Протокол генерации общего ключа, использующий группу матриц над конечным полем и атаку линейным разложением

И. В. Зубков (МГУ имени М. В. Ломоносова, Москва)

В настоящей работе предложен протокол генерации общего ключа, использующий группу матриц над конечным полем. В качестве одного из этапов протокола используется атака линейным разложением, недавно предложенная В. А. Романьковым для компрометации протоколов, в которых платформа является линейной группой. Анализируется стойкость предложенной криптосистемы против различных известных атак.

Ключевые слова: группа матриц над конечным полем, некоммутативная криптография, криптография с открытым ключом, протокол генерации общего ключа, атака линейным разложением.

Введение

Для обеспечения высокого уровня надежности передачи секретных данных необходимо регулярно менять ключи. Для этого нужно разрабатывать протоколы выработки общего ключа. Это позволяет осуществлять криптография с открытым ключом. Существует ряд подходов, связанных с данным направлением: криптосистема Диффи и Хеллмэна [?] с использованием мультипликативной группы поля вычетов по простому модулю p; криптографический протокол Р. Ривеста, А. Шамира и Л. Адлемана [?] асимметричного шифрования, основанный на использовании функции с секретом (возведение в степень e по модулю pq, где p и q — простые числа); схема открытого распределения ключей для конференц-связи, предложенная Асмутом и Блюмом [?], использующая китайскую теорему об остатках. С развитием криптографии с открытым ключом были предприняты попытки использования некоммутативных структур,

в том числе группы: протокол генерации общего ключа Ко, Ли и др. [?] с использованием группы кос; протокол генерации общего ключа Стикеля [?] с использованием некоммутативной конечной группы; протокол генерации общего ключа Альвареса, Мартинеса и др. [?] с использованием группы матриц над конечным полем; протокол генерации общего ключа Шпильрайна-Ушакова [?] с использованием группы Томпсона; протокол генерации общего ключа Романчука-Устименко [?] с использованием группы невырожденных матриц над конечным полем; протокол генерации общего ключа Махаланобиса [?] с использованием некоммутативной нильпотентной группы и группы её автоморфизмов.

Полугруппа матриц 3×3 над $\mathbf{F}_7[\mathbf{A}_5]$, где $\mathbf{A}_5$ — знакопеременная группа, используется Хабибом, Кахроби, Куписом и Шпильрайном [?] в качестве платформы в протоколе генерации общего ключа с использованием голоморфа группы. Некоммутативный моноид матриц 3×3 над усечёнными многочленами степени 1000 от десяти переменных над кольцом $\mathbf{Z}_{12}$ является платформой в протоколе генерации общего ключа, предложенном Вангом, Као и др. [?].

Недавно В. А. Романьков предложил в [?] принципиально новую атаку на протоколы, названную *атакой линейным разложением*. С помощью данной атаки при условии, что используемая в криптосистеме группа является линейной, за время, полиномиальное от исходных данных, во многих случаях удается получить секретный ключ, не находя секретные данные пользователей.

Новизна предлагаемого ниже подхода к построению протокола заключается в том, что первый пользователь (Алиса) на одном из этапов применяет атаку линейным разложением для нахождения промежуточных данных, используемых в дальнейшем, не находя секретные данные второго пользователя (Боба).

Протокол генерации общего ключа

Пусть $G = \mathrm{GL}_k(\mathbf{F}_{3^m})$ и $\mathrm{Aut}(G)$ — группа автоморфизмов группы G. Далее, пусть U и W — два конечных подмножества $\mathrm{Aut}(G)$, причем элементы U попарно коммутируют с элементами из W, а также элементы U коммутируют друг с другом.

Замечание. В данной работе в качестве элементов U будут использованы автоморфизмы сопряжением. Их действие определено на всём кольце матриц $\mathrm{M}_k(\mathbf{F}_{3^m})$, при этом для любых элементов $g_1, g_2 \in \mathrm{M}_k(\mathbf{F}_{3^m})$ и для

любого $u \in U$ выполнено соотношение $u(g_1 + g_2) = u(g_1) + u(g_2)$, где под сложением понимается обычное матричное сложение в $\mathrm{M}_k(\mathbf{F}_{3^m})$.

Обозначим через A и B подгруппы $\mathrm{Aut}(G)$, порожденные U и W соответственно. Зафиксируем элемент $g \in G$.

Открытые данные: U, W, g.

Алиса выбирает автоморфизм $b_1 \in B$, вычисляет $b_1(g)$, затем строит матрицу $f \in G$ такую, чтобы для любого $u \in U$ было выполнено $u(f) = f$, причем матрица $b_1(g) + f$ должна быть вырожденной, и отправляет Бобу $b_1(g) + f$.

