УДК 681.3

Кравцов Г.А., директор ООО «НВФ «БКП-Консалтинг», г.Киев.

Задача Диффи-Хелмана и ее развитие.

Известная задача Диффи-Хелмана [1] основана на использовании функции возведения в степень в мультипликативной группе простого поля: $f(x) = a^x \bmod p$, где p - простое число, a - примитивный элемент поля $GF(p)$, $1 < x < p-1$. Эта функция является кандидатом в однонаправленные функции. Действительно, она легко вычислима, так как, используя метод квадратов, значения этой функции можно вычислять с полиномиальной сложностью, оцениваемой величиной $O((\log p)^3)$, в то время как обратная задача является сложной.

Однако нельзя полагать, что за более чем двадцать лет не достигнуто определенных результатов в решении задачи дискретного логарифмирования. Тем самым цель усиления задачи Диффи-Хелмана является оправданной.

Для достижения поставленной цели исследовано множество рациональных функций (элементарных и специальных) и особое внимание было уделено гамма-функции (интегралу Эйлера 2-го рода) [2]. За основу был взято произведение

$$\Gamma(z) = \lim_{n\to\infty} \frac{n^z}{z} \prod_{k=1}^{n} \frac{k}{z+k},$$

которое было представлено в виде

$$G(n,a) = \frac{n^a}{a} \prod_{k=1}^{n} \frac{k}{a+k}. \qquad (1)$$

Основное свойство (1) заключается в следующем:

$$G^m(n,a) = \frac{n^{am}}{a^m} \prod_{k=1}^{n} \left(\frac{k}{a+k}\right)^m. \qquad (2)$$

Значения $G(n,a)$ могут быть «помещены» в поле Галуа метрики p следующим образом

$$G(n,a) = \left(\frac{n^a}{a} \prod_{k=1}^{n} \frac{k}{a+k}\right) \bmod p. \qquad (3)$$

При известных значениях a,n уравнение $f(x) = G^x(n,a)$ сводиться к задаче Диффи-Хелмана [1]. При неизвестных значениях a,n, задача нахождения x очевидно усложняется. Выражение (3) имеет определенный смысл при использовании в процессорах цифровой обработки сигнала. Для использования в системах, где операции деления с плавающей запятой затруднительны, лучше использовать

$$G(n,a) = (n^a \prod_{k=1}^{n} a^k) \bmod p = (n^a a^{\sum_{k=1}^{n} k}) \bmod p = (n^a a^{\frac{n(n+1)}{2}}) \bmod p. \quad (4)$$

Предложенная функция (4) нашла применение в протоколе с открытыми ключами с арбитром и центром сертификации ключей. Свойство (2) в таком случае немного преображается

$$G^m(n,a) = (n^{am} \prod_{k=1}^{n} a^{km}) \bmod p = (n^{am} a^{m\sum_{k=1}^{n} k}) \bmod p = (n^{ma} a^{\frac{mn(n+1)}{2}}) \bmod p.$$

Можно сформулировать следующие задачи в алгебраическом виде:

Пусть $f(n,a) = n^a \prod_{k=1}^{n} a^k$. Найти значение n, если известно $a, f(n,a)$ и найти a, если известно $n, f(n,a)$. Если попытаться решить эти задачи через логарифмирование, то придем к необходимости решения следующих двух уравнений:

$$\begin{aligned} &\log_a f(n,a) = a \log_a n + \sum_{k=1}^{n} k \ \text{(неизвестно } n\text{)}, \\ &\log_n f(n,a) = a + (\log_n a) \sum_{k=1}^{n} k \ \text{(неизвестно } a\text{)}. \end{aligned} \quad (5)$$

Выражение $\sum_{k=1}^{n} k$ является арифметической прогрессией и может быть заменено по формуле $S_n = \frac{n(a_1 + a_n)}{2}$ (S_n - сумма n членов). Уравнения (5) примут вид:

$$\log_a f(n,a) = a \log_a n + \frac{n(1+n)}{2} \ \text{(неизвестно } n\text{)},$$

$$\log_n f(n,a) = a + (\log_n a) \frac{n(n+1)}{2} \ \text{(неизвестно } a\text{)}.$$

Приведенные выше уравнения являются трансцендентными, т.е. вообще могут быть решены только приблизительно, а в нашем случае только перебором, что является положительным качеством.

