Анализ слепых цифровых подписей на основе дискретного логарифмирования

**Фаль Алексей Михайлович,
ведущий научный сотрудник**

**Институт кибернетики им. В.М. Глушкова
НАН Украины**

В 1994 г. в работе [1] были предложены два алгоритма слепой подписи, использующие проблему нахождения дискретных логарифмов. Первый из них в качестве основной схемы цифровой подписи использовал схему, фактически равнозначную схеме российского стандарта Р 34.10-95. Вторым алгоритмом в качестве основной схемы использовалась цифровая подпись, предложенная в [2] Nyberg и Rueppel.

Для полноты приведем алгоритм, предложенный в работе [1]. Напомним, что общесистемными параметрами является простое число p , делитель q , также являющийся простым числом и элемент порядка r . Секретным ключом подписывающего является случайный элемент x , а соответствующим открытым ключом есть y .

Протокол создания слепой подписи

сообщения $m \in Z_q$ состоит в следующем.

1. а) Подписывающий выбирает случайное $\tilde{k} \in Z_q$ и вычисляет $\tilde{R} = g^{\tilde{k}} \pmod{p}$

б) Подписывающий проверяет условие $(\tilde{R}, q) = 1$. В случае неудачи возвращается к а). В противном случае, он отправляет $\tilde{R}$ заказчику.

2. а) Заказчик проверяет, что $(\tilde{R}, q) = 1$
- б) Заказчик выбирает случайные $\alpha, \beta \in Z_q$
и вычисляет $R = \tilde{R}^\alpha g^\beta \pmod{p}$
- в) Заказчик проверяет, что $(\tilde{R}, q) = 1$.
Если неудача, то возвращается к б). В
противном случае, он вычисляет
 $\tilde{m} = \alpha m \tilde{R} R^{-1} \pmod{q}$ и отправляет $\tilde{m}$
подписывающему

3. Подписывающий вычисляет

$$\tilde{S} = (\tilde{k}\tilde{m} + \tilde{R}x) \pmod{q}$$

и отправляет $\tilde{S}$ заказчику.

4. Заказчик вычисляет $S = (\tilde{S}R\tilde{R}^{-1} + \beta m) \pmod{q}$
и $r = R \pmod{q}$.

Пара (r, s) является значением цифровой подписи сообщения m .

Для проверки подписи вычисляют

$$T = (g^s y^{-r})^{m^{-1}} \bmod p .$$

Подпись является верной, если выполняется условие $T \bmod q = r$.

Перенесем данный алгоритм на случай эллиптических кривых, изложенный в стандарте Р 34.10-2000

Изложим алгоритм этого стандарта в виде, в котором он представлен в ISO/IEC 14888-3:2006, Amedment 1.

Общесистемные параметры.

p - простое число

E - группа точек эллиптической кривой
над полем $GF(p)$

$\#E$ - к-во точек на E

q - простой делитель $\#E$

G - точка эллиптической кривой порядка q

Выбранная хэш-функция в отличие от
российского стандарта

Генерирование секретного и открытого ключей

Секретным ключом является случайно сгенерированное число X , $0 < X < q$.

Соответствующим открытым ключом является точка $Y = [X]G$.

Процесс подписывания

Подписывающий выбирает случайное K ,
 $0 < K < q$ и вычисляет $\Pi = [K]G$.

Далее вычисляется число $R = FE2I(\Pi_x) \bmod q$, где
 Π_x - x -вая координата точки Π .

Вычисляется $h(M)$ и хэш-код преобразуют в
целое число H . Подписью является пара

чисел (R, S) , где S вычисляется по формуле

$$S = (RX + KH) \pmod{q}$$

Процесс проверки подписи

Вычисляют $\bar{\Pi} = \left[-H^{-1}R \bmod q \right] Y + \left[H^{-1}S \bmod q \right] G$

$$\bar{R} = FE2I(\bar{\Pi}_x)$$

Подпись верна, если $\bar{R} = R$

Протокол создания слепой подписи, соответствующий стандарту Р 34.10-2001

1. Подписывающий выбирает случайное $\tilde{K} \in Z_q$ и вычисляет

$$\tilde{\Pi} = [\tilde{K}]G \text{ и отправляет } \tilde{\Pi} \text{ заказчику.}$$

2. Заказчик выбирает случайные $\alpha, \beta \in Z_q$ и вычисляет

$$\Pi = [\alpha]\Pi + [\beta]G. \text{ Далее вычисляется } \tilde{R} = FE2I(\tilde{\Pi}_x) \bmod q \text{ и } R = FE2I(\Pi_x) \bmod q \text{ и } \tilde{H} = \alpha H \tilde{R} R^{-1} \pmod{q}. \tilde{H} \text{ отправляется подписывающему.}$$

3. Подписывающий вычисляет $\tilde{S} = (\tilde{K}\tilde{H} + \tilde{R}X) \pmod{q}$ и отправляет $\tilde{S}$ заказчику.

4. Заказчик вычисляет $S = (\tilde{S}R\tilde{R}^{-1} + \beta H) \pmod{q}$.

Подписью является пара чисел (R, S)

Процесс проверки подписи

Вычисляем

$$\begin{aligned}\bar{\Pi} &= \left[-H^{-1}R \bmod q \right] Y + \left[H^{-1}S \right] G = \left[-H^{-1}RX + H^{-1}\tilde{S}R\tilde{R}^{-1} + \beta \right] G = \\ &= \left[-H^{-1}RX + H^{-1}\tilde{K}\tilde{H}R\tilde{R}^{-1} + H^{-1}RX + \beta \right] G = \left[\alpha\tilde{K} + \beta \right] G = \Pi\end{aligned}$$

Подпись верна, если $\bar{R} = FE2I(\bar{I}_x) \bmod q$

совпадает с R .

Литература

- 1. J.A. Camenish, J-M Piveteau, M.A. Stadler Blind Signatures Based on the Discrete Logarithm Problem // Eurocrypt – 1994**
- 2. K.Nyberg, R.A. Rueppel. A New Signature Scheme Based on the DSA Giving Message Recovery // 1st ACM conf. on computer and commun. security**