Боб выбирает два автоморфизма $a_1, a_2 \in A$ и отправляет Алисе пару элементов

$$a_1(b_1(g) + f) = a_1(b_1(g)) + f, \qquad a_2(b_1(g) + f) = a_2(b_1(g)) + f.$$

Алиса вычитает из обоих элементов, полученных от Боба, матрицу f и применяет автоморфизм b_1^{-1} к полученной паре:

$$b_1^{-1}(a_1(b_1(g))) = a_1(g), \qquad b_1^{-1}(a_2(b_1(g))) = a_2(g).$$

После этого она применяет атаку линейным разложением (см. [**?**]) и получает матрицу $a_1(a_2(g))$. Наконец, Алиса выбирает автоморфизм $b_2 \in B$ и отправляет Бобу $b_2(g)$.

Получение ключа. Алиса вычисляет $K_A = b_2(a_1(a_2(g)))$, Боб вычисляет $K_B = a_1(a_2(b_2(g)))$. Тогда общий ключ равен $K = K_A = K_B$, поскольку элементы A и B попарно коммутируют.

Выбор U, W, g

Пусть отображение $\det\colon \mathrm{GL}_k(\mathbf{F}_{3^m}) \to \mathbf{F}_{3^m}^*$ любой матрице сопоставляет её определитель, тогда $\chi \in \mathrm{Aut}(G)$ определим так: для любого $g \in G$ положим $\chi(g) = \det(g) \cdot g$.

Также нам понадобятся три попарно коммутирующие матрицы $x, y, z \in \mathrm{GL}_k(\mathbf{F}_{3^m})$. Тогда определим $U = \{\overline{x}; \overline{y}\}$, $W = \{\chi; \overline{z}\}$, где автоморфизмы типа $\overline{x}$ понимаются как действие сопряжением соответствующей матрицей x, то есть $\overline{x}(g) = xgx^{-1}$, где $g \in G$.

Если $\overline{x}$ — автоморфизм сопряжением, $g \in G$, то

$$\chi{\circ}x(g) = \chi(xgx^{-1}) = \det x{\cdot}\det g{\cdot}\det x^{-1}{\cdot}xgx^{-1} = x{\cdot}(\det g{\cdot}g){\cdot}x^{-1} = x{\circ}\chi(g),$$

следовательно, автоморфизм χ коммутирует со всеми автоморфизмами сопряжения. Поэтому, учитывая, что матрицы x, y и z попарно перестановочны, получаем, что элементы U попарно коммутируют с элементами из W, а также элементы U коммутируют друг с другом.

Для выбора вышеупомянутых матриц x, y и z нам понадобится матрица $P \in \mathrm{GL}_{20m}(\mathbf{F}_3)$ (выбор параметра $20m$ обусловлен вычислительной сложностью), реализующая умножение на примитивный элемент в мультипликативной группе поля $\mathbf{F}_{3^{20m}}$. Пусть r — примитивный элемент и $\{1, e, e^2, \ldots, e^{20m-1}\}$ — некоторый базис поля $\mathbf{F}_{3^{20m}}$ как векторного пространства над $\mathbf{F}_3$. Для всех $0 \leqslant j \leqslant 20m-1$ вычислим $r \cdot e^j = \sum_{i=0}^{20m-1} p_{ij} \cdot e^i$, тогда для любого вектора $v = (v_0; v_1; \ldots; v_{20m-1})$ из элементов $\mathbf{F}_3$ имеем:

$$r \cdot v = r \cdot \sum_{j=0}^{20m-1} v_j \cdot e^j = \sum_{j=0}^{20m-1} v_j \cdot r \cdot e^j = \sum_{j=0}^{20m-1} v_j \Big(\sum_{i=0}^{20m-1} p_{ij} \cdot e^i \Big) =$$

$$= \sum_{j=0}^{20m-1} \sum_{i=0}^{20m-1} p_{ij} \cdot v_j \cdot e^i = \sum_{i=0}^{20m-1} \Big(\sum_{j=0}^{20m-1} p_{ij} \cdot v_j \Big) \cdot e^i, \quad (1)$$

что соответствует умножению матрицы $P = (p_{ij})$ на вектор v.

Заметим, что $P \in \mathrm{GL}_{20m}(\mathbf{F}_3)$. Для этого докажем, что столбцы матрицы P, равные $r \cdot 1$, $r \cdot e$, $r \cdot e^2$, …, $r \cdot e^{20m-1}$, линейно независимы. Действительно, пусть существует набор коэффициентов $(\lambda_0; \lambda_1; \ldots; \lambda_{20m-1})$ из $\mathbf{F}_3$ такой, что $\sum_{i=0}^{20m-1} \lambda_i r e^i = 0$. Это равносильно тому, что $r \cdot \sum_{i=0}^{20m-1} \lambda_i e^i = 0$, то есть $\sum_{i=0}^{20m-1} \lambda_i e^i = 0$, откуда следует, что все $\lambda_i = 0$, поскольку $\{1, e, e^2, \ldots, e^{20m-1}\}$ — базис.