Однако, попытаемся решить уравнение $f_0(n,a) = n^a a^n$. Если нам удастся его решить, то по аналогии можно решить уравнение $f(n,a) = n^a a^{\frac{n(n+1)}{2}}$.

Представим a^n и n^a в виде сумм и найдем произведение.

$$n^a = \sum_{k=0}^{\infty} \frac{(a \ln n)^k}{k!},\ a^n = \sum_{k=0}^{\infty} \frac{(n \ln a)^k}{k!},$$

$$a^n n^a = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \frac{a^i n^j (\ln n)^i (\ln a)^j}{4^{i+j} \prod_{k=1}^{\infty} \frac{\Gamma(\frac{1}{2} + \frac{i}{2^k}) \Gamma(\frac{1}{2} + \frac{j}{2^k})}{\Gamma^2(\frac{1}{2})}} \quad (6)$$

Функция $f_0(n,a) = n^a a^n$ имеет ряд интересных свойств:

$$\frac{df_0(n,a)}{da} = f_0(n,a)(\frac{n}{a} + \ln n),$$

$$df_0(n,a) = f_0(n,a)((\frac{n}{a} + \ln n)da + (\frac{a}{n} + \ln a)dn).$$

На базе данной функции (4) рассмотрим протокол взаимодействия.

Рассмотрим алгоритм взаимодействия двух абонентов X, Y, арбитра A и центра сертификации C.

Действующие лица:

№	Участник	Имя	Секретный ключ
1.	Абонент X	Алиса	x
2.	Абонент Y	Боб	y
3.	Арбитр A	Уолтер	a
4.	Центр сертификации C	Виктор	c

Параметры n, m являются данными, принадлежащими Арбитру (Уолтеру) A.

Открытыми параметрами являются значения g, p, которые участвуют в создании первичной линии передачи по Диффи-Хелману. Центр сертификации и арбитр являются элементами одной системы и обмен данными между ними защищен технологически. Доступ к каналу между арбитром и центром недопустим.

Следующее формальное описание $X(g^{ax} \bmod p) - n, m \to (g^{ax} \bmod p)Y$ следует понимать так: Алиса X по закрытому каналу с ключом $g^{ax} \bmod p$ передает Бобу Y, которому известен ключ $g^{ax} \bmod p$ информацию (данные) n и m. Формальное описание $X, A : g^{ax} \bmod p$ следует понимать так: Алиса X и Уолтер A вычисляют значение $g^{ax} \bmod p$.

Представим алгоритм в виде последовательных шагов:

№	Формальное описание	Примечание
1.	Открыто публикуются значения: g, p.	
2.	$X() - g^x \bmod p \to ()A$	Абонент X передает Арбитру A по открытому каналу $g^x \bmod p$, где x - случайное число, сгененированное Абонентом X.
3.	$A() - g^a \bmod p \to ()X$	Арбитр A передает Абоненту X по открытому каналу $g^x \bmod p$, где a - случайное число, сгененированное Арбитром A для даннго сеанса связи.
4.	$X, A: g^{ax} \bmod p$	Арбитр A и Абонент X вычисляют значение $g^{ax} \bmod p$, являющееся сеансовым ключом для передачи параметров n, m, которые являются основными для получения ключевой информации.
5.	$A(g^{ax} \bmod p) - n, m \to (g^{ax} \bmod p)X$	Передачи взаимнопростых параметров n, m, сгенерированных Арбитром A по закрытому каналу с ключом $g^{ax} \bmod p$.
6.	$X: G^x(m,n)$, $A: G^a(m,n)$	Арбитром A вычисляет значение $G^a(m,n)$, Абонент X вычисляет значение $G^x(m,n)$.
7.	$A() - G^a(m,n) \to ()X$	Арбитр A передает Абоненту X по открытому каналу $G^a(m,n)$.
8.	$X() - G^x(m,n) \to ()A$	Абонент X передает Арбитру A по открытому каналу $G^x(m,n)$.
9.	$X, A: G^{ax}(m,n)$	Арбитр A и Абонент X вычисляют значение $G^{ax}(m,n)$, являющееся сеансовым ключом для передачи имени адресата (Абонент Y).

