УДК 681.3

ПРИМИТИВЫ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ: КОНЕЧНЫЕ НЕКОММУТАТИВНЫЕ ГРУППЫ ЧЕТЫРЕХМЕРНЫХ ВЕКТОРОВ

***Д. Н. Молдовян*[1],**
младший научный сотрудник
Санкт-Петербургский институт информатики и автоматизации РАН

Для синтеза производительных алгоритмов распределения открытых ключей и открытого шифрования вводится новая вычислительно трудная задача над конечными некоммутативными группами. Предложен подход к построению некоммутативных групп четырехмерных векторов над простым полем и выводится формула для порядка этих групп. Описана схема согласования общего секретного ключа двух удаленных абонентов и алгоритм открытого шифрования на основе новой трудной задачи.

Ключевые слова *— криптография, криптосистемы с открытым ключом, протокол открытого согласования ключа, открытое шифрование, конечные группы, некоммутативные группы, группы векторов, трудная задача.*

Введение

В последние годы возрос интерес к использованию некоммутативных групп в качестве примитивов криптосистем с открытым ключом [1], связанный с ожиданием разработки действующего квантового компьютера, с применением которого задачи факторизации и дискретного логарифмирования в циклической группе будут решаться за полиномиальное время [2]. Последнее означает, что все наиболее широко применяемые алгоритмы открытого распределения ключей, открытого шифрования и электронной цифровой подписи (ЭЦП) станут небезопасными, поскольку их стойкость основана на сверхполиномиальной сложности указанных двух задач при их решении на имеющихся в настоящее время компьютерах. «Постквантовая» криптография связана с использованием новых трудных задач, сложность которых была бы сверхполиномиальна и в случае применения квантового вычислителя. В работах [3, 4] такие задачи сформулированы над бесконечными некоммутативными группами переплетения, а затем применены для построения алгоритмов открытого шифрования [4] и ЭЦП [5].

В данной статье формулируется новая вычислительно трудная задача над конечными некоммутативными группами, рассматривается построение на ее основе алгоритмов открытого согласования общего секретного ключа двух удаленных абонентов и открытого шифрования, описывается подход к заданию конечных некоммутативных групп четырехмерных векторов и выводится формула для вычисления порядка таких групп.

Криптосхемы с открытым ключом на основе конечных некоммутативных групп

Одним из способов синтеза криптосистем с открытым ключом на основе некоммутативных конечных групп является использование их подгрупп, обладающих достаточно большим простым порядком. Такие подгруппы являются циклическими, а групповая операция в них коммутативна. В этом случае синтез криптосхем, основанных на сложности задачи дискретного логарифмирования, аналогичен синтезу в случае коммутативных групп. Обоснованием данного подхода является ожидание, что сведение задачи дискретного логарифмирования в циклической подгруппе некоммутативной группы к задаче дискретного логарифмирования в конечном поле или конечном кольце многочленов будет невозможно. В частных случаях такое сведение возможно, поэтому требуется выполнить выбор подгрупп, об-

[1] Научный руководитель — доктор технических наук, профессор, заместитель директора по научной работе СПИИРАН *Б. В. Соколов*.

ладающих соответствующим значением простого порядка [6].

Более интересным является подход, использующий задачу вычисления элемента некоммутативной группы X и числа x (пара этих элементов служит секретным ключом) в уравнении $Y = X \circ G^x \circ X^{-1}$, где Y — элемент группы, используемый в качестве открытого ключа; G — элемент достаточно большого простого порядка q (элементы Y и G считаются известными); X — элемент, для которого выполняются неравенства $X \circ G \neq G \circ X$ и $Y \circ G \neq G \circ Y$ (при заданном числе x значение элемента X определяет значение Y). Операции умножения на взаимно обратные элементы X и X^{-1} реализуют операцию автоморфизма [7]. Решение указанного выше уравнения представляет собой самостоятельную трудную вычислительную задачу, отличную от задачи дискретного логарифмирования. При известном X можно вычислить $Y' = X^{-1} \circ Y \circ X$ или $G' = X \circ G \circ X^{-1}$, после чего число x можно найти из уравнения $Y' = G^x$ или $Y = G'^{\,x}$ соответственно, т. е. решая задачу дискретного логарифмирования. Однако значение X является неизвестным, поэтому задача дискретного логарифмирования в циклической подгруппе не стоит. Можно ожидать, что в конечной некоммутативной группе при известном x сравнительно легко вычислить неизвестный элемент X, однако одновременное нахождение X и x является сложной задачей, несмотря на то, что существует очень большое число различных решений (если X и x — некоторое решение, то для произвольного элемента группы θ, коммутирующего со всеми другими элементами, пара $(\theta X, x)$ также является решением).