Заметим, что столбцы матрицы P^i, где $i \in \mathbb{N}$, представляют из себя столбцы матрицы P, умноженные на r^{i-1}, откуда следует, что все матрицы P, P^2, …, $P^{3^{20m}-1}$ различны, поскольку порядок r равен $3^{20m} - 1$.

Матрицы x, y и z будут блочно-диагональными. Матрица x будет состоять из трёх блоков. Первым блоком (в левом верхнем углу) будет матрица P, вторым — единичная матрица порядка $40m$, а последним — некоторая матрица $x_1 \in \mathrm{GL}_{k-60m}(\mathbf{F}_{3^m})$, выбор которой обсуждается ниже. Матрица y будет состоять из четырёх блоков. Первым блоком (в левом верхнем углу) будет единичная матрица порядка $20m$, вторым — матрица P, третьим — снова единичная порядка $20m$, а последним — некоторая матрица $y_1 \in \mathrm{GL}_{k-60m}(\mathbf{F}_{3^m})$, выбор которой также обсуждается ниже. Матрица z будет состоять из трёх блоков. Первым блоком (в левом верхнем углу) будет единичная матрица порядка $40m$, вторым —

матрица P, а последним — некоторая матрица $z_1 \in \mathrm{GL}_{k-60m}(\mathbf{F}_{3^m})$ (выбор которой обсуждается ниже). Тогда матрицы x, y и z попарно коммутируют, если только коммутируют матрицы x_1, y_1 и z_1. В таком случае все матрицы x, x^2, …, $x^{3^{20m}-1}$ различны, y, y^2, …, $y^{3^{20m}-1}$ различны, а также все матрицы z, z^2, …, $z^{3^{20m}-1}$ различны между собой, поскольку матрицы P, P^2, …, $P^{3^{20m}-1}$ различны. Для выбора матриц x_1, y_1 и z_1 введем понятие класса C_t матриц, где $t \in \mathbb{N}$, C — фиксированная матрица, принадлежащая $\mathrm{GL}_t(\mathbf{F}_{3^m})$.

$$C_t = \{CDC^{-1} \mid D = diag\{d_1, \ldots, d_t\}, d_1, \ldots, d_t \in \mathbf{F}_{3^m}^*\}.$$

Иными словами, ко всем возможным диагональным матрицам порядка t применяется сопряжение фиксированной матрицей C. Для любых матриц $d_1, d_2 \in C_t$ выполнено $d_1 = CD_1C^{-1}$, $d_2 = CD_2C^{-1}$, следовательно,

$$d_1 \cdot d_2 = CD_1C^{-1} \cdot CD_2C^{-1} = CD_1D_2C^{-1} = CD_2D_1C^{-1} = d_2 \cdot d_1.$$

Таким образом, все матрицы из класса C_t коммутируют друг с другом. Отметим, что этот класс замкнут относительно умножения и содержит $(3^m - 1)^t$ элементов.

Для выбора матрицы C нам понадобится конструкция построения матрицы, определитель которой является порождающим элементом мультипликативной группы поля $\mathbf{F}_{3^m}$, при этом сама матрица C должна выглядеть «случайной». Для этого случайным образом выбираем матрицу $C_1 = (c_{ij}) \in \mathrm{GL}_{t-1}(\mathbf{F}_{3^m})$ и элементы t-й строки и t-го столбца $c_{t,1}$, …, $c_{t,t-1}$, $c_{1,t}$, …, $c_{t-1,t} \in \mathbf{F}_{3^m}$. Последний элемент $c_{t,t}$ подбираем из следующих соображений. Используя разложение по последнему столбцу для матрицы $C = (c_{ij}) \in \mathrm{GL}_t(\mathbf{F}_{3^m})$, получаем $\det C = c_{t,t} \cdot \det c_1 + c'$, где $c' \in \mathbf{F}_{3^m}$. Следовательно, существует элемент $c_{t,t}$, при котором определитель матрицы C равен порождающему элементу мультипликативной группы поля $\mathbf{F}_{3^m}$.

Итак, строим матрицу C с помощью такой конструкции для $t = k - 60m$. Матрицы x_1, y_1 и z_1 выбираем случайно из полученного класса.

В качестве элемента $g \in G$ берем блочную матрицу:

$$\begin{pmatrix} G_1 & M_1 & M_2 & M_3 \\ O & G_2 & M_4 & M_5 \\ O & O & G_3 & M_6 \\ O & O & O & G_4 \end{pmatrix},$$

где $G_1, G_2, G_3 \in \mathrm{GL}_{20m}(\mathbf{F}_{3^m})$ выбираются случайно; $G_4 \in \mathrm{GL}_{k-60m}(\mathbf{F}_{3^m})$ строится с помощью конструкции, описанной выше, таким образом, что произведение определителей матриц G_1, G_2, G_3, G_4 равняется порождающему элементу мультипликативной группы поля $\mathbf{F}_{3^m}$; $M_1, \ldots, M_6$ — произвольные матрицы над $\mathbf{F}_{3^m}$ с размерами, согласованными с G_1, G_2, G_3, G_4; O — нулевые матрицы с согласованными размерами.

