Простой алгоритм обмена ключами и трех проходной алгоритм шифрования, на модулях над кольцами.

С.Ф. Кренделев
Новосибирский Государственный Университет
JetBrains
2017 г.

Введение

- Ожидаемое развитие квантовых компьютеров привело к интенсивному развитию практических схем криптографических примитивов под названием Постквантовая криптография.
- 6 февраля 2016 г. National Institute of Standards and Technology (NIST) предложил начать разработку новых стандартов для использования Постквантовой криптографии в государственных нуждах.
- Согласно документу NIST к риску вскрытия относятся крипто примитивы, основанные на сложности дискретного логарифмирования.
- Это значит, что нужно менять алгоритм обмена ключами Диффи-Хеллмана в TLS протоколе.

- В настоящее время предлагаются алгоритмы обмена ключами, основанные на теории решеток (LWE, RLWE), которые используется в алгоритмах обмена ключами под названием “Hew hope”, “Frodo”.
- Эти варианты поддерживает Google, для построения TLS в рамках использования Постквантовой криптографии.
- Использование методов эллиптической криптографии согласно NIST является уязвимым.

- Отметим, что существует много разнообразных методов для построения алгоритма Диффи - Хеллмана для различного вида конечных групп, в основном это группы, построенные на основе некоторых подгрупп в полной группе обратимых матриц. Здесь основная проблема с реализацией.
- В работе рассматривается вариант объединения матричных колец и представлении матричных колец в некоторых модулях в духе теории представления симметрических групп.

- Чтобы не загромождать работу частными деталями рассматривается только представление в кососимметрических модулях. В этом случае можно использовать простейшие методы из линейной алгебры.

Модуль кососимметрических тензоров

Опишем основной пример модуля. Зафиксируем некоторое коммутативное кольцо с единицей R. Введем стандартный модуль R^n над кольцом R. Обозначим через $\xi_1, \xi_2, ..., \xi_n$ некоторый базис модуля R^n. Введем множество матриц размера $n \times n$ с элементами из кольца R, $Mat(R, n)$.

Со всяким модулем R^n можно связать новый модуль по следующему правилу. Выберем некоторое число $0 \le \mathrm{k} \le \mathrm{n}$, введем Грассманово произведение векторов $\wedge$ (другое название внешнее произведение векторов). Данное произведение обладает свойством $\xi_i \wedge \xi_i = 0, \xi_i \wedge \xi_j = -\xi_j \wedge \xi_i \quad \mathrm{i} \ne \mathrm{j}$. Теперь выберем набор чисел $1 \le i_1 < i_2 < \ldots < i_k \le \mathrm{n}$, сопоставим этому набору, набор $\xi_{i_1} \wedge \xi_{i_2} \wedge \ldots \wedge \xi_{i_k}$. Всевозможные такие наборы образуют базис модуля, который обозначается $\Lambda(n,k)$. Нетрудно заметить, что размерность этого модуля равна $\dfrac{n!}{k!(n-k)!}$.

Пусть $\mathbf{A} \in Mat(R,n)$, очевидно, что всякой такой матрице соответствует матрица $C_k(\mathbf{A}) \in Mat(R, \frac{n!}{k!(n-k)!})$. Элементы матрицы $C_k(\mathbf{A})$ состоят из всевозможных миноров размера $k \times k$ матрицы $\mathbf{A}$.

Имеют место следующие свойства матрицы $C_k(\mathbf{A})$

1. $\forall \mathbf{A}, \mathbf{B} \in Mat(R,n) \quad C_k(\mathbf{AB}) = C_k(\mathbf{A})C_k(\mathbf{B})$
2. $\forall \lambda \in R \quad C_k(\lambda \mathbf{A}) = \lambda^k C_k(\mathbf{A})$
3. Если $\mathbf{A}, \mathbf{B} \in Mat(R,n)$, то равенство $C_k(\mathbf{A}+\mathbf{B}) = C_k(\mathbf{A}) + C_k(\mathbf{B})$, вообще говоря, не имеет место.
4. Если $\mathbf{I} \in Mat(R,n)$ - единичная матрица, то $C_k(\mathbf{I})$ единичная матрица в $Mat(R, \frac{n!}{k!(n-k)!})$.
5. Если матрица $\mathbf{A}$ обратимая, то $C_k(\mathbf{A}^{-1}) = C_k(\mathbf{A})^{-1}$
6. $\det C_k(\mathbf{A}) = [\det(\mathbf{A})]^{\mu}$ где $\mu = \frac{(n-1)!}{(k-1)!(n-k-1)!}$.