Схема открытого согласования ключа на основе предлагаемой задачи описывается следующим образом. Пусть два удаленных абонента имеют открытые ключи $Y_1 = X_1 \circ G^{x_1} \circ X_1^{-1}$ и $Y_2 = X_2 \circ G^{x_2} \circ X_2^{-1}$, где (X_1, x_1) и (X_2, x_2) — личные секретные ключи первого и второго абонентов такие, что $X_1 \circ X_2 = X_2 \circ X_1$. После открытого обмена открытыми ключами первый абонент вычисляет общий секретный ключ по формуле $K_{12} = X_1 \circ Y_2^{x_1} \circ X_1^{-1}$, а второй — по формуле $K_{21} = X_2 \circ Y_1^{x_2} \circ X_2^{-1} = K_{12}$. Комбинируя аналогичным образом операцию автоморфизма и операцию возведения в большую дискретную степень, можно построить алгоритмы коммутативного и открытого шифрования. Техническим вопросом является согласование выбора секретных значений X_1 и X_2 из одной и той же коммутативной подгруппы, который решается заданием дополнительного известного элемента Q такого, что $Q \circ G \neq G \circ Q$, также обладающего большим простым порядком. В этом случае открытые ключи вычисляются по формулам

$$Y_1 = Q^{w_1} \circ G^{x_1} \circ Q^{-w_1} \text{ и } Y_2 = Q^{w_2} \circ G^{x_2} \circ Q^{-w_2},$$

где пары (w_1, x_1) и (w_2, x_2) являются личным секретным ключом первого и второго абонентов соответственно. В случае, когда порядки элементов Q и G равны большому простому числу q, имеющему размер $|q|$ бит, вычисление пары неизвестных (w, x) может быть выполнено методом, аналогичным методу больших и малых шагов [8], с трудоемкостью $2^{|q|}$ операций возведения в степень. Из этой оценки следует, что рассмотренная схема открытого согласования ключа имеет приемлемую для практического применения криптостойкость при $q \geq 2^{80}$.

Алгоритм открытого шифрования можно построить по следующей схеме. Пусть некоторый пользователь желает послать секретное сообщение M владельцу открытого ключа $Y = Q^w \circ G^x \circ Q^{-w}$, где (w, x) — личный секретный ключ получателя сообщения. Отправитель сообщения формирует разовый личный секретный ключ в виде пары чисел (u, v), вычисляет разовый открытый ключ $R = Q^u \circ G^v \circ Q^{-u}$, вычисляет разовый общий секретный ключ $K = Q^u \circ Y^v \circ Q^{-u}$, по ключу K зашифровывает сообщение и отправляет разовый открытый ключ и зашифрованное сообщение получателю. Получатель по разовому открытому ключу R вычисляет разовый общий секретный ключ $K = Q^w \circ R^x \circ Q^{-w}$, затем по ключу K расшифровывает сообщение M. Пусть в данной схеме используется алгоритм шифрования, представленный функцией шифрования E_K, управляемой секретным ключом в виде элемента некоммутативной группы K. Тогда описанная выше схема реализуется следующим алгоритмом.

1. Отправитель генерирует пару случайных чисел (u, v), вычисляет элементы $R = Q^u \circ G^v \circ Q^{-u}$ и $K = Q^u \circ Y^v \circ Q^{-u}$ некоммутативной группы, где Y — открытый ключ получателя.

2. Используя значение K в качестве ключа шифрования, отправитель зашифровывает сообщение M: $C = E_K(M)$.

3. Отправитель направляет получателю криптограмму C и значение R.

4. Получатель вычисляет значение $K' = Q^w \circ R^x \circ Q^{-w} = K$, где (w, x) — личный секретный ключ получателя, и расшифровывает криптограмму C: $M = D_K(C)$, где D_K — функция расшифрования, обратная E_K.

В описанных выше криптосхемах используется отображение циклической подгруппы Γ_G, порождаемой элементом G в некоторую другую (скрытую) циклическую подгруппу того же простого порядка q, задаваемого отображением $\varphi_X(G^i) = X \circ G^i \circ X^{-1}$, где $i = 1, 2, \ldots, q$, которое является автоморфизмом рассматриваемой конечной некоммутативной группы. При этом элемент X за-

дается в виде $X = Q^w$. Возникает вопрос о различии циклических подгрупп, в которые отображается подгруппа Γ_G при различных значениях $1 \le w \le q'$, где q' — порядок элемента Q. Ответ на этот вопрос дает следующая теорема.

Теорема 1. Пусть G и Q — элементы некоммутативной группы, имеющие простые порядки q и q' соответственно, такие, что $Q \circ G \ne G \circ Q$ и $Z \circ G \ne G \circ Z$, где $Z = Q \circ G \circ Q^{-1}$. Тогда все элементы $Z_{ij} = Q^j \circ G^i \circ Q^{-j}$, где $i = 1, 2, ..., q - 1$ и $j = 1, 2, ..., q'$, попарно различны.

Доказательство: Очевидно, что при фиксированном j элементы $Z_{ij} = Q^j \circ G^i \circ Q^{-j}$, где $i = 1, 2, ..., q$, образуют циклическую подгруппу порядка q. Условие $Z \circ G \ne G \circ Z$ означает, что элемент Z не принадлежит подгруппе Γ_G, порождаемой степенями элемента G (при предположении противного легко устанавливается противоречие). Пусть при некоторых i, $i' \ne i$, j и $j' \ne j$ (для определенности положим $j' > j$) элементы $Z_j = Q^j \circ G^i \circ Q^{-j}$ и $Z_{j'} = Q^{j'} \circ G^{i'} \circ Q^{-j'}$ равны, т. е. $Q^j \circ G^i \circ Q^{-j} = Q^{j'} \circ G^{i'} \circ Q^{-j'}$. Умножая обе части последнего выражения справа на Q^j и слева на Q^{-j}, получаем $G^i = Q^{j'-j} \circ G^{i'} \circ Q^{-j'+j}$. Так как Γ_G есть подгруппа простого порядка q, то любой неединичный элемент подгруппы Γ_G является порождающим, т. е. при $1 \le i' \le q - 1$ элемент $P = G^{i'}$ является порождающим, а значит степени P^z ($z = 1, 2, ..., q$) пробегают все элементы подгруппы Γ_G. При этом для всех z имеет место соотношение

$$(G^i)^z = (Q^{j'-j} \circ P \circ Q^{-j'+j})^z = Q^{j'-j} \circ P^z \circ Q^{-j'+j} \in \Gamma_G,$$