В качестве используемой на втором этапе протокола матрицы f такой, что для любого $u \in U$ выполнено $u(f) = f$, Алиса выбирает блочно-диагональную матрицу

$$\begin{pmatrix} P^{t_1} & O & O & O \\ O & P^{t_2} & O & O \\ O & O & F' & O \\ O & O & O & F'' \end{pmatrix},$$

где t_1, t_2 — случайным образом выбранные натуральные числа, $1 \leqslant t_1, t_2 \leqslant 3^{20m} - 1$, блок $F'' \in C_{k-60m}$ также выбирается случайным образом, а выбор блока $F' \in \mathrm{M}_{20m}(\mathbf{F}_{3^m})$ производится из следующих соображений.

Представим матрицу f в виде суммы $f = f_1 + f_2$, где

$$f_1 = \begin{pmatrix} P^{t_1} & O & O & O \\ O & P^{t_2} & O & O \\ O & O & O & O \\ O & O & O & F'' \end{pmatrix}, \qquad f_2 = \begin{pmatrix} O & O & O & O \\ O & O & O & O \\ O & O & F' & O \\ O & O & O & O \end{pmatrix}.$$

Приведем матрицу $b_1(g) + f_1$ методом Гаусса к ступенчатому виду. Если матрица $b_1(g) + f_1$ является вырожденной, то в качестве F' достаточно выбрать нулевой блок. Кроме того, заметим, что если линейно зависимыми оказываются уже первые $40m$ столбцов матрицы $b_1(g) + f_1$, то на самом деле блок F' можно выбрать произвольным образом: преобразования над первыми $40m$ строками при приведении матрицы $b_1(g) + f_1$ к ступенчатому виду не зависят от блока F'.

Теперь будем рассматривать случай, когда матрица $b_1(g) + f_1$ невырождена, а значит, преобразованиями над строками она приводится к диагональному виду. Такое приведение соответствует умножению слева на некоторую матрицу $\alpha \in \mathrm{GL}_k(\mathbf{F}_{3^m})$. Пусть полученная диагональная матрица $\alpha \cdot (b_1(g) + f_1)$ имеет вид $diag\{d_1, \ldots, d_k\}$. Для удобства будем использовать блочное представление $\alpha \cdot (b_1(g) + f_1) = diag\{D_1, D_2, D_3, D_4\}$, где блоки D_1, D_2, D_3 имеют размер $20m$, а блок D_4 имеет размер $k - 60m$.

Заметим, что блочный вид матрицы α является верхнетреугольным, поскольку как $b_1(g)$, так и f_1 имеют верхнетреугольный блочный вид.

При умножении матрицы f_2 слева на α получается матрица $\alpha \cdot f_2$, у которой ненулевыми могут являться только столбцы с номерами $40m + 1, \ldots, 60m$. Разобьем подматрицу из этих столбцов размером $k \times 20m$ на четыре блока: верхние три блока содержат по $20m$ строк, последний — $k - 60m$. Обозначим верхние три блока через H_1, H_2, H_3, соответственно. Последний же блок, как нетрудно видеть, полностью состоит из нулей.

Имеем

$$\alpha \cdot (b_1(g) + f) = \alpha \cdot (b_1(g) + f_1) + \alpha \cdot f_2 = \begin{pmatrix} D_1 & O & H_1 & O \\ O & D_2 & H_2 & O \\ O & O & D_3 + H_3 & O \\ O & O & O & D_4 \end{pmatrix}.$$

Определитель этой матрицы равен

$$\det D_1 \cdot \det D_2 \cdot \det(D_3 + H_3) \cdot \det D_4.$$

Теперь Алисе нужно выбрать такую матрицу F', чтобы матрица $D_3 + H_3$ была вырожденной. Заметим, что блок H_3 является результатом умножения блока F' на соответствующий блок α' матрицы α, который, очевидно, является невырожденным.

Соответствующий выбор блока H_3 достаточно велик. Например, можно взять произвольную верхнетреугольную матрицу из $\mathrm{M}_{20m}(\mathbf{F}_{3^m})$, у которой хотя бы один диагональный элемент $f_{i,i}$ равен $-d_i$, то есть является обратным к соответствующему диагональному элементу матрицы $\alpha(b_1(g) + f_1)$. Или произвольную матрицу из $\mathrm{M}_{20m}(\mathbf{F}_{3^m})$, в которой i-я строка (для некоторого фиксированного i) содержит все нули и диагональный элемент $f_{i,i} = -d_i$.