Можно считать, что $C_k(\mathbf{A}) = \mathbf{A} \wedge \mathbf{A} \wedge \ldots \wedge \mathbf{A}$ (внешнее произведение берется k раз).

Описание протокола обмена ключами.

Алиса и Боб хотят обменяться ключами.

Алиса выбирает числа n, k, кольцо R, матрицу $\mathbf{A} \in Mat(R,n)$, и элемент $\boldsymbol{\omega} \in \Lambda(n,k)$. Вычисляет многочлен $f(\mathbf{A}) = \mathbf{S}$, и элемент $\boldsymbol{\omega}_1 = C_k(\mathbf{S})\boldsymbol{\omega} \in \Lambda(n,k)$. Посылает Бобу $\mathrm{n}, k, R, \mathbf{A}, \boldsymbol{\omega}, \boldsymbol{\omega}_1$.

Боб вычисляет многочлен $\mathbf{T} = g(\mathbf{A})$, вычисляет два элемента $\boldsymbol{\omega}_2 = C_k(\mathbf{T})\boldsymbol{\omega} \in \Lambda(n,k)$ и $\boldsymbol{\omega}_3 = C_k(\mathbf{T})\boldsymbol{\omega}_1 \in \Lambda(n,k)$. Элемент $\boldsymbol{\omega}_3$ оставляет себе, элемент $\boldsymbol{\omega}_2$ отправляет Алисе.

Алиса вычисляет $\boldsymbol{\omega}_4 = C_k(\mathbf{S})\boldsymbol{\omega}_2 \in \Lambda(n,k)$. В силу того, что матрицы $\mathbf{S}, \mathbf{T}$ коммутируют, $\boldsymbol{\omega}_4 = \boldsymbol{\omega}_3$. Тем самым коэффициенты элементов являются общим ключом. Для усиления стойкости желательно, что матрицы $\mathbf{S}, \mathbf{T}$ были необратимы.

Описание трех проходного протокола.

Алиса в качестве открытого ключа предлагает кольцо R и генерирует некоторую матрицу $\mathbf{A} \in Mat(R, n)$.

Боб знает кольцо R, в силу того, что ему известно число n, он может взять любое число k, следовательно, использовать модуль $\Lambda(n, k)$. Предположим, что $\boldsymbol{\omega} \in \Lambda(n, k)$ является сообщением, которое Боб хочет передать. Боб выбирает многочлен и строит обратимую матрицу $\mathbf{T} = g(\mathbf{A})$. После чего посылает элемент $\boldsymbol{\omega}_1 = C_k(\mathbf{T})\boldsymbol{\omega}$ Алисе.

Алиса строит обратимую матрицу $\mathbf{S} = f(\mathbf{A})$ и возвращает

$$\boldsymbol{\omega}_2 = C_k(\mathbf{S})\boldsymbol{\omega}_1 = C_k(\mathbf{S})C_k(\mathbf{T})\boldsymbol{\omega} = C_k(\mathbf{ST})\boldsymbol{\omega} = C_k(\mathbf{TS})\boldsymbol{\omega}$$

Боб вычисляет

$$\boldsymbol{\omega}_3 = C_k(\mathbf{T}^{-1})\boldsymbol{\omega}_2 = C_k(\mathbf{T}^{-1})C_k(\mathbf{TS})\boldsymbol{\omega} = C_k(\mathbf{T}^{-1}\mathbf{TS})\boldsymbol{\omega} = C_k(\mathbf{S})\boldsymbol{\omega}$$

И возвращает $\boldsymbol{\omega}_3$ Алисе.

Алиса вычисляет $C_k(\mathbf{S}^{-1})\boldsymbol{\omega}_3 = C_k(\mathbf{S}^{-1})C_k(\mathbf{S})\boldsymbol{\omega} = \boldsymbol{\omega}$ и читает посланное сообщение.

Игрушечный пример.

Будем обозначать через R одно из колец Z, Z_n. Рассмотрим модули R^3.

Пусть ξ_1, ξ_2, ξ_3 стандартный базис в R^3. Введем стандартный базис в модуле $\Lambda(3,2)$, базис имеет вид $\xi_1 \wedge \xi_2, \xi_1 \wedge \xi_3, \xi_2 \wedge \xi_3$

Предположим, что выбрана матрица (открытый ключ)

$$\mathbf{A} = \begin{pmatrix} 2 & -1 & 3 \\ -3 & 1 & 5 \\ 2 & 0 & 4 \end{pmatrix}$$

Вычислим

$$\mathbf{A}^2 = \begin{pmatrix} 13 & -3 & 13 \\ 1 & 4 & 16 \\ 12 & -2 & 22 \end{pmatrix}$$