т. е. отображение $\varphi_{Q^{j'-j}}(P^z) = Q^{j'-j} \circ P^z \circ Q^{-j'+j}$ переводит любой элемент подгруппы Γ_G в некоторый элемент этой же подгруппы. Это означает, что отображение $\varphi_{Q^{j'-j}}(\Gamma_G)$ отображает подгруппу Γ_G в себя. Рассмотрим отображение $\varphi_Q(\Gamma_G)$. Поскольку порядок элемента Q есть простое число q', то для $j' \ne j$ существует некоторое число $u = (j'-j)^{-1} \bmod q'$, для которого имеют место соотношения

$$Q = (Q^{j'-j})^u$$

и

$$\varphi_Q(\Gamma_G) = \varphi_{(Q^{j'-j})^u}(\Gamma_G) = \\ = \varphi_{Q^{j'-j}}(\varphi_{Q^{j'-j}}(...\varphi_{Q^{j'-j}}(\Gamma_G)...)),$$

где в правой части последнего выражения выполняется u последовательных отображений $\varphi_{Q^{j'-j}}(\Gamma_G)$. Так как $\varphi_{Q^{j'-j}}(\Gamma_G)$ — это отображение подгруппы Γ_G в себя, то u таких отображений также переводит подгруппу Γ_G в себя, т. е. $Z = \varphi_Q(G) = Q \circ G \circ Q^{-1} \in \Gamma_G$. Из сделанного предположения вытекает, что элемент Z принадлежит циклической подгруппе, порождаемой элементом G, следовательно, для элементов Z и G должно выполняться свойство коммутативности, т. е. $Z \circ G = G \circ Z$, однако это противоречит условию $Z \circ G \ne G \circ Z$ теоремы. Полученное противоречие доказывает теорему.

В соответствии с теоремой 1 число различных неединичных элементов Z_{ij} составляет $(q - 1)q'$, и они образуют вместе с единичным элементом N подгрупп простого порядка q, где $N = q'$, причем каждый неединичный элемент принадлежит только одной из этих подгрупп.

Построение конечных некоммутативных групп четырехмерных векторов

Рассмотрим множество векторов вида $(a, b, c, d) = a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, где $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$ и $\mathbf{k}$ — формальные базисные векторы; a, b, c и d – целые числа, называемые координатами и принадлежащие конечному простому полю $GF(p)$, где p — простое число. Выражения $a\mathbf{e}$, $b\mathbf{i}$, $c\mathbf{j}$ и $d\mathbf{k}$ обозначают векторы $(a, 0, 0, 0)$, $(0, b, 0, 0)$, $(0, 0, c, 0)$ и $(0, 0, 0, d)$ соответственно и называются компонентами вектора (a, b, c, d). Определим операцию сложения векторов как сложение одноименных координат: $(a, b, c, d) + (x, y, z, w) = (a + x, b + y, c + z, d + w)$, где знак «+» применен для обозначения двух разных операций — сложения элементов поля $GF(p)$ и сложения векторов, что не вносит неопределенности ввиду очевидности интерпретации знака в каждом случае его применения. Операцию умножения векторов $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ и $x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$ определим по правилу «умножения многочленов»:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = \\ = ax\mathbf{e} \circ \mathbf{e} + ay\mathbf{e} \circ \mathbf{i} + az\mathbf{e} \circ \mathbf{j} + aw\mathbf{e} \circ \mathbf{k} + bx\mathbf{i} \circ \mathbf{e} + \\ + by\mathbf{i} \circ \mathbf{i} + bz\mathbf{i} \circ \mathbf{j} + bw\mathbf{i} \circ \mathbf{k} + cx\mathbf{j} \circ \mathbf{e} + cy\mathbf{j} \circ \mathbf{i} + \\ + cz\mathbf{j} \circ \mathbf{j} + cw\mathbf{j} \circ \mathbf{k} + dx\mathbf{k} \circ \mathbf{e} + dy\mathbf{k} \circ \mathbf{i} + \\ + dz\mathbf{k} \circ \mathbf{j} + dw\mathbf{k} \circ \mathbf{k},$$

где координаты вектора умножаются как элементы поля $GF(p)$, а операция $\circ$ имеет более высокий приоритет по сравнению со сложением, а произведения всевозможных пар базисных векторов заменяются базисным вектором или однокомпонентным вектором в соответствии с правилом умножения, задаваемым табл. 1, в которой пара-

■ **Таблица 1.** *Правила умножения четырехмерных базисных векторов ($\varepsilon < p$)*

Базисный вектор	Базисный вектор			
	e	**i**	**j**	**k**
e	**e**	**i**	**j**	**k**
i	**i**	$-\varepsilon\mathbf{e}$	$\varepsilon\mathbf{k}$	$-\mathbf{j}$
j	**j**	$-\varepsilon\mathbf{k}$	$-\varepsilon\mathbf{e}$	**i**
k	**k**	**j**	$-\mathbf{i}$	$-\mathbf{e}$

