

Обобщения протокола Диффи-Хеллмана

Анатолий Лебедев
АО «ИИТ» (г. Москва)

Общий протокол Диффи-Хеллмана

Стороны A и B , умеют вычислять дискретные функции $f(x), g(x, y)$

Функция f определена на X и принимает значения в Y $f: X \rightarrow Y$

Функция g определена на $X \times Y$ и принимает значения в Z $g: X \times Y \rightarrow Z$

(2)

Стороны выбирают x, y из X , вычисляют $f(x), f(y)$ и обмениваются ими

$$f(x) \leftrightarrow f(y)$$

(3)

вычисляют общий секрет по формулам

$$K = g(x, f(y)) = g(y, f(x)).$$

(4)

Ранние криптографические примитивы

Дискретная экспонента по модулю большого простого числа p :

$$f: \mathbb{Z}_q \rightarrow \mathbb{Z}_p, f(x) = a^x \pmod{p}, \quad q \mid (p-1)$$

$$g: \mathbb{Z}_q \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p, \quad g(x, y) = y^x \pmod{p}$$

$$K = g(x, f(y)) = f(y)^x \pmod{p} = g(y, f(x)) = f(x)^y \pmod{p},$$

$$K = a^{xy \pmod{q}} \pmod{p} = a^{yx \pmod{q}} \pmod{p}$$

Современные криптографические примитивы

Вычисление кратной точки эллиптической кривой над полем $\mathbb{Z}_p$

$$E_{a,b}(p) = \{(x, y) \mid x, y \in \mathbb{Z}_p, y^2 = x^3 + ax + b \pmod{p}\}$$

$$f: \mathbb{Z}_q \rightarrow E_{a,b}(p)$$

$$g: \mathbb{Z}_q \times E_{a,b}(p) \rightarrow E_{a,b}(p)$$

$$q * P = O, \quad f(x) = x * P, \quad g(x, f(y)) = x * (y * P)$$

$$K = g(x, f(y)) = x * (y * P) = g(y, f(x)) = y * (x * P).$$

Обобщение протокола Диффи-Хеллмана (DHL)

$$f: \mathbb{Z}_q \rightarrow \mathbb{Z}_p,$$

$$f(x) = a^{\delta(x)} \pmod{p},$$

$\delta(x): \mathbb{Z}_q \rightarrow \mathbb{Z}_q$, подстановка на $\mathbb{Z}_q$.

Функция $g(x, y)$

$$g: \mathbb{Z}_q \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p,$$

$$g(x, y) = y^{\lambda(x)} \pmod{p},$$

$\lambda(x): \mathbb{Z}_q \rightarrow \mathbb{Z}_q$, подстановка на $\mathbb{Z}_q$

Протокол DH

$$K = g(x, f(y)) = f(y)^{\delta(x)} \pmod{p}$$

$$= g(y, f(x)) = f(x)^{\lambda(y)} \pmod{p} =$$

$$= a^{\tau[\delta(x) * \lambda(y) \bmod q]} \pmod{p}.$$

Обобщение протокола ECDH

$$f: \mathbb{Z}_q \rightarrow E_{a,b}(p),$$
$$f(x) = \delta(x)P,$$

$\delta(x): \mathbb{Z}_q \rightarrow \mathbb{Z}_q$, подстановка на множестве $\mathbb{Z}_q$.

Функция $g(x, y)$

$$g: \mathbb{Z}_q \times E_{a,b}(p) \rightarrow E_{a,b}(p),$$
$$g(x, y) = \lambda(x)[\delta(y)P],$$

$\lambda(x), \tau(x): \mathbb{Z}_q \rightarrow \mathbb{Z}_q$, подстановки на множестве $\mathbb{Z}_q$,

Протокол ECDH

$$K = g(x, f(y)) = \lambda(x)[\delta(y)P]$$

$$= g(y, f(x)) = \lambda(y)[\delta(x)P]$$

$$= \tau[\delta(x)\lambda(y) \bmod q]P$$

Пример

Пусть

$$\delta(x) = x, \quad \gamma(y) = y, \quad \lambda(x) = x - \alpha, \quad \mu(y) = y - \beta, \\ \sigma_x(y) = y(a^{-\beta})^{(x-\alpha)}, \quad \tau_y(x) = x(a^{-\alpha})^{(y-\beta)},$$

тогда

$$K = g_A(x, f_B(y)) = \sigma[f_B(y)^{\lambda(x)}](\text{mod } p)$$

$$= g_B(y, f_A(x)) = \tau[f_A(x)^{\mu(y)}](\text{mod } p)$$

$$= a^{(x-\alpha)(y-\beta)} (\text{mod } p)$$

Дробно-линейные преобразования

$$\sigma(x) = \begin{cases} \frac{ax + b}{cx + d} & , x \neq -\frac{d}{c} \\ \frac{a}{c} & , x = -\frac{d}{c} \end{cases}$$

$$\sigma^{-1}(x) = \begin{cases} \frac{dx - b}{a - cx} & , x \neq \frac{a}{c} \\ -\frac{d}{c} & , x = \frac{a}{c} \end{cases}$$

Протокол ECDH

1. Пользователи, обозначаемые как A и B , умеют вычислять дискретные функции

$$f(x) = x * P,$$

$$g(x, f(y)) = g(y, f(x)) = (x \otimes y)P$$

в аддитивной циклической группе $\langle P \rangle$ порядка q точки P некоторой эллиптической кривой

$$E_{a,b}(p) = \{(x, y) \mid x, y \in \mathbb{Z}_p, y^2 = x^3 + ax + b\} \quad \text{над полем } \mathbb{Z}_p.$$

2. Стороны независимо генерируют случайные целые числа $1 < x, y < q$.

