А. Г. Ростовцев, Е. Б. Маховенко

Простое усиление схемы цифровой подписи Эль-Гамаля, DSS, ГОСТ Р 34.10–94

Обобщенный протокол подписи Эль-Гамаля основан на задаче дискретного логарифмирования в произвольной циклической подгруппе G простого порядка q группы $\boldsymbol{G}$. В качестве группы $\boldsymbol{G}$ может использоваться мультипликативная группа конечного поля, группа классов квадратичного поля, группа точек эллиптической кривой, якобиан алгебраической кривой. Протокол подписи Эль-Гамаля в подгруппе мультипликативной группы простого поля положен в основу стандартов DSS и ГОСТ Р 34. 10–94.

Открытым ключом проверки подписи является тройка: {группа G, образующая Q группы G, элемент $P \in G$}; секретным ключом создания подписи — показатель $l \in \mathbf{Z}$ такой, что $P = lQ$. Кроме того, общеизвестными являются хэш-функция h и вычислимая в одну сторону функция

$$f\colon G \to \mathbf{Z}/q\mathbf{Z}.$$

Будем использовать аддитивную запись групповой операции в G.

Для создания подписи отправитель сообщения m генерирует случайный показатель k, вычисляет $R = kQ$, полагает $r = f(R)$ и находит значение s решением уравнения в $\mathbf{Z}/q\mathbf{Z}$:

$$h(m) = lr + ks. \tag{1}$$

Подписью является пара (R, s).

Получатель сообщения m проверяет, что $R \in G$, и сравнивает элементы $h(m)Q$ и $f(R)P + sR$. Если они равны, то подпись правильная.

Хэш-функция h позволяет исключить возможность подделки подписи на основе правильной пары сообщение/подпись.

Протокол подписи Эль-Гамаля допускает следующую атаку. Нечестный исполнитель, подающий начальнику документ на подпись, может заготовить коллизию (пару текстов m_1, m_2 таких, что $h(m_1) = h(m_2)$), отдать m_1 на подпись и, получив подписанный текст m_1, заменить его на m_2. Такая атака допускает предвычисления.

На практике ключ l или группу G можно периодически менять. Однако при использовании DSS и ГОСТ Р 34.10–94 замена только персонального ключа l бессмысленна. Хэш-функция h и ее параметры обычно сохраняются. Поэтому сложность вычисления коллизий хэш-функции h должна превышать сложность раскрытия ключа создания подписи.

Для раскрытия ключа создания подписи достаточно решить задачу дискретного логарифмирования. Сложность раскрытия ключа в ГОСТ Р 34.10–94 методом решета числового поля описывается субэкспонентой $S = O(\exp(c\sqrt[3]{\ln p(\ln\ln p)^2}))$, где p — характеристика поля, c = 1,92 при

"Методы и технические средства обеспечения безопасности информации". Тезисы докладов. Под ред. П. Д. Зегжды. Спб., Изд-во СПбГТУ, 2000. С. 128–130.

“правильном” выборе характеристики поля и $c \approx 1{,}6$ при “неправильном” ее выборе. Под “неправильным” выбором понимается существование неприводимого над $\mathbf{F}_p$ многочлена специального вида, связанного с простым числом p, например, так, что имеет место сравнение $ax^n + b \equiv 0 \pmod p$ с малыми по абсолютной величине значениями a, b, x, n. Поэтому на практике при использовании в качестве группы G мультипликативной группы простого поля поиск коллизий хэш-функции обычно является более трудоемким, чем раскрытие ключа.

Как правило, мощность множества значений хэш-функции близка к q. Сложность нахождения коллизии любой хэш-функции алгоритмом Полларда не может превышать $O(\sqrt{q})$. Сложность логарифмирования в некоторых группах, например, в группе точек эллиптической кривой и в якобиане алгебраической кривой, равна $O(\sqrt{q})$. Поэтому здесь хэш-функция может оказаться “слабым местом”.

Однако схема подписи Эль-Гамаля и, следовательно, протоколы DSS и ГОСТ Р 34.10–94 допускают простое усиление. Для этого достаточно изменить уравнение (1) создания подписи:

$$h(m\|R) = lr + ks, \tag{2}$$

где $\|$ — символ конкатенации. Это сделает заготовку коллизий практически невозможной, так как часть R аргумента хэш-функции заранее неизвестна.

Такое изменение уравнения создания подписи не влияет на сложность раскрытия ключа. Действительно, секретный ключ полностью определяется открытым ключом и может быть найден с помощью логарифмирования. Кроме того, ключ может быть найден, если один и тот же показатель k используется дважды или если $ks = 0$ в $\mathbf{Z}/q\mathbf{Z}$, независимо от аргумента хэш-функции. В ГОСТ Р 34.10–94 в уравнении (1) значения s и $h(m)$ меняются местами, поэтому здесь нужно обеспечить $h(m\|R) \neq 0$.

Протокол Эль-Гамаля с уравнением (1) в некоторых случаях допускает возможность подделки подписи без раскрытия ключа. В этом случае нарушитель по известной тройке (m, R, s) может найти тройку (m', R', s'), удовлетворяющую проверочным условиям. Для этого нарушитель выбирает сообщение m', вычисляет коэффициент β такой, что $h(m') = \beta h(m)$ в $\mathbf{Z}/q\mathbf{Z}$, полагает $r' = \beta r$, находит R' по r' и решает задачу логарифмирования: определяет показатель α такой, что $R' = \alpha R$. Тогда $s' = \alpha^{-1}\beta s$.

В случае уравнения (2) эта атака усложняется, так как уже показатель β вычислить сложно — нужно решить систему уравнений $h(m'\|R') = \beta h(m\|R)$, $f(R') = \beta f(R)$. Таким образом, предлагаемое изменение протокола подписи не только исключает заготовку коллизий, но и затрудняет подделку подписи без знания ключа. Использование уравнения (2) позволяет обеспечить стойкость схемы даже при условии неизменности параметров хэш-функции.