метр $\varepsilon \in GF(p)$ называется структурным коэффициентом. Различным значениям ε соответствуют формально различные операции умножения векторов. Определенная таким способом операция умножение векторов (a, b, c, d) и (x, y, z, w) выполняется по правилу

$$(a, b, c, d) \circ (x, y, z, w) = \\ = (ax - \varepsilon by - \varepsilon cz - dw)\mathbf{e} + (bx + ay - dz + cw)\mathbf{i} + \\ + (cx + dy + az - bw)\mathbf{j} + (dx - \varepsilon cy + \varepsilon bz + aw)\mathbf{k}.$$

Легко проверить, что определенная операция умножения обладает свойством ассоциативности и в общем случае является некоммутативной. Нейтральным элементом по умножению является вектор $E = (1, 0, 0, 0)$.

Множество всех векторов $\{A\}$ такое, что каждому вектору A может быть сопоставлен обратный вектор A^{-1}, для которого выполняется соотношение $AA^{-1} = E$, образует конечную группу. Для вычисления порядка Ω построенной некоммутативной группы рассмотрим решение уравнения вида $AX = E$, которое можно представить следующим образом:

$$(a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \circ (x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}) = \\ = (ax - \varepsilon by - \varepsilon cz - dw)\mathbf{e} + \\ + (bx + ay - dz + cw)\mathbf{i} + (cx + dy + az - bw)\mathbf{j} + \\ + (dx - \varepsilon cy + \varepsilon bz + aw)\mathbf{k} = 1\mathbf{e} + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}.$$

Из последней записи вытекает, что для определения обратных значений следует решать следующую систему из четырех линейных сравнений с четырьмя неизвестными:

$$\begin{cases} ax - \varepsilon by - \varepsilon cz - dw \equiv 1 \bmod p \\ bx + ay - dz + cw \equiv 0 \bmod p \\ cx + dy + az - bw \equiv 0 \bmod p \\ dx - \varepsilon cy + \varepsilon bz + aw \equiv 0 \bmod p \end{cases}. \qquad (1)$$

Если главный определитель $\Delta(A)$ системы (1) не равен нулю, то существует решение, которое дает значение координат вектора, являющегося обратным к вектору $A = (a, b, c, d)$. Если $\Delta(A) = 0$, то вектор A необратим. Значение Ω определим как число всех четырехмерных векторов, равное p^4, за вычетом числа необратимых векторов. Запишем значение определителя $\Delta(A)$:

$$\Delta(A) = \begin{vmatrix} a & -\varepsilon b & -\varepsilon c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -\varepsilon c & \varepsilon b & a \end{vmatrix} = a \begin{vmatrix} a & -d & c \\ d & a & -b \\ -\varepsilon c & \varepsilon b & a \end{vmatrix} + \\ + \varepsilon b \begin{vmatrix} b & -d & c \\ c & a & -b \\ d & \varepsilon b & a \end{vmatrix} - \varepsilon c \begin{vmatrix} b & a & c \\ c & d & -b \\ d & -\varepsilon c & a \end{vmatrix} + d \begin{vmatrix} b & a & -d \\ c & d & a \\ d & -\varepsilon c & \varepsilon b \end{vmatrix}.$$

Четыре слагаемых в правой части последнего выражения содержат одинаковый множитель:

$$a \begin{vmatrix} a & -d & c \\ d & a & -b \\ -\varepsilon c & \varepsilon b & a \end{vmatrix} = a(a(a^2 + \varepsilon b^2) + d(ad - \varepsilon bc) + \\ + c(\varepsilon bd + \varepsilon ac)) = a^2(a^2 + \varepsilon b^2 + \varepsilon c^2 + d^2);$$

$$\varepsilon b \begin{vmatrix} b & -d & c \\ c & a & -b \\ d & \varepsilon b & a \end{vmatrix} = \varepsilon b(b(a^2 + \varepsilon b^2) + d(ac + bd) + \\ + c(\varepsilon bc - ad)) = \varepsilon b^2(a^2 + \varepsilon b^2 + \varepsilon c^2 + d^2);$$

$$-\varepsilon c \begin{vmatrix} b & a & c \\ c & d & -b \\ d & -\varepsilon c & a \end{vmatrix} = -\varepsilon c(b(ad - \varepsilon bc) - a(ac + bd) + \\ + c(-\varepsilon c^2 - d^2)) = \varepsilon c^2(a^2 + \varepsilon b^2 + \varepsilon c^2 + d^2);$$

$$d \begin{vmatrix} b & a & -d \\ c & d & a \\ d & -\varepsilon c & \varepsilon b \end{vmatrix} = d(b(\varepsilon bd + \varepsilon ac) - a(\varepsilon bc + ad) - \\ - d(-\varepsilon c^2 - d^2)) = d^2(a^2 + \varepsilon b^2 + \varepsilon c^2 + d^2).$$

Складывая правые части последних четырех выражений, получаем

$$\Delta(A) = (a^2 + \varepsilon b^2 + \varepsilon c^2 + d^2)^2,$$

откуда следует, что число необратимых векторов равно числу решений сравнения

$$a^2 + \varepsilon b^2 + \varepsilon c^2 + d^2 \equiv 0 \bmod p \qquad (2)$$

относительно неизвестных (a, b, c, d). Рассмотрим следующее утверждение.

