\nu \bmod N,\ z_2 = -c\nu \bmod N$$

при $\nu = e^{-1} \bmod N$.

В этом случае на этапе проверки цифровой подписи приходится выполнять операции умножения и мультипликативного обращения в группе Z_N^*. Порядок N базовой точки P в данном случае есть простое число.

Пример 2.1 Возьмем базовую точку $P = (0001, 11111)$ той же кривой, что и в предыдущем примере и образуем цифровую подпись под сообщением m с хеш-значением $e = h(m) = 2$, (то же, что и в предыдущем примере, но приведенное по модулю $N = 11$) на том же ключе подписи $k = 7$ и с тем же рандомизатором $r = 5$. Порядок N точки P есть простое число 11.

Точка ключа проверки есть $Q = kP = 7(0001, 11111) = (01111, 10101)$ «Точка возврата» есть $R = rP = 5(0001, 11111) = (0101, 01001)$.

Первое число цифровой подписи $c = (0101)_2 = (10)_{10}$,

Второе число цифровой подписи $d = (ck + re) \mod N = (10 \cdot 7 + 5 \cdot 2) \bmod 11 = 3$.

Цифровая подпись есть пара чисел $(c, d) = (10, 3)$

Для проверки цифровой подписи вычислим

$\nu = e^{-1} \bmod N = 2^{-1} \bmod 11 = 6$,

$z_1 = d\nu \bmod N = 3 \cdot 6 \bmod 11 = 7$,

$z_2 = -c\nu \bmod N = -10 \cdot 6 \bmod 11 = 6$.

Восстановленная точка возврата вычисляется в соответствии с (7):
$R' = z_1P + z_2Q = 7(0001, 11111) + 6(01111, 10101) = (01111, 10101) + (11001, 10101) = (0101, 01001) = (x', y')$. Как видим, $x' = c$.

3 Контрольные вопросы

1. В чем особенность цифровой подписи с возвратом сообщения?

2. Опишите алгоритм формирования цифровой подписи с возвратом сообщения и алгоритм ее проверки.

3. Чем отличается алгоритм российского стандарта цифровой подписи с возвратом сообщения?