что вместе с равенством $s = lm$ и условием $(l, q) = 1$ влечет сравнение $n \equiv m \pmod q$. Таким образом, приходим к сравнению $rp^{i-j} \equiv km \pmod q$, противоречащему выбору q.

5. Оставшийся случай, когда $s \neq 0$, $j \leqslant i$, $s = lm$ для некоторого целого числа m и $m = m_1 p^{i-j}$ для некоторого m_1, но $r \neq km_1$, рассматривается аналогично. Если простое число q выбрать отличным от p, взаимно простым с l и не делящим разности $r - km_1$ и снова положить $N = A^q B^q$, то предположение о справедливости включения $g \in HN$ повлечет сравнение $rp^{i-j} \equiv km_1 p^{i-j}$, равносильное сравнению $r \equiv km_1$. Предложение 4 доказано.

Таким образом, в силу предложений 1 и 4 группа G $\mathcal{F}_\pi$-аппроксимируема и любая ее π'-изолированная циклическая подгруппа $\mathcal{F}_\pi$-отделима. Вместе с тем прямой сомножитель A группы G обладает циклическими подгруппами, π'-изоляторы которых циклическими не являются.

Библиографический список

1. *Бардаков В. Г.* К вопросу Д. И. Молдаванского о p-отделимости подгрупп свободной группы // Сибирский математический журнал. 2004. Т. 45, № 3. С. 505—509.
2. Коуровская тетрадь. Нерешенные вопросы теории групп. 15-е изд. Новосибирск : Новосиб. гос. ун-т, 2002. 172 с.
3. *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М. : Наука, 1974. 455 с.
4. *Романовский Н. С.* О финитной аппроксимируемости свободных произведений относительно вхождения // Известия АН СССР. Сер. математическая. 1969. Т. 33, № 6. С. 1324—1329.
5. *Allenby R., Gregorac R.* On locally extended residually finite groups // Lecture Notes Math. 1973. Vol. 319. P. 9—17.
6. *Hall M.* Coset representations in free groups // Trans. Amer. Math. Soc. 1949. Vol. 67. P. 421—432.
7. *Meskin S.* Nonresidually finite one-relator groups // Trans. Amer. Math. Soc. 1972. Vol. 164. P. 105—114.
8. *Sokolov E. V.* On the cyclic subgroup separability of the free product of two groups with commuting subgroups // Int. J. Algebra Comput. 2014. Vol. 24, № 5. P. 741—756.
9. *Stebe P.* Residual finiteness of a class of knot groups // Comm. Pure Appl. Math. 1968. Vol. 21. P. 563—583.

УДК 519.688

Е. В. Соколов

АЛГОРИТМЫ ПОЛУЧЕНИЯ ОБЩЕГО СЕКРЕТНОГО КЛЮЧА, ИСПОЛЬЗУЮЩИЕ ГРУППЫ С ТОЖДЕСТВАМИ

Приводятся обобщения двух известных криптографических алгоритмов получения общего секретного ключа, использующие в качестве базовой произвольную группу, удовлетворяющую нетривиальному тождеству определенного вида.

Ключевые слова: криптография с открытым ключом, проблема поиска сопрягающего элемента, проблема поиска разложения элемента.

We obtain the generalizations of two known key agreement cryptographic protocols based on an arbitrary group satisfying certain nontrivial identity.

Key words: public-key cryptography, conjugacy search problem, decomposition search problem.

Пусть имеется некоторая группа G. Классическая *проблема сопряженности* для этой группы формулируется следующим образом: для заданных элементов g_1, $g_2 \in G$ определить, существует ли элемент x такой, что выполняется соотношение $g_1 = x^{-1}g_2x$. Наряду с проблемой сопряженности рассматривают и *проблему поиска сопрягающего элемента* (см., напр.: [1]): для заданных сопряженных элементов g_1, $g_2 \in G$ найти хотя бы один элемент x, удовлетворяющий условию $g_1 = x^{-1}g_2x$.

Если множество элементов группы G рекурсивно перечислимо и в G разрешима проблема равенства, то для отыскания сопрягающего элемента достаточно перечислять все элементы $x \in G$ и для каждого из них сравнивать элемент $x^{-1}g_2x$ с g_1. Рано или поздно элемент x, для которого выполняется равенство $g_1 = x^{-1}g_2x$, будет найден. Однако описанный алгоритм, как правило, имеет экспоненциальную сложность. Если неизвестно, существует ли другой, полиномиальный, алгоритм для решения проблемы поиска сопрягающего элемента, а операция сопряжения элемента группы G имеет полиномиальную сложность, то для заданного элемента $g \in G$ функция $f_g\colon G \to G$, переводящая элемент $x \in G$ в $x^{-1}gx$, оказывается односторонней: алгоритм вычисления $f_g(x)$ имеет полиномиальную сложность, в то время как алгоритм вычисления $f_g^{-1}(y)$ — экспоненциальную. Поэтому данная функция может применяться для построения криптографических протоколов.