Утверждение 1. Пусть простое число p представляется в виде $p = 4k + 1$ **при некотором натуральном** $k \geq 1$. Тогда число решений сравнения (2) равно $p^3 + p^2 - p$ при произвольных значениях $1 \leq \varepsilon \leq p - 1$.

Доказательство: Для рассматриваемых значений простого числа p число -1 является квадратичным вычетом. Действительно, в соответствии с критерием Эйлера имеем $(-1)^{(p-1)/2} = (-1)^{2k} \equiv 1 \bmod p$. Следовательно, существует квадратный корень из -1, т. е. для некоторого целого числа $\lambda < p - 1$ имеем $\lambda^2 \equiv -1 \bmod p$. Перепишем сравнение (2) в тождественном виде:

$$a^2 - (\lambda d)^2 \equiv -\varepsilon(b^2 + c^2) \bmod p;$$

$$(a + \lambda d)(a - \lambda d) \equiv -\varepsilon(b^2 + c^2) \bmod p;$$

$$\alpha\delta \equiv -\varepsilon(b^2 + c^2) \bmod p, \qquad (3)$$

где $\alpha \equiv a + \lambda d \bmod p$; $\delta \equiv a - \lambda d \bmod p$; $0 \le \alpha \le p-1$ и $0 \le \delta \le p-1$. **Легко видеть, что между множеством пар** (α, δ) и множеством пар (a, d) существует взаимно однозначное соответствие, следовательно, число решений сравнения (3) относительно неизвестных (α, b, c, δ) равно числу решений сравнения (2) относительно неизвестных (a, b, c, d). Подсчитаем число решений сравнения (3). Если $\tau = b^2 + c^2 \ne 0 \bmod p$, то $\alpha \ne 0$ и $\delta \ne 0$. **Сравнение** $b^2 + c^2 \equiv 0 \bmod p$ имеет $2p-1$ **решений относительно неизвестных** b и c: одно решение имеет вид $(b, c) = (0, 0)$ и $2(p-1)$ решений имеют вид $(b, c) = (\pm\lambda c, c)$, где $1 \le c \le p-1$. Для каждого значения $\tau \ne 0$ (это имеет место для $N_{bc} = p^2 - 2p + 1$ различных пар значений b и c) и каждого значения $\alpha \ne 0$ (число различных значений α равно $N_\alpha = p-1$) **существует** единственное δ, удовлетворяющее сравнению (3), т. е. случаю $\tau \ne 0$ соответствуют $N_{\tau \ne 0} = N_{bc}N_\alpha = (p-1)^3$ различных решений сравнения (3). Каждому из $2p-1$ вариантов пар значений b и c, при которых имеет место случай $\tau = 0$, **соответствуют** $p-1$ различных решений, образуемых парами значений $\alpha = 0$ и $\delta \ne 0$ плюс $p-1$ **различных решений**, образуемых парами значений $\alpha \ne 0$ и $\delta = 0$ плюс решение $(\alpha, \delta) = (0, 0)$, т. е. значению $\tau = 0$ соответствуют $N_{\tau = 0} = (2p-1)^2$ различных решений сравнения (3). Таким образом, число различных решений сравнения (3), а значит и сравнения (2), равно

$$N_{\tau \ne 0} + N_{\tau = 0} = (p-1)^3 + (2p-1)^2 = p^3 + p^2 - p,$$

что и требовалось доказать.

Утверждение 2. Пусть простое число p представляется в виде $p = 4k + 1$ **при некотором натуральном** $k \ge 1$. Тогда порядок некоммутативной группы четырехмерных векторов, групповая операция которой задана по табл. 1, равен $\Omega = p(p-1) \times (p^2-1)$.

Доказательство: Число всех различных четырехмерных векторов над простым полем характеристики p равно $N = p^4$. В соответствии с утверждением 1 число необратимых векторов равно $N' = p^3 + p^2 - p$. Порядок группы равен числу обратимых векторов $\Omega = N - N' = p^4 - p^3 - p^2 + p = p(p^2(p-1) - (p-1)) = p(p-1)(p^2-1)$, **что требовалось доказать.**

Утверждение 3. При $\varepsilon = 0$ порядок некоммутативной группы четырехмерных векторов равен $\Omega = p^2(p^2-1)$, если простое число p представляется в виде $p = 4k + 3$, или $\Omega = p^2(p-1)^2$, если простое число p представляется в виде $p = 4k + 1$.

Доказательство: При $\varepsilon = 0$ определитель системы сравнений (1), из которой вычисляются координаты обратного вектора, равен $\Delta(A) \equiv a^2 + d^2 \bmod p$. Для значений простого числа p, представимых в виде $p = 4k + 3$, число -1 является квадратичным невычетом. Действительно, в соответствии с критерием Эйлера имеем $(-1)^{(p-1)/2} = (-1)^{2k+1} \equiv -1 \bmod p$. Следовательно, не существует квадратный корень из -1, поэтому сравнение $a^2 + d^2 \equiv 0 \bmod p$ имеет решение только при $(a, d) = (0, 0)$, т. е. все векторы вида $(0, b, c, 0)$ являются необратимыми. Число таких векторов равно p^2. В рассмотренном случае порядок группы векторов равен $\Omega = p^4 - p^2 = p^2(p^2-1)$. **Для значений простого числа** p, представимых в виде $p = 4k + 1$, число -1 является квадратичным вычетом, поэтому сравнение $a^2 + d^2 \equiv 0 \bmod p$ имеет $2p-1$ различных решений (см. доказательство утверждения 1), которым соответствуют необратимые векторы вида $(\pm(-d)^{1/2}, b, c, d)$, где b и c — произвольные значения. Число необратимых векторов равно $p^2(2p-1)$. В этом случае порядок группы векторов равен $\Omega = p^4 - p^2(2p-1) = p^2(p-1)^2$. Утверждение 3 доказано.