Тогда

$$\alpha' \cdot F' = H_3 \Leftrightarrow F' = (\alpha')^{-1} \cdot H_3.$$

Таким образом, искомая матрица f построена, поскольку вырожденность матрицы $\alpha \cdot (b_1(g) + f)$ равносильна вырожденности матрицы $b_1(g) + f$. Заметим, что, например, количество матриц f, полученных из верхнетреугольных блоков H_3, не меньше, чем $3^{10m(20m-1)} \cdot (3^m - 1)^{k-60m}$, поскольку в ячейках матрицы H_3, расположенных выше диагонали, могут стоять любые элементы поля $\mathbf{F}_{3^m}$, а число матриц в классе C_{k-60m} равно $(3^m - 1)^{k-60m}$.

Атака линейным разложением

Утверждение 1. *Пусть* $G = \mathrm{GL}_k(\mathbf{F}_{3^m})$, $U = \{\overline{x}; \overline{y}\}$, $A = \langle U \rangle$ *является подгруппой* $\mathrm{Aut}(G)$, *порожденной множеством* U. *Выберем произвольные* $a_1, a_2 \in A$ *и* $g \in G$. *Тогда по открытым данным* $U, g, a_1(g), a_2(g)$ *за* $O(k^6 m^2)$ *операций в* $\mathbf{F}_3$ *и* $O(k^4)$ *операций применения каждого автоморфизма из* U *можно вычислить* $a_1(a_2(g))$.

Доказательство. Будем трактовать $\mathrm{M}_k(\mathbf{F}_{3^m})$ как векторное пространство V размерности k^2 над полем $\mathbf{F}_{3^m}$, интерпретируя матрицы как наборы из k^2 элементов поля. Любой автоморфизм $a \in A$ может быть продолжен до элемента из $\mathrm{End}(V)$, где $\mathrm{End}(V)$ — группа эндоморфизмов V, поскольку для любых $g, h \in \mathrm{M}_k(\mathbf{F}_{3^m})$ и для произвольного автоморфизма сопряжением $\overline{x}$ верно $x(g+h)x^{-1} = xgx^{-1} + xhx^{-1}$.

Тогда, согласно утверждению 1 из [**?**], мы можем по открытым данным найти $a_1(a_2(g))$ при помощи построения базиса пространства $\mathrm{Sp}(A(g))$, где $\mathrm{Sp}(A(g))$ — подпространство V, порожденное векторами $A(g) = \{a(g) \mid a \in A\}$. Для этого полагается $L_0 = \{g\}$, L_{i+1} — максимальное линейно независимое подмножество $L_i \cup U(L_i)$, где $U(L_i) = \{u(l_i) \mid u \in U, l_i \in L_i\}$. Цепочка $L_0 < L_1 < \ldots < L_t$ с некоторого момента стабилизируется, поскольку $L_t \subseteq V$, следовательно, момент стабилизации наступит не более, чем через k^2 шагов, так как размерность пространства V равна k^2. Поэтому каждый автоморфизм из U придется применять максимум столько раз, сколько в сумме элементов во всей цепочке, значит, не более $1 + 2 + \ldots + k^2 = O(k^4)$ раз.

Согласно лемме 3.1 из [**?**] на нахождение базиса пространства $\mathrm{Sp}(A(g))$ требуется (без учета операций применения автоморфизмов из U) $O(k^6)$ операций в поле $\mathbf{F}_{3^m}$ или $O(k^6 m^2)$ операций в $\mathbf{F}_3$. Утверждение доказано.

Отметим, что в процессе вычисления $a_1(a_2(g))$ сами автоморфизмы a_1, a_2 не находятся.

Вычислительная сложность протокола

Сложность протокола будем оценивать при фиксированных значениях параметров $k = 10001$, $m = 53$.

Для применения автоморфизма χ оценим количество различных элементов в последовательности

$$id, \chi, \chi^2, \ldots, \chi^n, \ldots$$

Пусть $\chi^t(g) = (\det g)^{\alpha_t} \cdot g$. Элементы последовательности $\{\alpha_t\}$ удовлетворяют рекуррентному соотношению. Действительно,

$$\chi^{t+1}(g) = \det((\det g)^{\alpha_t} \cdot g) \cdot (\det g)^{\alpha_t} \cdot g = \\ = (\det g)^{k\alpha_t} \cdot \det g \cdot (\det g)^{\alpha_t} \cdot g = (\det g)^{k\alpha_t + \alpha_t + 1} \cdot g,$$

и, следовательно, $\alpha_{t+1} = (k+1)\alpha_t + 1$. С учетом того, что $\alpha_1 = 1$, имеем $\alpha_t = \frac{(k+1)^t - 1}{k}$.