Примером такого применения служит алгоритм получения общего секретного ключа, предложенный в [2]. Задача отыскания общего секрета состоит в том, чтобы два участника обмена информацией (обычно их называют Элис и Боб), пользуясь только открытыми (т. е. известными всем) данными и передавая информацию по открытым каналам связи, могли сгенерировать некоторый общий для них секрет (например, элемент группы), который никто другой за разумное время определить был бы не в состоянии.

Алгоритм 1 [2]. Имеются открытые группа G и элемент $g \in G$, а также множество S попарно перестановочных между собой элементов группы G.

Элис произвольным образом выбирает элемент $a \in S$ и передает Бобу элемент $g_1 = a^{-1}ga$. В то же время Боб выбирает элемент $b \in S$ и передает Элис элемент $g_2 = b^{-1}gb$. После этого Элис сопрягает принятый ею элемент g_2 при помощи известного только ей элемента a и получает элемент $a^{-1}(b^{-1}gb)a$. Боб действует аналогичным образом, сопрягая g_1 при помощи b и получая $b^{-1}(a^{-1}ga)b$. Так как элементы a и b были выбраны из множества S, они перестановочны, и потому

$$a^{-1}(b^{-1}gb)a = x = b^{-1}(a^{-1}ga)b$$

— общий секрет.

Потенциальному взломщику известны группа G, множество S и элементы g, g_1, g_2, но неизвестны элементы a и b, хотя бы один из которых

нужен для получения x из g_1 или g_2. Чтобы узнать a или b, и нужно решить проблему поиска сопрягающего элемента.

При практической реализации данного алгоритма определенные трудности вызывает выбор группы G, так как она должна обладать, с одной стороны, множеством S попарно перестановочных элементов достаточно большой мощности, а с другой — трудноразрешимой проблемой поиска сопрягающего элемента. Автором предложено обобщение описанного алгоритма, в котором множество S по-прежнему удовлетворяет нетривиальному тождеству, но оно уже необязательно является коммутатором. Так, например, данное обобщение может использовать в качестве базовой группу треугольных или унитреугольных матриц небольшой размерности над конечным полем.

Введем сначала ряд обозначений. Пусть w — некоторое слово в алфавите $\{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_l\}$. Максимальное (по включению) подслово слова w, состоящее только из символов $x_1, x_2, \ldots, x_k$, будем называть *x-слогом*, максимальное подслово, состоящее только из символов $y_1, y_2, \ldots, y_l$, — *y-слогом*. Количество слогов в слове w назовем его *слоговой длиной* (в отличие от обычной длины, равной количеству символов в слове w).

Далее будем считать, что слово w начинается с x-слога и имеет слоговую длину, кратную 4. Тогда w можно записать в виде произведения двух слов u и v равной слоговой длины:

$$w = uv, \quad u = u_1 u_2 \ldots u_{2n}, \quad v = v_1 v_2 \ldots v_{2n}.$$

При этом u_i и v_i являются x-слогами, если i — нечетно, и y-слогами в противном случае.

Алгоритм 2. Пусть имеются открытые группа G, фиксированный элемент $g \in G$ и подмножества $A_1, A_2, \ldots, A_k, B_1, B_2, \ldots, B_l$ элементов группы G, удовлетворяющие условию

$$\forall a_1 \in A_1,\, a_2 \in A_2,\, \ldots,\, a_k \in A_k,\, b_1 \in B_1,\, b_2 \in B_2,\, \ldots,\, b_l \in B_l$$
$$w(a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l) = 1.$$

0. Элис выбирает закрытые элементы $a_1 \in A_1, a_2 \in A_2, \ldots, a_k \in A_k$, Боб — закрытые элементы $b_1 \in B_1, b_2 \in B_2, \ldots, b_l \in B_l$.

1. Элис вычисляет и передает Бобу элемент

$$s_1 = u_1(\mathfrak{a}, \mathfrak{b})^{-1} g u_1(\mathfrak{a}, \mathfrak{b})$$

(здесь и далее кортежи

$$(a_1, a_2, \ldots, a_k) \quad \text{и} \quad (b_1, b_2, \ldots, b_l)$$

обозначены для краткости через $\mathfrak{a}$ и $\mathfrak{b}$).

2. Боб вычисляет и передает Элис элемент

$$t_{2n} = v_{2n}(\mathfrak{a}, \mathfrak{b}) g v_{2n}(\mathfrak{a}, \mathfrak{b})^{-1}.$$

3. Получив элемент t_{2m} $(1 \leqslant m \leqslant n)$, Элис вычисляет элемент

$$t_{2m-1} = v_{2m-1}(\mathfrak{a}, \mathfrak{b}) t_{2m} v_{2m-1}(\mathfrak{a}, \mathfrak{b})^{-1}$$

и, если $m \neq 1$, передает его Бобу.