Утверждение 4. Пусть простое число p представляется в виде $p = 4k + 3$ **при некотором натуральном** $k \ge 1$. **Тогда если структурный коэффициент** ε является квадратичным невычетом, то порядок некоммутативной группы четырехмерных векторов, групповая операция которой задана по табл. 1, равен $\Omega = p(p-1)(p^2-1)$.

Доказательство: Для рассматриваемых значений простого числа p число -1 является квадратичным невычетом. Действительно, в соответствии с критерием Эйлера имеем $(-1)^{(p-1)/2} = (-1)^{2k+1} \equiv -1 \bmod p$. Поскольку ε – квадратичный невычет, то $\varepsilon^{(p-1)/2} \equiv -1 \bmod p$ и $(-\varepsilon)^{(p-1)/2} \equiv 1 \bmod p$. Следовательно, число $-\varepsilon$ является квадратичным вычетом и существует квадратный корень из $-\varepsilon$, т. е. для некоторого целого числа $\lambda < p-1$ имеем $\lambda^2 \equiv -\varepsilon \bmod p$. Перепишем сравнение (2) в тождественном виде:

$$a^2 - (\lambda b)^2 \equiv -(d^2 - (\lambda c)^2) \bmod p;$$

$$(a + \lambda b)(a - \lambda b) \equiv -(d^2 - (\lambda c)^2) \bmod p;$$

$$\alpha\delta \equiv -(d^2 - (\lambda c)^2) \bmod p, \qquad (4)$$

где $\alpha \equiv a + \lambda b \bmod p$; $\delta \equiv a - \lambda b \bmod p$; $0 \le \alpha \le p-1$ и $0 \le \delta \le p-1$. **Подсчитаем число решений сравнения** (4) относительно неизвестных (a, b, c, d) аналогично тому, как это сделано в доказательстве утверждения 1. Если $\tau = d^2 - (\lambda c)^2 \ne 0 \bmod p$, то $\alpha \ne 0$ и $\delta \ne 0$. Сравнение $d^2 - (\lambda c)^2 \equiv 0 \bmod p$ имеет $2p-1$ решений относительно неизвестных c и d: одно решение имеет вид $(c, d) = (0, 0)$ и $2(p-1)$ **решений** имеют вид $(c, d) = (c, \pm\lambda c)$, где $1 \le c \le p-1$. Для каждого значения $\tau \ne 0$ (это имеет место для $N_{bc} = p^2 - 2p + 1$ различных пар значений c и d) и $\alpha \ne 0$ ($N_\alpha = p-1$ различных значений α) суще-

ствует единственное δ, удовлетворяющее сравнению (4), т. е. случаю $\tau \neq 0$ соответствуют $N_{\tau \neq 0} = N_{bc}N_{\alpha} = (p-1)^3$ различных решений сравнения (4). Каждому из $2p-1$ вариантов пар значений c и d, при которых имеет место случай $\tau = 0$, соответствуют $p-1$ различных решений, образуемых парой значений $\alpha = 0$ и $\delta \neq 0$ плюс $p-1$ различных решений, образуемых парой значений $\alpha \neq 0$ и $\delta = 0$ плюс решение $(\alpha, \delta) = (0, 0)$, т. е. случаю $\tau = 0$ соответствуют $N_{\tau = 0} = (2p-1)^2$ различных решений сравнения (4). Таким образом, число различных решений сравнения (4), а значит и сравнения (2), равно

$$N' = N_{\tau \neq 0} + N_{\tau = 0} = \\ = (p-1)^3 + (2p-1)^2 = p^3 + p^2 - p.$$

Число всех различных четырехмерных векторов равно $N = p^4$. Порядок Ω группы равен числу обратимых векторов, следовательно:

$$\Omega = N - N' = p^4 - p^3 - p^2 + p = p(p-1)(p^2-1),$$

что и требовалось доказать.

Экспериментальные результаты

Доказанные выше утверждения о порядке конечной некоммутативной группы четырехмерных векторов для различных значений p и ε были проверены экспериментально с помощью компьютерной программы, реализующей алгоритм вычисления строения группы (под строением группы понимается таблица, показывающая число векторов для каждого возможного значения их порядка). Типичные результаты, полученные в ходе вычислительного эксперимента, который подтвердил доказанные в предыдущем разделе утверждения, показывает табл. 2. Эксперимент также показал, что в утверждении 4 требование того, что структурный коэффициент является квадратичным невычетом, может быть удалено, т. е. во всех экспериментах порядок конечной некоммутативной группы четырехмерных векторов оказался равным $\Omega = p(p-1)(p^2-1)$ независимо от структуры простого числа p и значения коэффициента $\varepsilon \neq 0$.

