Схема генерации ключей на базе полупрямого произведения групп

А. А. Григорьев, П. В. Дудкин

Предложена модификация известной схемы генерации секретного ключа Диффи-Хеллмана [1], использующая операцию возведения в степень в некоммутативной группе порядка p^3, построенной как полупрямое произведение циклических групп порядков p^2 и p. Показано, что для несанкционированного получения секретного ключа в предложенной схеме требуется решение некоторой вычислительно трудной задачи, сложность которой превышает сложность вычисления дискретного логарифма.

1. Схема Диффи-Хеллмана

Пусть две стороны, A и B, соединенные каналом связи, хотят стать обладателями секретного ключа K, недоступного какой-либо третьей стороне. Для этого они предварительно выбирают и публикуют больше простое число p и некоторый элемент ξ из мультипликативной группы Z_p^* кольца Z_p чисел по модулю p.

Сторона A случайно выбирает большое натуральное l, вычисляет число $L = \xi^l$ и передает его стороне B. Сторона B выбирает случайное r и передает стороне A число $R = \xi^r$. По завершении обмена $L \leftrightarrows R$ стороны получают возможность вычислить общий ключ K

$$R^l = (\xi^r)^l = K = (\xi^l)^r = L^r.$$

Для того, чтобы третья сторона, перехватившая сообщения $L = \xi^l$ и $R = \xi^r$, смогла вычислить ключ K, она должна найти хотя бы один из случайных показателей l, r, то есть, решить задачу вычисления дискретного логарифма $l = \log_\xi L$ или $r = \log_\xi R$. На сегодняшний день эти задачи слывут вычислительно не реализуемыми при достаточно больших p, что и служит обоснованием стойкости схемы.

Очевидный путь развития схемы Диффи-Хеллмана может состоять в переходе от вычислений в структурно простой циклической группе Z_p^* к вычислениям в более сложных, в том числе некоммутативных группах. Подход, предложенный в [2], как раз и является шагом в этом направлении. Он опирается на хорошо известную конструкцию полупрямого произведения групп.

2. Полупрямые произведения

Пусть даны две группы N и H и пусть $\varphi : H \to Aut(N)$ – гомоморфизм группы H в группу автоморфизмов группы N. Иными словами, пусть каждому элементу $h \in H$ поставлен с соответствие автоморфизм $\varphi_h(n) : N \to N$, так что $\varphi_{h_1}(\varphi_{h_2}(n)) = \varphi_{h_1 h_2}(n)$.

Полупрямое произведение $G = N \times_\varphi H$ вводится как множество пар (n, h), $n \in N, h \in H$ с групповой операцией

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

Ассоциативность так введенного умножения легко проверяется. Нейтральным элементом группы $G = N \times_\varphi H$ является пара (e, e) нейтральных элементов N и H. Обратным к (n,h) является элемент $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Наборы (n, e), $n \in N$ и (e, h), $h \in H$ образуют подгруппы, изоморфные N и H. Пересечение этих подгрупп состоит из единственного нейтрального элемента (e, e). Легко показать, что $(\mathrm{e}, h)(n, e)(e, h)^{-1} = (\varphi_h(n), e)$, так что подгруппа N нормальна в G (инварианта относительно внутренних автоморфизмов), а действие на N внутреннего автоморфизма, отвечающего элементу (e, h), совпадает с действием φ_h.

3. Генерация ключей на полупрямых произведениях

Пусть в публичном доступе находится элемент (n,h) полупрямого произведения $G = N \times_\varphi H$. Как и ранее, сторона A выбирает случайное l и вычисляет $(n,h)^l$. Получается:

$$(n,h)^2 = (n,h)(n,h) = (n\varphi_h(n), h^2),$$

$$(n,h)^3 = (n\varphi_h(n), h^2)(n,h) = (n\varphi_h(n)\varphi_{h^2}(n), h^3),$$

и так далее до

$$(n,h)^l = (n\varphi_h(n)\varphi_{h^2}(n)\dots\varphi_{h^{(l-1)}}(n), h^l) = (L, h^l).$$

Элемент $L = n\varphi_h(n)\varphi_{h^2}(n)\dots\varphi_{h^{(l-1)}}(n)$ передается стороне B. Сторона B выбирает случайное r, вычисляет $(n,h)^r = (R, h^r)$ и передает $R = n\varphi_h(n)\varphi_{h^2}(n)\dots\varphi_{h^{(r-1)}}(n)$ стороне A. Теперь стороны A и B оказываются с состоянии вычислить общий ключ. На стороне A вычисление проводится по схеме

$$(n,h)^{l+r} = (n,h)^l(n,h)^r = (L,h^l)(R,\dots) = (L\varphi_{h^l}(R),\dots),$$

а на стороне B несколько иначе

$$(n,h)^{l+r} = (n,h)^r(n,h)^l = (R,h^r)(L,\dots) = (R\varphi_{h^r}(L),\dots).$$

Общим для двух сторон ключем становится элемент $K = L\varphi_{h^l}(R) = R\varphi_{h^r}(L)$.