Далее, совпадение автоморфизмов χ^{r_1} и χ^{r_2} при некоторых натуральных $r_1 > r_2$, то есть выполнение условия $\chi^{r_1}(g) = \chi^{r_2}(g)$ для всех $g \in \mathrm{GL}_k(\mathbf{F}_{3^m})$, равносильно тому, что $\alpha_{r_1} - \alpha_{r_2}$ делится на $3^m - 1$, поскольку мультипликативная группа поля $\mathbf{F}_{3^m}$ является циклической порядка $3^m - 1$. Из формулы для α_r получаем, что это равносильно тому, что $(k+1)^{r_1}$ сравнимо с $(k+1)^{r_2}$ по модулю $3^m - 1$, поскольку $k = 10001$ взаимно просто с $3^m - 1 = 3^{53} - 1$. Отсюда следует, что $10002^{r_2} \cdot (10002^{r_1 - r_2} - 1)$ делится на $3^{53} - 1$. Поскольку наибольший общий делитель чисел 10002 и $3^{53} - 1$ равен 2, то $10002^{r_2} \cdot (10002^{r_1 - r_2} - 1)$ будет делится на $3^{53} - 1$, только если $r_2 \geqslant 1$ и $r_1 - r_2$ не меньше, чем порядок элемента 10002 в кольце вычетов по модулю $\frac{3^{53}-1}{2}$, который равен приблизительно 2^{68} (данный факт проверен с помощью системы компьютерной математики PARI/GP). Поэтому можно считать, что все автоморфизмы χ^t, где $1 \leqslant t \leqslant 2^{68}$, различны.

Для вычисления автоморфизма χ^t, где $1 \leqslant t \leqslant 2^{68}$, требуется сначала вычислить определитель за $O(k^3 m^2) = O(2^{52})$ операций в $\mathbf{F}_3$ по методу Гаусса, после этого нужно возвести определитель в степень $\frac{(k+1)^t - 1}{k}$, на что затратится $O(tm^2 \log k) = O(2^{80})$ операций в $\mathbf{F}_3$ с помощью алгоритма быстрого возведения в степень. Останется каждый из k^2 элементов умножить на полученное число за $O(k^2 m^2) = O(2^{38})$ операций. Всего: $O(2^{80})$ операций в $\mathbf{F}_3$.

Теперь оценим сложность самого протокола. Алисе и Бобу нужно суммарно девять раз применять случайные автоморфизмы из подгрупп A и B. Для этого элемент $a \in A$ будем выбирать в виде $\overline{x}^i \circ \overline{y}^j$, где $1 \leqslant i, j \leqslant 3^{20m} - 1$. Элемент $b \in B$ выбираем в виде $\chi^i \circ \overline{z}^j$, где $1 \leqslant i \leqslant 2^{68}, 1 \leqslant j \leqslant 3^{20m} - 1$. На умножение матриц в группе G, как

и на нахождение обратной матрицы, требуется $O(k^3)$ операций в поле $\mathbf{F}_{3^m}$ или $O(k^3m^2) = O(2^{52})$ операций в поле $\mathbf{F}_3$. Следовательно, на вычисление матрицы при действии автоморфизмом сопряжения требуется $O(k^3m^2 \log(3^{20m} - 1))$ операций (при применении алгоритма быстрого возведения в степень), что можно заменить на $O(k^3m^3) = O(2^{60})$. На применение автоморфизма χ^i требуется $O(2^{80})$ операций. Также Алисе нужно применить атаку линейным разложением, на что необходимо $O(k^6m^2)$ операций в $\mathbf{F}_3$ и $O(k^4)$ операций применения автоморфизмов из $U = \{\overline{x}; \overline{y}\}$, согласно утверждению 1. Следовательно, на атаку уйдет $O(k^7m^2) = O(2^{105})$ операций. Для выбора матрицы g с нужным определителем можно считать, что потратится столько же операций по порядку, сколько на вычисление определителя, то есть $O(k^3m^2) = O(2^{52})$ операций. На приведение матрицы $b_1(g) + f$ к верхнетреугольной и применение обратных преобразований строк также понадобится $O(k^3m^2) = O(2^{52})$ операций.

Вывод. На протокол требуется $O(2^{105})$ операций в $\mathbf{F}_3$.

Оценка мощности множества генерируемых ключей

Результатом выполнения протокола является строка длины k^2 из элементов поля $\mathbf{F}_{3^m}$. Оценим грубо количество разных строк, которые могут получиться после всех обменов данными. Для этого рассмотрим квадратную подматрицу M_1 матрицы g, являющуюся пересечением первых $20m$ строк со столбцами с номерами $20m + 1, \ldots, 40m$. Пусть $a_1 = \overline{x}^{i_1} \circ \overline{y}^{j_1}$, $a_2 = \overline{x}^{i_2} \circ \overline{y}^{j_2}$, тогда в ключе $a_1(a_2(b_2(g)))$ блок M_1 перейдет в $P^{i_1+i_2} M_1 P^{-j_1-j_2}$, умноженный на некоторый ненулевой элемент поля $\mathbf{F}_{3^m}$, откуда следует, что количество различных ключей, которые могут быть сгенерированы в результате работы алгоритма, не меньше, чем порядок P (если $M_1 \in \mathrm{GL}_{20m}(\mathbf{F}_{3^m})$), то есть $3^{20m} - 1 \approx 2^{1680}$.