Рассмотрим пример выбора простых чисел p, q, q' и векторов G и Q, удовлетворяющих условиям $Q \circ G \neq G \circ Q$ и $Z \circ G \neq G \circ Z$, где $Z = Q \circ G \circ Q^{-1}$, и $q = q'$, $|q| \approx |p|$, где $|q|$ ($|p|$) — длина двоичной записи числа q (p):

$$p = 751788397;\ q = q' = (p+1)/2 = \\ = 375894199;\ \varepsilon = 1;$$

$$G = (493205368, 605223810, \\ 704049712, 215749841);$$

■ **Таблица 2.** *Строение частных вариантов конечных групп четырехмерных векторов (N_ω — число элементов порядка ω)*

$p = 7; \varepsilon = 1$		$p = 11; \varepsilon = 10$		$p = 11; \varepsilon = 0$		$p = 13; \varepsilon = 0$	
ω	N_ω	ω	N_ω	ω	N_ω	ω	N_ω
2	57	2	133	2	1	2	339
3	170	3	110	3	242	3	1016
4	42	4	110	4	242	4	1692
6	618	5	1324	5	4	6	3720
7	48	6	110	6	242	12	15552
8	84	8	220	8	484	13	168
12	84	10	4492	10	4	26	168
14	48	11	120	11	120	39	336
16	168	12	220	12	484	52	336
21	96	15	440	15	968	78	336
24	168	20	440	20	968	156	672
42	96	22	120	22	120	–	–
48	336	24	440	24	968	–	–
–	–	30	440	30	968	–	–
–	–	40	880	40	1936	–	–
–	–	55	480	55	480	–	–
–	–	60	880	60	1936	–	–
–	–	110	480	110	480	–	–
–	–	120	1760	120	3872	–	–
$1+\sum_\omega N_\omega =$	2016	–	13200	–	14520	–	24336
$\Omega = p(p-1)\times$ $\times(p^2-1)$		$\Omega = p(p-1)\times$ $\times(p^2-1)$		$\Omega = p^2\times$ $\times(p^2-1)$		$\Omega = p^2\times$ $\times(p-1)^2$	

$$Q = (204543067, 267966222, \\ 209297175, 161608828);$$

$$Q^{-1} = (204543067, 483822175, \\ 542491222, 590179569);$$

$$Z = (493205368, 638573510, \\ 56561748, 103277561);$$

$$Q \circ G = (478445912, 349091248, \\ 194139031, 297937680);$$

$$G \circ Q = (478445912, 529600113, \\ 62144304, 36127512);$$

$$Z \circ G = (325816345; 478721415; \\ 216264816; 409136505);$$

$G \circ Z =$ (325816345; 196930991; 521380191; 144664353).

Алгоритм вычисления секретного ключа

В схемах открытого согласования ключа и открытого шифрования, описанных в первом разделе, используется открытый ключ Y, который вычисляется по личному секретному ключу (w, x) по формуле $Y = Q^w \circ G^x \circ Q^{-w}$, где Q и G — известные элементы некоммутативной группы достаточно большого простого порядка q и q' соответственно. Сложность вычисления секретного ключа по открытому задает верхнюю границу стойкости предложенных криптосхем. Для вычисления секретного ключа по открытому может быть использован алгоритм, аналогичный алгоритму больших и малых шагов, применяемому для решения задачи дискретного логарифмирования [8]. Рассмотрим вычисление секретного ключа в случае $q = q'$ (алгоритм может быть легко адаптирован для $q \neq q'$).

1. Для всех значений $w = 1, 2, ..., q$ вычислить таблицу значений $T(w) = Q^{-w} \circ Y \circ Q^w$. (Трудоемкость этого шага составляет $2q$ операций умножения элементов группы.)

2. Упорядочить таблицу, вычисленную на шаге 1. (Трудоемкость этого шага составляет $q\log_2 q$ операций сравнения элементов группы.)

3. Установить счетчик $i = 1$ и значение вектора $V = (1, 0, ..., 0)$.

4. Вычислить вектор $V = V \circ G$.

5. По отсортированной таблице проверить, имеется ли в ней значение V. Если в таблице имеется значение $T(w') = V$, то вывести значение секретного ключа $(w, x) = (w', i)$ и СТОП, в противном случае перейти к шагу 6.

6. Если $i \neq q$, то прирастить значение счетчика $i \leftarrow i + 1$ и перейти к шагу 4, в противном случае — СТОП и вывести сообщение «условия некорректны». (Трудоемкость шагов 5 и 6 составляет не более q операций умножения и $q\log_2 q$ операций сравнения.)

Если условия корректны, т. е. решение задачи имеется, то приведенный алгоритм при некотором значении счетчика i' найдет значение вектора V в таблице, т. е. в этот момент будет выполняться соотношение $T(w') = V = G^{i'}$. Поскольку $T(w') = Q^{-w'} \circ Y \circ Q^{w'}$, то $Y = Q^{w'} \circ G^{i'} \circ Q^{-w'}$, т. е. при корректно заданных условиях алгоритм действительно найдет решение. Трудоемкость алгоритма S составляет $3q$ операций умножения плюс $2q\log_2 q$ операций сравнения, т. е. $S = O(q)$, где $O(q)$ — обозначение порядка. Если принять достаточной верхнюю границу стойкости, равную $O(2^{80})$ операций (как в случае 1024-битовой криптосистемы RSA), то в предложенных в первом разделе криптосхемах следует выбрать некоммутативную группу, для которой значение порядка элементов Q и G равно $q \geq 2^{80}$.