Чтобы вычислить ключ K по результатам перехвата L, R, необходимо знать хотя бы один из показателей l, r, а их нахождение по известным L, R представляется вычислительно трудной задачей со сложностью, не уступающей сложности вычисления дискретного логарифма. Разумеется, эта сложность зависит от того, насколько удачно выбрана структура полупрямого произведения групп.

4. Генерация ключей на группе порядка p^3

Известно, что существует в точности две некоммутативные группы порядка p^3. Одна из них является полупрямым произведением циклической группы $N = C_{p^2}$ порядка p^2 на циклическую группу $H = C_p$ порядка p. Вторая получается как полупрямое произведение группы $N = C_p \times C_p$ – декартова произведения двух групп C_p на ту же группу $H = C_p$. Более предпочтительной с позиций криптографии представляется первая группа, содержащая элементы периода p^2. Периоды элементов второй группы составляют p.

Группа автоморфизмов группы C_{p^2} изоморфна декартову произведению $C_p \times C_{p-1}$ и содержит подгруппу, изоморфную C_p. Так что вложение группы $H = C_p$ в группу автоморфизмов группы $N = C_{p^2}$ конструируется естественным образом.

Циклическую группу C_{p^2} можно реализовать как подгруппу мультипликативной группы $Z^*_{p^3}$ кольца Z_{p^3}. Группа $Z^*_{p^3}$ циклическая порядка $p^2(p-1)$. В ней существует подгруппа порядка p^2, порожденная степенями некоторого элемента $\xi \in Z_{p^3}$ порядка p^2. Итак, пусть

$$N = \{1 = \xi^0, \xi^1, \xi^2, \dots \xi^{p^2-1}, \xi^{p^2} = \xi^0 = 1\}, \quad \xi \in Z_{p^3},\ \xi^{p^2} = 1.$$

В этом представлении отображение аддитивной группы $H = C_p$ в группу автоморфизмов группы $N = C_{p^2}$ строится элементарно: элементу $h \in C_p$ поставим в соответствие автоморфизм $\varphi_h(\xi^n) = \xi^{n(1+ph)}$. Это соответствие действительно является гомоморфизмом, поскольку

$$\varphi_{h_2}(\varphi_{h_1}(\xi^n)) = \xi^{n(1+ph_1)(1+ph_2)} = \xi^{n(1+p(h_1+h_2))} = \varphi_{h_1+h_2}(\xi_n).$$

Степень s элемента (ξ, n) в $G = C_{p^2} \times_\varphi C_p$ вычисляется как

$$(\xi,n)^s = (\xi\xi^{1+np}\xi^{1+2np}\dots\xi^{1+n(s-1)p}, sn) = (\xi^{s+np\frac{s(s-1)}{2}}, ns).$$

Результатом становится следующая схема генерации ключей: Публикуемые данные – простое p, элемент $\xi \in Z_{p^3}$ порядка p^2, натуральное $n \in Z_p$.

Сторона A выбирает случайное l, вычисляет $L = \xi^{l+np\frac{l(l-1)}{2}}$ и передает L на сторону B.

Сторона B выбирает случайное r, вычисляет $R = \xi^{r+np\frac{r(r-1)}{2}}$ и передает R на сторону A.

Стороны вычисляют общий секретный ключ по схеме

$$K = LR^{(1+npl)} = RL^{(1+npr)}.$$

Для нахождения секретного ключа K по перехваченным L, R злоумышленнику придется решить уравнение

$$S = \xi^{s+np\frac{s(s-1)}{2}}$$

в кольце Z_{p^3} относительно показателя s, что представляется более сложным по сравнению с обычной задачей нахождения дискретного логарифма.

5. Заключение

Конструкция полупрямого произведения групп может стать основой чрезвычайно широкого класса схем генерации ключей, родственных схеме Диффи-Хеллмана. Более или менее ясно, что полупрямые произведения коммутативных групп приведут к результатам, близким к представленному выше. Значительно больший интерес могут представлять варианты, когда одна или обе исходные группы изначально некоммутативны. Построение и исследование таких схем представляется перспективной задачей.

Литература

1. *Diffie W., Hellman M. E.*, New Directions in Cryptography // IEEE Transactions on Information Theory 1976, IT-22, P 644.
2. *Kahrobaei D., Koupparis C., Shpilrain V.* Public key exchange using matrices over group rings // Groups, Complexity, Cryptology 2013, V. 5, P. 97.