Замечание 1. Проанализируем стойкость протокола против различных типов атак. Злоумышленник знает элементы $g, b_1(g) + f, a_1(b_1(g) + f), a_2(b_1(g) + f), b_2(g)$. Применяя атаку линейным разложением за время, по порядку равное времени работы протокола, можно получить $a_1(a_2(b_1(g) + f))$. Эта матрица равна $a_1(a_2(b_1(g))) + f$, но поскольку злоумышленник не знает f, ему придется работать с вырожденной матрицей $a_1(a_2(b_1(g)+f))$. Для того, чтобы найти ключ, равный $a_1(a_2(b_2(g)))$, мож-

но попытаться найти автоморфизм $b' \in \mathrm{Aut}(G)$ такой, что $b'(b_1(g)+f) = b_2(g)$, причем b' коммутирует со всеми элементами из U. При успешном поиске можно вычислить $b' \circ a_1(a_2(b_1(g)+f)) = a_1(a_2(b'(b_1(g)+f))) = a_1(a_2(b_2(g))) = K$. Но тогда матрица $b_1(g)+f$ является прообразом $b_2(g)$ при действии автоморфизмом b', следовательно, является невырожденной. Алиса же специально подбирала матрицу f так, чтобы это условие не выполнялось. Полученное противоречие доказывает, что данный тип атаки к протоколу не применим.

Полный перебор всех автоморфизмов из подгрупп A и B также невозможен, поскольку они содержат не меньше, чем $3^{20m} - 1 \approx 2^{1680}$ различных элементов, поэтому за разумное время соперник не сможет перебрать все автоморфизмы.

Замечание 2. Для увеличения стойкости протокола можно ввести предварительный шаг, использующий конструкцию, аналогичную [**?**].

Зафиксируем элемент $h \in G$ и автоморфизм $\varphi \in \mathrm{Aut}(G)$. К открытым данным добавятся h, φ.

Алиса выбирает $l \in \mathbb{N}$, вычисляет $(\varphi, h)^l = (\varphi^l, \varphi^{l-1}(h) \cdot \ldots \cdot \varphi(h) \cdot h)$ и отправляет Бобу $a_l = \varphi^{l-1}(h) \cdot \ldots \cdot \varphi(h) \cdot h$. Боб выбирает $s \in \mathbb{N}$, вычисляет $(\varphi, h)^s = (\varphi^s, \varphi^{s-1}(h) \cdot \ldots \cdot \varphi(h) \cdot h)$ и отправляет Алисе a_s. После этого Алиса вычисляет $\varphi^l(a_s) \cdot a_l = a_{l+s}$, а Боб вычисляет $\varphi^s(a_l) \cdot a_s = a_{l+s}$. Обозначим матрицу a_{l+s} за $g \in G$. Именно с этой матрицы начнется основной шаг работы предложенного выше протокола.

В качестве элемента $h \in G$ берем блочную матрицу, аналогичную матрице g, выбираемой выше, определитель которой является порождающим элементом мультипликативной группы поля $\mathbf{F}_{3^m}$, используя конструкцию выше. В качестве автоморфизма $\varphi \in \mathrm{Aut}(G)$ берем χ. Выбор l, s производится случайным образом из промежутка $[2^k; 2^{2k}]$. Тогда при выборе $k = 10001$, $m = 53$ сложность протокола по порядку останется прежней.

С использованием этого дополнительного шага протокола связаны следующие два замечания.

Замечание 3. Если $\varphi(h) = \chi(h) = \det h \cdot h$, то при некоторых условиях на h Алиса и Боб смогут скрыть g от противника при использовании атаки последовательным перебором.

Доказательство. Из доказанного выше имеем: $\varphi^p(h) = (\det h)^{\alpha_p} \cdot h$, где $\alpha_p = \frac{(k+1)^p - 1}{k}, p \in \mathbb{N}$. Тогда $a_l = (\det h)^{\alpha_1 + \ldots + \alpha_{l-1}} \cdot h^l$, откуда $a_{l'} = a_l \Leftrightarrow (\det h)^{\alpha_{l'} + \ldots + \alpha_{l-1}} \cdot h^{l-l'} = e$ — единичная матрица.