4. Получив элемент s_{2m-1} $(1 \leqslant m \leqslant n)$, Боб вычисляет элемент

$$s_{2m} = u_{2m}(\mathfrak{a}, \mathfrak{b})^{-1} s_{2m-1} u_{2m}(\mathfrak{a}, \mathfrak{b})$$

и, если $m \neq n$, передает его Элис.

5. Получив элемент s_{2m} $(1 \leqslant m \leqslant n-1)$, Элис вычисляет и передает Бобу элемент

$$s_{2m+1} = u_{2m+1}(\mathfrak{a}, \mathfrak{b})^{-1} s_{2m} u_{2m+1}(\mathfrak{a}, \mathfrak{b}).$$

6. Получив элемент t_{2m-1} $(2 \leqslant m \leqslant n)$, Боб вычисляет и передает Элис элемент

$$t_{2m-2} = v_{2m-2}(\mathfrak{a}, \mathfrak{b}) t_{2m-1} v_{2m-2}(\mathfrak{a}, \mathfrak{b})^{-1}.$$

Можно заметить, что в процессе вычислений Элис, кроме полученных от Боба элементов, использует лишь слоги слов u и v с нечетными индексами, которые являются x-слогами и, значит, зависят только от $\mathfrak{a}$. Бобу, напротив, требуются лишь y-слоги, зависящие только от $\mathfrak{b}$. Таким образом, закрытая информация между Элис и Бобом не передается.

Алгоритм завершается, когда Элис вычислит элемент t_1, а Боб — элемент s_{2n}. При этом оказывается, что

$$s_{2n} = u(\mathfrak{a}, \mathfrak{b})^{-1} g u(\mathfrak{a}, \mathfrak{b}), \quad t_1 = v(\mathfrak{a}, \mathfrak{b}) g v(\mathfrak{a}, \mathfrak{b})^{-1}.$$

Далее необходимо вспомнить, что $w = uv$ и $w(\mathfrak{a}, \mathfrak{b}) = 1$ в силу выбора элементов a_i и b_j. Стало быть,

$$u(\mathfrak{a}, \mathfrak{b}) = v(\mathfrak{a}, \mathfrak{b})^{-1},$$

и потому $s_{2n} = t_1$. Это и есть общий секретный ключ.

Как и в алгоритме 1, для взлома необходимо определить либо элемент $u_{2n}(\mathfrak{a}, \mathfrak{b})$, либо элемент $v_1(\mathfrak{a}, \mathfrak{b})$. И то, и другое требует, по крайней мере, однократного решения проблемы поиска сопрягающего элемента.

Рассмотрим теперь еще одну алгоритмическую проблему, называемую *проблемой поиска разложения элемента* [1]: для заданных элементов g_1, $g_2 \in G$ и подмножеств A, $B \subseteq G$ найти элементы $a \in A$, $b \in B$, удовлетворяющие условию $g_1 = a g_2 b$, если известно, что хотя бы одна пара таких элементов существует. Алгоритм отыскания общего секретного ключа, основанный на сложности решения данной проблемы, предложен в [3] и формулируется следующим образом.

Алгоритм 3 [3]. Имеются открытые группа G и элемент $g \in G$, а также поэлементно перестановочные подмножества A, $B \subseteq G$.

Элис произвольным образом выбирает элементы $a_1 \in A$, $b_1 \in B$ и передает Бобу элемент $g_1 = a_1 g b_1$. Аналогично Боб выбирает элементы $a_2 \in A$, $b_2 \in B$ и передает Элис элемент $g_2 = b_2 g a_2$. После этого Элис вычисляет элемент $a_1 g_2 b_1 = a_1 b_2 g a_2 b_1$, Боб — элемент $b_2 g_1 a_2 = b_2 a_1 g b_1 a_2$. Поскольку $[a_1, b_2] = 1 = [a_2, b_1]$, указанные элементы равны и определяют общий секретный ключ.

Приведенный алгоритм также можно обобщить, отказавшись от требования поэлементной перестановочности подмножеств A и B.

Алгоритм 4. Пусть слова w, u, v, группа G, элемент $g \in G$ и подмножества A_1, A_2, …, A_k, B_1, B_2, …, $B_l \subseteq G$ удовлетворяют тем же ограничениям, что и в алгоритме 2.

