XXXIII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V: С.141-142, 2005.

УДК 50.41.00, 50.37.23

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

ЗАЩИЩЕННЫЙ ПРОТОКОЛ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Прокол электронной цифровой подписи, регламентированный российским стандартом ГОСТ Р 34.10–2001, а также стандартом США ECDSS, использует эллиптические кривые над конечными полями. При формировании подписи выполняются следующие действия:

1) вычисляется значение e, $0 < e < r$, — хэш-образ подписываемого сообщения m;
2) вырабатывается случайный показатель k, $0 < k < r$;
3) вычисляется точка эллиптической кривой: $R \leftarrow kQ$, $R = (x_R, y_R)$, причем $x_R \neq 0 \pmod r$;
4) вычисляется значение $s \leftarrow (l \cdot x_R + k \cdot e) \pmod r$, причем $s \neq 0$.

Таким образом, подписанное сообщение представляет собой тройку $(m, x_R \pmod r, s)$, где число r и точка Q – параметры схемы подписи, число l – ключ подписи.

Предположим, что нарушитель может измерять слабые сигналы, возникающие при формировании подписи, и использовать их для вскрытия ключа. Такие атаки («side channel attack») известны с 1950-х годов. Основаны они на анализе электромагнитных и акустических полей, потребляемой мощности, длительности выполнения операций и т.п. Потенциально уязвимыми являются сигналы, появляющиеся при формировании подписи на шаге 4 при умножении ключа на число x_R.

Для защиты протокола от такого рода атак при первом вычислении электронной цифровой подписи вместо постоянного ключа l можно использовать «замаскированное» значение $k_1^{-1}l \pmod r$, где k_1 — случайное число, обратимое по модулю r [1]. Преобразуем уравнение формирования подписи шага 4 с учетом наложения и снятия «маски». Получим

$$s \equiv k_1(k_1^{-1}lx_R + e) \pmod r, \qquad (1a)$$

причем показатель s не зависит от наложения и снятия «маски» $(k_1^{-1}) \pmod r$:

$$s \equiv (k_1k_1^{-1}lx_R + k_1e) \equiv (lx_R + k_1e) \pmod r.$$

Для формирования первой подписи отправитель вычисляет точку $R_1 = (x_R, y_R) = k_1Q$, вычисляет подпись s согласно выражению (1a) и полагает $u_1 = k_1$. При последующих процедурах формирования подписи отправитель вырабатывает случайный показатель k_i, $0 < k_i < r$, а также точку $R_i = k_iQ$, $i = 2, 3, \ldots$.Тогда уравнение формирования подписи на итерациях $i = 2, 3, \ldots$ преобразовывается к виду

$$s \equiv k_iu_{i-1}(k_i^{-1}(u_{i-1}^{-1}l)x_R + u_{i-1}^{-1}e) \pmod r,\ u_i \equiv u_{i-1}k_i \pmod r, \qquad (1b)$$

где показатель s также не зависит от наложения и снятия «маски» $(k_i^{-1}u_{i-1}^{-1}) \pmod r$.

Процедура проверки подписи выполняется согласно стандарту.

Для формирования i-й подписи необходимо хранить текущие значения u_{i-1} и $u_{i-1}^{-1}l$ вместо ключа l. Ключ подписи l используется только в первой процедуре формирования подписи, «маска» постоянно изменяется.

Для оптимизации вычисления подписи можно хранить три параметра u_{i-1}, u_{i-1}^{-1} и $u_{i-1}^{-1}l$: $u_i^{-1} \equiv (u_{i-1}k_i)^{-1} \equiv u_{i-1}^{-1}k_i^{-1} \pmod r$. Это позволит не вычислять значение, мультипликативно обратное к u_i, при формировании подписи каждого нового сообщения.

Независимое вскрытие слов ключа l становится затруднительным, так как каждое слово ключа зависит от всех слов чисел u_i и $u_i^{-1}l$, то есть ключ становится «единым и неделимым».

Определим число арифметических операций в защищенном протоколе подписи. При умножении точки на число длиной 256 бит с использованием бинарного алгоритма производится 256 удвоений точки и в среднем 128 сложений различных точек [2]. Для

удвоения точек в проективных координатах требуется 13 модульных умножений, для сложения точек — 15 модульных умножений [3]. Итого 3315 + 1920 = 5235 модульных умножений. Рассмотренный алгоритм защиты от «side channel attack» требует всего пяти модульных умножений и одного модульного обращения, которое сводится к вычислению наибольшего общего делителя при помощи расширенного алгоритма Евклида [2]. Таким образом, применение рассмотренного подхода не приводит к сколько-нибудь заметному замедлению вычисления подписи и в то же время является эффективным средством обеспечения безопасности ключа при формировании электронной цифровой подписи.

ЛИТЕРАТУРА:

1. Ростовцев А.Г. Защита ключа формирования подписи от Side channel attack // Проблемы информационной безопасности. Компьютерные системы. СПб.: 2003. № 4.
2. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1997.
3. Ростовцев А.Г. Алгебраические основы криптографии. СПб.: Мир и Семья, Интерлайн, 2000.