№	Формальное описание	Примечание
10.	$X(G^{ax}(m,n)) - Y \to (G^{ax}(m,n))A$	Абонент X передает Арбитру A имя адресата (Абонент Y). На данном шаге возможен учет и биллинг.
11.	$A() - g^a \bmod p \to ()Y$	Арбитр A передает Абоненту Y по открытому каналу $g^a \bmod p$ для сеанса связи.
12.	$Y() - g^y \bmod p \to ()A$	Абонент Y передает Арбитру A по открытому каналу $g^y \bmod p$
13.	$Y, A: g^{ay} \bmod p$	Арбитр A и Абонент Y вычисляют значение $g^{ay} \bmod p$, являющееся сеансовым ключом для передачи параметров n, m, которые являются основными для получения ключевой информации.
14.	$A(g^{ay} \bmod p) - n, m \to (g^{ay} \bmod p)Y$	Передачи взаимнопростых параметров n, m по закрытому каналу с ключом $g^{ay} \bmod p$.
15.	$Y: G^y(m,n)$	Абонент Y вычисляют значение $G^y(m,n)$
16.	$Y() - G^y(m,n) \to ()A$	Абонент Y передает значение $G^y(m,n)$ Арбитру A.
17.	$A() - G^a(m,n) \to ()Y$	Арбитр A передает Абоненту Y по открытому каналу $G^a(m,n)$.
18.	$A, Y: G^{ay}(m,n)$	Арбитр A и Абонент Y вычисляют значение $G^{ay}(m,n)$, являющееся сеансовым ключом для передачи имени вызывающего абонента (Абонент X).
19.	$A(G^{ay}(m,n)) - X \to (G^{ay}(m,n))Y$	Арбитр A передает Абоненту Y имя вызывающего абонента (Абонент X) по закрытому каналу ключом

№	Формальное описание	Примечание
		$G^{ay}(m,n)$.
20.	$A() - X, Y, G^{ay}(m,n), G^{ax}(m,n), a \to ()C$	Обмен данными защищен технологически. По «короткому» каналу передаются данные $X, Y, G^{ay}(m,n), G^{ax}(m,n), a$. Принципиально, канал можно защитить и криптографически, что объективно не усложняет схему.
21.	$Y() - G^{y}(m,n) \to ()C$	Абонент Y передает значение $G^{y}(m,n)$ Центру сертификации C.
22.	$X() - G^{x}(m,n) \to ()C$	Абонент X передает значение $G^{x}(m,n)$ Центру сертификации C.
23.	$C : G^{ay}(m,n), G^{ax}(m,n)$	Вычисляет параметры защищенной связи и сравнивает с полученными параметрами от A.
24.	$C : G^{ayc}(m,n), G^{axc}(m,n)$	Центр сертификации изменяет значения ключей для последующего использования.
25.	$C() - G^{ayc}(m,n) \to ()X$	Центр сертификации C передает Абонентам X и Y промежуточное значение для получения окончательного ключа.
26.	$C() - G^{axc}(m,n) \to ()Y$	
27.	$X, Y : G^{ayxc}(m,n)$	Абонент X и Абонент Y вычисляют уникальное значение ключа для сеанса связи между собой, которое неизвестно Арбитру A и Центру сертификации C.

На 9 шаге возможно предусмотреть учет и биллинг при коммерческом использовании.

На 22 шаге Виктор C по известному ключу a вычисляет значения, которые должны быть получены из значений, которые представляют Виктору C Алиса X и Боб Y.

На 26 шаге Алиса X и Боб Y получают ключ, неизвестный Уолтеру A и Виктору C.

Рассмотрение алгоритма в схемах приводиться в Приложении 1.

Предложенный алгоритм (протокол) позволяет решить ряд задач, однако автор считает предложенную функцию (4) необходимой, но недостаточной для организации связи с открытым распространением ключей с гарантированной стойкостью.

Библиография

1. Dh.W.Diffie, M.E.Hellman. “New directions in cryptography”, IEEE Trans. Inform. Theory, vol.IT-22, pp.644-654, Nov.1976
2. И.С.Градштейн, И.М.Рыжик, «Таблицы интегралов, сумм, рядов и произведений», М., Физматгиз, 1962 г., 1100 стр.с илл., стр.950 (См III 267 (130)).

Григорий А. Кравцов

Digitally signed by Григорий А. Кравцов
DN: cn=Григорий А. Кравцов, ou=SMTP, dc=org
Reason: I am the author of this document
Date: 2006.01.18 11:24:39 +02'00'