Заключение

В качестве примитива протоколов открытого согласования секретного ключа и открытого шифрования предложена новая вычислительно трудная задача над конечными некоммутативными группами, которую можно назвать задачей дискретного логарифмирования в скрытой циклической подгруппе. На основе данной задачи построена схема согласования по открытому каналу общего секретного ключа двух удаленных абонентов и алгоритм открытого шифрования. В основе этих построений лежит процедура, комбинирующая функцию, задающую автоморфизм конечной некоммутативной группы, и операцию возведения элемента достаточно большого простого порядка в большую целочисленную степень. Разработан алгоритм решения рассматриваемой задачи, из которого дана оценка стойкости предложенных криптосхем. Однако данная задача является новой, поэтому требуются другие независимые исследования для более полной оценки безопасности этих криптосхем. Доказанная теорема 1 имеет общее значение для конечных некоммутативных групп различных типов. Эта теорема отражает «локальное» строение некоммутативной группы, а именно строение в той ее части, которая используется в построении криптосхем на основе новой задачи.

Предложенные криптосхемы могут быть реализованы над построенными конечными некоммутативными группами четырехмерных векторов, над конечными некоммутативными группами векторов других размерностей [9] или над конечными группами невырожденных матриц [10]. Выбор конкретного варианта некоммутативной группы для построения криптографических алгоритмов и протоколов будет определяться вычислительной эффективностью алгоритмов и протоколов при заданном уровне стойкости. Сравнительный анализ быстродействия криптосхем на основе конечных некоммутативных групп различного типа представляет самостоятельный интерес.

Предложенная вычислительно трудная задача может быть применена и для построения криптосхем других типов, например для разработки быстродействующих алгоритмов коммутативного шифрования и протоколов аутентификации с нулевым разглашением. Эти вопросы также представляют интерес как тема отдельного исследования.

Работа поддержана грантом РФФИ № 08-07-00096-а.

Литература

1. **Anshel I., Anshel M., Goldfeld D.** An Algebraic Method for Public Key Cryptography // Mathematical Research Letters. 1999. Vol. 6. P. 287–291.
2. **Shor P. W.** Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM Journal of Computing. 1997. Vol. 26. P. 1484–1509.
3. **Ko K. H. et al.** New Public-Key Cryptosystems Using Braid Groups // Advances in Cryptology — Crypto 2000: Lecture Notes in Computer Science. Springer-Verlag, 2000. Vol. 1880. P. 166–183.
4. **Lee E., Park J. H.** Cryptanalysis of the Public Key Encryption Based on Braid Groups // Advances in Cryptology — Eurocrypt 2003: Lecture Notes in Computer Science. Springer-Verlag, 2003. Vol. 2656. P. 477–489.
5. **Verma G. K.** A Proxy Blind Signature Scheme over Braid Groups // Int. Journal of Network Security. 2009. Vol. 9. N 3. P. 214–217.
6. **Молдовяну П. А., Дернова Е. С., Костина А. А., Молдовян Н. А.** Гомоморфизм конечных групп векторов малой размерности и синтез схем цифровой подписи // Информационно-управляющие системы. 2009. № 4. С. 26–32.
7. **Каргаполов М. И., Мерзляков Ю. И.** Основы теории групп. — М.: Физматлит, 1996. — 287 с.
8. **Menezes A. J., Van Oorschot P. C., Vanstone S. A.** Handbook of Applied Cryptography. — Boca Raton, FL: CRC Press, 1997. — 780 p.
9. **Молдовян Д. Н., Куприянов А. И., Костина А. А., Захаров Д. В.** Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи // Вопросы защиты информации. 2009. № 4. С. 13–18.
10. **Дернова Е. С., Костина А. А., Молдовяну П. А.** Конечные группы матриц как примитив алгоритмов цифровой подписи // Вопросы защиты информации. 2008. № 3(82). С. 8–12.

Новиков Ф. А., Иванов Д. Ю.
Моделирование на UML. Теория, практика, видеокурс. — СПб.: Профессиональная литература, Наука и Техника, 2010. — 640 с.: ил. + цв. вклейки (+2 DVD) ISBN 978-5-94387-610-3.

Книга содержит полное описание всех основных версий унифицированного языка моделирования UML и набор рекомендаций по применению языка для моделирования программных систем. При этом высокий уровень понимания авторами UML, умение его использовать вкупе с блестящими педагогическими навыками и хорошим, доступным языком позволяют сделать из учебника (которым книга, несомненно, является) нечто большее, чем просто учебник. Передаваемый опыт и идеи, которыми авторы щедро делятся на страницах книги, делают ее интересной как для читателя уже знакомого с UML, так и для читателя, которому просто интересно узнать, что такое UML и как его применять в своей практике.

В конце книги размещены сводные таблицы, толковый словарь и развитый предметный указатель, что позволяет использовать книгу в качестве справочника. На цветной вклейке дается графическая нотация-шпаргалка, представляющая собой квинтэссенцию нотации UML с необходимыми пояснениями. К книге прилагается видеокурс по UML на двух DVD.

Книга предназначена для практикующих разработчиков программного обеспечения, руководителей IT-проектов и их заказчиков, системных архитекторов, студентов высших и средних специальных учебных заведений, а также всех желающих освоить унифицированный язык моделирования UML или познакомиться с ним.

Книгу можно приобрести на официальном сайте данного издания: www.umlmanual.ru