УДК 003.26

КОМПОЗИЦИЯ СИММЕТРИЧНОГО ШИФРА И ШИФРА НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ ДЛЯ ПОСТРОЕНИЯ ЭЦП

Дихтенко А.А., Рыбак Е.М., Шкодина Л.Н.
Донецкий национальный университет

Рассмотрена задача обеспечения информационной безопасности электронных документов с помощью электронно-цифровой подписи. Предлагается алгоритм для построения хэш-функции по типу «разработанной с нуля». Все операции выполняются в классе вычетов. Для получения ЭЦП результат хэш-функции зашифровывается композицией одного из симметричных алгоритмов и ассиметричного шифра на эллиптических кривых. Создан программный комплекс в среде Visual C++ для получения хэш-кода и построения ЭЦП.

С переходом к безбумажным способам передачи информации и хранения данных, а также с развитием систем электронного перевода денежных средств, проблема виртуального подтверждения аутентичности документа приобрела особую остроту. Развитие любых подобных систем теперь немыслимо без существования электронных подписей под электронными документами. Неотъемлемой частью электронно-цифровой подписи является использование хэш-функций [1-5].

В данной работе построена хэш-функция по типу «разработанная с нуля» [1] с использованием операций в классе вычетов [3], а ЭЦП под электронным документом создается при помощи композиции двух шифров: шифра матричного обхода (или общего шифра перестановки) и шифра, основанного на эллиптических кривых.

Работа хэш-функции начинается с того, что входная последовательность делится на блоки (векторы) по 30 элементов. В случае если длина исходного текста не кратна 30, то он дополняется пробелами. Далее инициализируется пять целочисленных векторов по 30 элементов *A, B, C, D, E* и пять дополнительных векторов с начальными значениями *a=A, b=B, c=C, d=D, e=E*. Основной цикл, совершаемый над каждым 30-элементным блоком, состоит из последовательного применения различных операторов, состоящих из операций над функциями $f_1(X,Y,Z)$, $f_2(X,Y,Z)$, $f_3(X,Y,Z)$, $f_4(X,Y,Z)$ и векторами *a, b, c, d, e*. Функции $f_i(X,Y,Z)$ содержат операции над аргументами, такие как обращения элементов векторов в классе вычетов, сдвиг, сложение векторов и т.д.

$$\begin{gathered} f_1(X,Y,Z)=(X^{-1}+Y)\times Z; \\ f_2(X,Y,Z)=((Z-X)^{-1}<<7)+Y; \\ f_3(X,Y,Z)=(X*Y)^{-1}\cdot Z)+X; \\ f_4(X,Y,Z)=(Z+Y)\times(X^{-1}<<2), \end{gathered} \tag{1}$$

где X^{-1} – вектор, состоящий из элементов, взаимнообратных к элементам *X* в классе вычетов, «×» - почленное перемножение элементов векторов, «*» - скалярное произведение векторов, «·» - умножение вектора на число, *(X<<n)* – циклический сдвиг элементов *X* на *n* позиций.

Каждый оператор над текущим *k*-м блоком имеет вид:

```
for (p=1; p≤4; ++p)
 {
  R=(a<<(3+p)+f_p(b,d,c)+W_k);
  e=d+e;                                  (2)
  d=c+(d<<7);
  c=b-a;
  a=R;
 }
```

где *k* – номер блока, W_k – *k*-й блок исходного текста.

В формулах (1) и (2) вычисления проводятся в классе вычетов по модулю *n*, где *n* – длина выбранного алфавита [3]. В качестве исходного алфавита выбран латинский алфавит, дополненный знаками « », «.», «,» (*n=29*). После обработки каждого блока W_k исходные векторы *A, B, C, D, E* изменяются следующим образом:

6

$A=A+a,\ B=B+b,\ C=C+c,\ D=D+d,\ E=E+e.$

После завершения обработки электронного документа получаем хэш-код $h=(A+B+C+D+E)\bmod n$.

Для построения электронной подписи к полученному хэш-коду применяется композиция шифров матричного обхода (или общего шифра перестановки) и асимметричного шифра, построенного на эллиптических кривых.