Аналогично, $a_{l'+s} = a_{l+s} \Leftrightarrow (\det h)^{\alpha_{l'+s}+\ldots+\alpha_{l+s-1}} \cdot h^{l-l'} = e$. Поэтому, если противник перебором нашел такое l', что $a_{l'} = a_l$, то равенство $a_{l'+s} = a_{l+s}$ равносильно тому, что $(\det h)^{\alpha_{l'+s}+\ldots+\alpha_{l+s-1}} \cdot h^{l-l'} = e = (\det h)^{\alpha_{l'}+\ldots+\alpha_{l-1}} \cdot h^{l-l'} \Leftrightarrow (\det h)^{\alpha_{l'+s}+\ldots+\alpha_{l+s-1}} = (\det h)^{\alpha_{l'}+\ldots+\alpha_{l-1}}$. Поскольку матрица h такова, что ее определитель является порождающим элементом мультипликативной группы поля $\mathbf{F}_{3^m}$, данное равенство равносильно $\alpha_{l'}+\ldots+\alpha_{l-1} \equiv \alpha_{l'+s}+\ldots+\alpha_{l+s-1}$ по модулю 3^m-1. Подставляя формулу для всех степеней α_p получаем, что это равносильно

$$(k+1)^{l'} + \ldots + (k+1)^{l-1} \equiv (k+1)^{l'+s} + \ldots + (k+1)^{l+s-1} \Leftrightarrow$$
$$\Leftrightarrow (k+1)^{l'} \cdot ((k+1)^s - 1) \cdot ((k+1)^{l-l'} - 1) \vdots 3^m - 1. \quad (2)$$

Поскольку выбор l, s производится из промежутка $[2^k; 2^{2k}]$, то Алиса и Боб могут выбрать достаточно много различных чисел l, s таких, что вышеполученное соотношение неверно при произвольном l' таком, что $a_{l'} = a_l$. Следовательно, противник не сможет таким образом вычислить матрицу g.

Замечание 4. В [?] к протоколу [?] успешно применяется атака линейным разложением. Но в книге разбирается только случай, когда $\varphi \in \mathrm{End}(G)$. В случае вышеизложенного дополнительного шага протокола автоморфизм $\varphi = \chi$ не продолжается естественным образом до эндоморфизма векторного пространства, поскольку легко придумать две матрицы g_1, g_2 такие, что $\chi(g_1+g_2) \neq \chi(g_1)+\chi(g_2)$. Поэтому данный тип атаки не применим.

Благодарности

Автор выражает благодарность научному руководителю к.ф.-м.н. А. Е. Пакратьеву за постановку задачи и помощь в работе, а также к.ф.-м.н. А. В. Галатенко и к.ф.-м.н. В. А. Носову, которые ознакомились с результатами работы и сделали ряд полезных замечаний.

Список литературы

[1] Diffie W., Hellman M. E. New directions in cryptography // IEEE Trans. Information Theory. — 1976. — 22. — P. 644–654.

[2] Rivest R. Cryptography. Chapter 13 of Handbook of Theoretical Computer Science. Vol. A: Algorithms and Complexity / ed. by J. van Leeuwen. — The MIT, 1990. — P. 717–755.

[3] Asmuth C., Bloom J. A modular approach to key safeguarding. — Mathematics Department, Texas A and M University, College Station, TX, 77844.

[4] Ko K. H., Lee S. J., Cheon J. H., Han J. W., Kang J., Park C. New public-key cryptosystem using braid groups // Advances in Cryptology — CRYPTO. — 2000.

[5] Stickel E. A New Method for Exchanging Secret Keys // Proc. of the Third Intern. Conf. on Information Technology and Applications (ICITA 05). — 2005. — Contemp. Math. 2, IEEE Computer Society. — P. 426–430.

[6] Alvarez R., Martinez F. M., Vicent J. F., Zamora A. A Matricial Public Key Cryptosystem with Digital Signature // WSEAS Trans. on Math. — 2008. — 4, No. 7. — P. 195–204.

[7] Shpilrain V., Ushakov A. Thompson's group and public key cryptography // Applied Cryptography and Network Security — ACNS 2005. — Springer, 2005. — 3531 of Lecture Notes Comp. Sc. — P. 151–164.

[8] Romanczuk U., Ustimenko V. On the PSL2(q), Ramanujan graphs and key exchange protocols. [Эл. ресурс]. — URL: http://aca2010.info/index.php/aca2010/aca2010/paper/viewFile/80/3.

[9] Mahalanobis A. The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups // Israel J. Math. — 2008. — 165. — P. 161–187.

[10] Habeeb M., Kahrobaei D., Koupparis C., Shpilrain V. Public key exchange using semidirect product of (semi)groups // arXiv math.: 1304.6572v1 [cs.CR]. — 24 Apr. 2013. — P. 1–12.

[11] Wang L., Wang L., Cao Z., Okamoto E., Shao J. New constructions of public-key encryption schemes from conjugacy search problems // Information security and cryptology. — Springer, 2010. — 6584 of Lecture Notes Comp. Sc. — P. 1–17.

[12] Романьков В. А. Алгебраическая криптография. — Омск: Омский государственный университет, 2013.