0. Элис выбирает закрытые элементы

$$a_1 \in A_1,\ a_2 \in A_2,\ \ldots,\ a_k \in A_k,\ d_1 \in B_1,\ d_2 \in B_2,\ \ldots,\ d_l \in B_l,$$

Боб — закрытые элементы

$$b_1 \in B_1,\ b_2 \in B_2,\ \ldots,\ b_l \in B_l,\ c_1 \in A_1,\ c_2 \in A_2,\ \ldots,\ c_k \in A_k.$$

Кортежи $(a_1, a_2, \ldots, a_k)$, $(b_1, b_2, \ldots, b_l)$, $(c_1, c_2, \ldots, c_k)$ и $(d_1, d_2, \ldots, d_l)$ далее для краткости будем обозначать через $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ и $\mathfrak{d}$ соответственно.

1. Элис вычисляет и передает Бобу элемент

$$q_1 = u_1(\mathfrak{a}, \mathfrak{b})^{-1} g v_{2n}(\mathfrak{c}, \mathfrak{d})^{-1}.$$

2. Боб вычисляет и передает Элис элемент

$$r_1 = v_{2n}(\mathfrak{a}, \mathfrak{b}) g u_1(\mathfrak{c}, \mathfrak{d}).$$

3. Получив элемент r_{2m-1} $(1 \leqslant m \leqslant n)$, Элис вычисляет элемент

$$r_{2m} = v_{2n+1-2m}(\mathfrak{a}, \mathfrak{b}) r_{2m-1} u_{2m}(\mathfrak{c}, \mathfrak{d})$$

и, если $m \neq n$, передает его Бобу.

4. Получив элемент q_{2m-1} $(1 \leqslant m \leqslant n)$, Боб вычисляет элемент

$$q_{2m} = u_{2m}(\mathfrak{a}, \mathfrak{b})^{-1} q_{2m-1} v_{2n+1-2m}(\mathfrak{c}, \mathfrak{d})^{-1}$$

и, если $m \neq n$, передает его Элис.

5. Получив элемент q_{2m} $(1 \leqslant m \leqslant n-1)$, Элис вычисляет и передает Бобу элемент

$$q_{2m+1} = u_{2m+1}(\mathfrak{a}, \mathfrak{b})^{-1} q_{2m} v_{2n-2m}(\mathfrak{c}, \mathfrak{d})^{-1}.$$

6. Получив элемент r_{2m} $(1 \leqslant m \leqslant n-1)$, Боб вычисляет и передает Элис элемент

$$r_{2m+1} = v_{2n-2m}(\mathfrak{a}, \mathfrak{b}) r_{2m} u_{2m+1}(\mathfrak{c}, \mathfrak{d}).$$

Снова заметим, что в процессе вычислений Элис использует лишь x-слоги слов $u(\mathfrak{a}, \mathfrak{b})$, $v(\mathfrak{a}, \mathfrak{b})$ и y-слоги слов $u(\mathfrak{c}, \mathfrak{d})$, $v(\mathfrak{c}, \mathfrak{d})$, которые зависят только от $\mathfrak{a}$ и $\mathfrak{d}$ соответственно. Аналогично Бобу требуются y-слоги слов $u(\mathfrak{a}, \mathfrak{b})$, $v(\mathfrak{a}, \mathfrak{b})$ и x-слоги слов $u(\mathfrak{c}, \mathfrak{d})$, $v(\mathfrak{c}, \mathfrak{d})$, зависящие от $\mathfrak{b}$ и $\mathfrak{c}$.

Алгоритм завершается, когда Элис вычислит элемент r_{2n}, Боб — элемент q_{2n}. Так как

$$q_{2n} = u(\mathfrak{a}, \mathfrak{b})^{-1} g v(\mathfrak{c}, \mathfrak{d})^{-1}, \quad r_{2n} = v(\mathfrak{a}, \mathfrak{b}) g u(\mathfrak{c}, \mathfrak{d}),$$
$$u(\mathfrak{a}, \mathfrak{b}) = v(\mathfrak{a}, \mathfrak{b})^{-1}, \quad u(\mathfrak{c}, \mathfrak{d}) = v(\mathfrak{c}, \mathfrak{d})^{-1},$$

то $q_{2n} = r_{2n}$ — общий секретный ключ, что и требовалось.

Библиографический список

1. *Myasnikov A., Shpilrain V., Ushakov A.* Group-Based Cryptography. Basel : Birkhäuser Verlag, 2008. 183 p.
2. New public-key cryptosystem using braid groups / K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park // Advances in Cryptology — CRYPTO 2000. Berlin : Springer, 2000. P. 166—183. (Lecture Notes in Computer Sciences ; iss. 1880).
3. *Shpilrain V., Ushakov A.* Thomson's group and public key cryptography // Applied Cryptography and Network Security — ACNS 2005. Berlin : Springer, 2005. P. 151—164. (Lecture Notes in Computer Sciences ; iss. 3531).