Матричный шифр обхода (общий шифр перестановки) относится к классу шифров перестановки и является симметричным шифром. Ключом данного шифра является слово в выбранном алфавите. На следующем этапе происходит шифрование полученной последовательности символов с использованием точек эллиптических кривых.

В общем случае эллиптической кривой ε называется гладкая кривая, состоящая из множества точек (x, y), удовлетворяющих уравнению Вейерштрасса

$$y^2+uxy+vy=x^3+px^2+qx+r \tag{3}$$

где u, v, p, q, r являются действительными числами [3].

6

Эллиптическая кривая включает также некоторый элемент, обозначаемый O и называемый *несобственным элементом* (а также бесконечным элементом, или нулевым элементом).

Уравнение (3) можно привести к виду [4]

$$y^2=x^3+ax^2+bx+c, \tag{4}$$

где $\Delta=-(4a^3+27b^2)$ – дискриминант кривой. Будем рассматривать кривые, дискриминант которых не равен нулю. На рисунке 1 приведен пример эллиптической кривой.

Для эллиптических кривых справедливо следующее утверждение: если прямая пересекает эллиптическую кривую в двух точках, то она пересекает ее и в третьей точке, для вертикальной прямой этой точкой считается нулевая точка O. И как следствие из вышесказанного: если три точки эллиптической кривой лежат на прямой линии, то их суммой есть O. Руководствуясь этим, на эллиптической кривой может быть определена операция сложения. Относительно этой операции точка в бесконечности $O \in \varepsilon$ служит

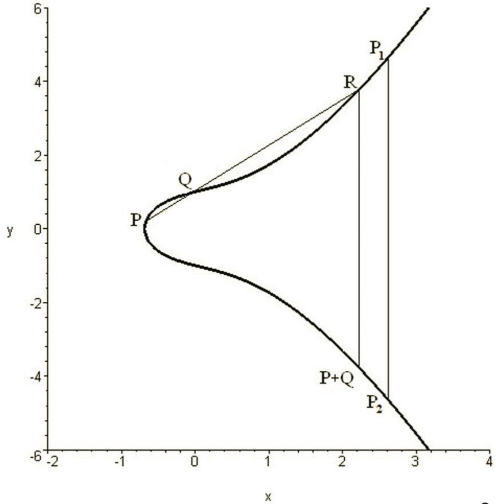

Рисунок 1 – Пример эллиптической кривой $y^2 = x^3 + x + 1$

нулем, а множество ε обладает структурой аддитивной группы.

Из определения и геометрических построений на эллиптических кривых вытекают следующие правила арифметических операции над точками эллиптической кривой [4].

Объект O выступает в роли нулевого элемента при сложении и для любой точки P на эллиптической кривой $P + O = P$.

Отрицание точки. Вертикальная линия пересекает кривую в двух точках с одной и той же координатой x: $P_1 = (x, y)$ и $P_2 = (x, -y)$. Эта линия пересекает кривую и в бесконечной точке. Поэтому $P_1 + P_2 + O = O$, тогда $P_1 = -P_2$. То есть $-(x, y) = (x, -y)$. Если $P_1 = -P_2$, то мы определяем сумму $P_1 + P_2$ как точку бесконечности O. Это правило отражено на рисунке 1.

Сложение точек. Если P и Q – точки эллиптической кривой, имеющие различные координаты, то прямая $l = PQ$ пересечет кривую еще только в одной точке R. Известно, что $P + Q + R = O$, следовательно $P + Q = -R$. Таким образом, чтобы сложить две точки P и Q с разными координатами x, необходимо провести через эти точки прямую и найти третью точку пересечения R этой прямой с эллиптической кривой, и сумма $P + Q$ будет равна отрицанию точки R. Эта конструкция также показана на рисунке 1.

Дублирование точки. Пусть теперь $P = Q$. Тогда прямая l является касательной к эллиптической кривой в точке P и пересекает кривую в единственной точке R. Тогда полагаем, что $2P = -R$.

Вышеприведенные правила сложения подчиняются всем обычным свойствам сложения, например коммутативному и ассоциативному законам. Умножение точки P эллиптической кривой на положительное целое число k также определено – это сумма k копий точки P. Так, $2P = P + P$, $3P = P + P + P$ и т.д.