3. Вычисляют значения $f(x)$, $f(y)$.

4. Обмениваются ими по открытому каналу,

$$f(x) \leftrightarrow f(y),$$

5. Зная общие параметры аутентификации - пару чисел (k, m) ,
вычисляют общий секрет по формулам

$$K = g(x, f(y)) = g(y, f(x)) = (x \otimes y)P.$$

Протокол LM^2

Рассмотрим 8-мерную конечную алгебру гиперкомплексных чисел (октонионов) над конечным простым полем $\mathbb{Z}_p$. Её элементы имеют следующий вид:

$$\mathbb{O} = \{a + bi + cj + dk + el + fil + gjl + hkl \mid a, b, c, d, e, f, g, h \in \mathbb{Z}_p\}$$

Алгебра $\mathbb{O}$ не является группой и не обладает свойством ассоциативности, однако она формирует так называемую лупу Муфанг.

Мощность множества $\mathbb{O}$ равна p^8 , где p – модуль.

При небольших p получаем лупу Муфанг с большим количеством элементов

Соотношения в лупе Муфанг

$$z (x (zy)) = ((zx)z)y \quad (1)$$

$$x (z (yz)) = ((xz)y)z \quad (2)$$

$$(zx)(yz) = (z(xy))z \quad (3)$$

$$(zx)(yz) = z((xy)z) \quad (4)$$

Протокол LM^2

Пусть L — лупа Муфанг, известная обоим абонентам, $a, b, c \in L$ — известные элементы, M, K и N — порядки элементов a, b и c .

Протокол выработки секрета таков:

1. A выбирает случайные натуральные числа $m < M, k < K, n < N$ и посылает B пару $(u_1, u_2) = (a^m b^k, b^k c^n)$.
2. B выбирает случайные натуральные числа $r < M, l < K, s < N$ и посылает A пару $(v_1, v_2) = (a^r b^l, b^l c^s)$.

Протокол LM^2

3. A вычисляет $(a^m v_1) b^k$ и $(b^k v_2) c^n$.

4. B вычисляет $(a^r u_1) b^l$ и $(b^l u_2) c^s$.

Общий секрет пары (A, B) - элемент лупы Муфанг - вычисляется по формуле:

$$K_{AB} = (a^{m+r} b^{k+l})(b^{k+l} c^{n+s})$$

Протокол LM^2

3. A вычисляет $(a^m v_1) b^k$ и $(b^k v_2) c^n$.

4. B вычисляет $(a^r u_1) b^l$ и $(b^l u_2) c^s$.

Общий секрет пары (A, B) - элемент лупы Муфанг - вычисляется по формуле:

$$K_{AB} = (a^{m+r} b^{k+l})(b^{k+l} c^{n+s})$$

Протокол LM^2

Из свойств лупы Муфанг следуют равенства:

$$(a^m v_1) b^k = (a^m (a^r b^l)) b^k = (a^m a^r) (b^l b^k) = a^{m+r} b^{l+k}$$

$$(a^r u_1) b^l = (a^r (a^m b^k)) b^l = (a^r a^m) (b^k b^l) = a^{m+r} b^{l+k}$$

Следовательно,

$$(a^m v_1) b^k (b^k v_2) c^n = (a^r u_1) b^l (b^l u_2) c^s = K_{AB}$$

Литература

1. Лебедев А.Н., Новые арифметика конечного коммутативного кольца и ее использование в криптографии, Электронные Информационные Системы (ЭИС), 3(30) стр. 49-63, 2021, Москва, Зеленоград, Изд-во АО «НТЦ ЭЛИНС».
2. Лебедев А.Н., Кокорин А.О., Обобщение протокола Диффи - Хеллмана с использованием дробно-линейного преобразования, Электронные Информационные Системы (ЭИС), 3(30) стр. 64-71, 2021, Москва, Зеленоград, Изд-во АО «НТЦ ЭЛИНС».
3. Лебедев А.Н., Карондеев А.М., Козлов А.А., Блочный алгоритм защитного кодирования NASH, Электронные Информационные Системы (ЭИС), 4(31) стр. 30-39, 2021, Москва, Зеленоград, Изд-во АО «НТЦ ЭЛИНС».
4. Лебедев А.Н., Можно ли контролировать данные в чужих руках, Современные Информационные Системы, 3(17) стр. 46-49, 2021, Москва, Изд-во ООО «Совинтегра», www.cis.ru

Спасибо за внимание