В случае криптографии с использованием эллиптических кривых приходится иметь дело с эллиптической кривой вида (4), которая определяется над конечным полем. Особый интерес для криптографии представляет объект, называемый эллиптической группой по модулю p, где p является простым числом. Такая группа определяется следующим образом. Выбираются два целых числа, a и b, которые меньше p и удовлетворяют условию $\Delta(mod\ p) \neq 0$.

Тогда $E_p(a,b)$ обозначает эллиптическую группу по модулю p, элементами которой (x,y) являются пары неотрицательных целых чисел, которые меньше p и удовлетворяют условию

$$y^2 \equiv x^3 + ax + b(mod\ p) \tag{5}$$

6

вместе с точкой в бесконечности O.

Правила сложения в эллиптической группе $E_p(a,b)$ соответствуют уже рассмотренным выше геометрическим приемам.

Формально эти приемы для всех точек $E_p(a,b)$ могут быть записаны следующим образом.

1. Для любого P имеем: $P + O = P$.
2. Если $P = (x, y)$, то $P + (x, -y) = O$. Точка $(x, -y)$ лежит на эллиптической кривой и принадлежит $E_p(a,b)$.
3. Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, где $P \neq Q$, то $P + Q = (x_3, y_3)$ определяется в соответствии с правилами

$$\begin{aligned} x_3 &\equiv \lambda^2 - x_1 - x_2(mod\ p), \\ y_3 &\equiv \lambda(x_1 - x_3) - y_1(mod\ p), \end{aligned} \tag{6}$$

где:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, if \ P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, if \ P = Q \end{cases} \tag{7}$$

Построение криптографической системы на основе эллиптических кривых состоит из нескольких этапов. Сначала выбирается большое простое число p и параметры a и b для эллиптической кривой. Это задает эллиптическую группу точек $E_p(a,b)$.

Для того, чтобы зашифровать открытый текст сообщения, буквам выбранного алфавита ставятся в соответствие точки группы $E_p(a,b)$ случайным образом. Необходимо обратить внимание на то, что мы не можем закодировать сообщение просто координатами (x,y), так как не все такие координаты имеются в $E_p(a,b)$.

Затем в $E_p(a,b)$ выбирается генерирующая точка $G=(x_1,y_1)$. При выборе G важно, чтобы наименьшее значение n, при котором $nG = O$, оказалось очень большим простым числом.

6

Пользователь B выбирает личный ключ $n_B<n$ и генерирует открытый ключ $P_B=n_B \times G$. Чтобы зашифровать и послать сообщение P_m пользователю B, пользователь A выбирает случайное положительное целое число $k< n$ и вычисляет шифрованный текст C_m состоящий из пары точек [3]

$$C_m = \{kG, P_m + kP_B\}. \tag{8}$$

Здесь сторона A использует открытый ключ P_B участника обмена B. Чтобы дешифровать этот шифрованный текст, B умножает первую точку в паре на секретный ключ B и вычитает результат из второй точки

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m. \tag{9}$$

Вычисления в формулах (8) и (9) проводятся по mod p.

Пользователь A замаскировал сообщение P_m с помощью добавления к нему kP_B Никто, кроме этого пользователя, не знает значения k, поэтому, хотя P_B и является открытым ключом, никто не сможет убрать маску kP_B. Противнику для восстановления сообщения придется вычислить k по данным G и kG, что представляется трудной задачей.

Для построения хэш-кода и электронно-цифровой подписи под исходным документом создан программный комплекс в среде Visual C++.

Литература

[1] Мао В. Современная криптография: Теория и практика/ В. Мао. – М.: Вильямс, 2005. – 763 с.

[2] Петров А.А. Компьютерная безопасность. Криптографические методы защиты / Петров А.А. – М.: ДМК, 2000. – 445с.

[3] Столингс В. Криптография и защита сетей / В. Столингс. – М.: Вильямс, 2001. – 669 с.

[4] Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник/В. Тилборг. – М.: Мир, 2006. – 471 с.

[5] Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си/ б. Шнайер. – М.: Триумф, 2002. – 816 с.