Теперь построим секретную матрицу

$\mathbf{S}=7\mathbf{E}-11\mathbf{A}+23\mathbf{A}^2$ набор $(7,-11,23)$ является секретным ключом

$$\mathbf{S}=7\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - 11\begin{pmatrix} 2 & -1 & 3 \\ -3 & 1 & 5 \\ 2 & 0 & 4 \end{pmatrix} + 23\begin{pmatrix} 13 & -3 & 13 \\ 1 & 4 & 16 \\ 12 & -2 & 22 \end{pmatrix}$$

Или

$$\mathbf{S} = \begin{pmatrix} 284 & -58 & 266 \\ 56 & 88 & 258 \\ 254 & -46 & 469 \end{pmatrix}$$

Предположим, что нужно передать секретное сообщение, которое записывается в виде

$$\boldsymbol{\omega} = 11\xi_1 \wedge \xi_2 + 8\xi_1 \wedge \xi_3 - 5\xi_2 \wedge \xi_3; \boldsymbol{\omega} \in \Lambda(3,2)$$

Данное выражение запишем в виде вектора

$$(11, 8, -5)$$

Индуцированное преобразование выглядит так

$$\mathbf{S}^*\boldsymbol{\omega} = 11(\mathbf{S}\xi_1) \wedge (\mathbf{S}\xi_2) + 8(\mathbf{S}\xi_1) \wedge (\mathbf{S}\xi_3) - 5(\mathbf{S}\xi_2) \wedge (\mathbf{S}\xi_3)$$

Имеют место следующие соотношения

$$\mathbf{S}\xi_1 = \begin{pmatrix} 284 \\ 56 \\ 254 \end{pmatrix} = 284\xi_1 + 56\xi_2 + 254\xi_3$$

$$\mathbf{S}\xi_2 = \begin{pmatrix} -58 \\ 88 \\ -46 \end{pmatrix} = -58\xi_1 + 88\xi_2 - 46\xi_3$$

$$\mathbf{S}\xi_3 = \begin{pmatrix} 266 \\ 258 \\ 469 \end{pmatrix} = 266\xi_1 + 258\xi_2 + 469\xi_3$$

Теперь вычисляем в новом базисе модуля

$$(\mathbf{S}\xi_1)\wedge(\mathbf{S}\xi_2)=(284\xi_1+56\xi_2+254\xi_3)\wedge(-58\xi_1+88\xi_2-46\xi_3)=$$
$$(284\times 88-56\times(-58)\xi_1\wedge\xi_2+(284\times(-46)\text{-}254\times(-58))\xi_1\wedge\xi_3+$$
$$(56\times(-46)\text{-}254\times 88)\xi_2\wedge\xi_3=28240\xi_1\wedge\xi_2+1668\xi_1\wedge\xi_3\text{-}24928\xi_2\wedge\xi_3$$

Заметим, что на самом деле коэффициенты при базисных векторах в модуле $\Lambda(3,2)$ это соответствующие миноры матрицы

$$\begin{pmatrix} 284 & \text{-}58 \\ 56 & 88 \\ 254 & -46 \end{pmatrix}$$

Теперь для вычисления $(\mathbf{S}\xi_1)\wedge(\mathbf{S}\xi_3)$ рассмотрим матрицу

$$\begin{pmatrix} 284 & 266 \\ 56 & 258 \\ 254 & 469 \end{pmatrix}$$

Тогда

$$(\mathbf{S}\xi_1)\wedge(\mathbf{S}\xi_3)=58376\xi_1\wedge\xi_2+65632\xi_1\wedge\xi_3\text{-}39268\xi_2\wedge\xi_3$$

Наконец вычислим $(\mathbf{S}\xi_2)\wedge(\mathbf{S}\xi_3)$. Для этого введем матрицу

$$\begin{pmatrix} \text{-}58 & 266 \\ 88 & 258 \\ -46 & 469 \end{pmatrix}$$

Тогда

$$(\mathbf{S}\xi_2)\wedge(\mathbf{S}\xi_3)=-53336\xi_1\wedge\xi_2-14966\xi_1\wedge\xi_3+11868\xi_2\wedge\xi_3$$

Получаем результат

$$\mathbf{S}^*\boldsymbol{\omega}=1043932\xi_1\wedge\xi_2+618234\xi_1\wedge\xi_3-647692\xi_2\wedge\xi_3$$

Следовательно, вектор $(11,8,-5)$ переходит в вектор $(1043932,618234,-647692)$.

По смыслу конструкции злоумышленник знает входной и выходной вектора, и открытую матрицу $\mathbf{A}$. В данном случае возможная атака выглядит так. Если злоумышленнику известно три линейно независимых входа и выхода (в данном случае матрицы размера 3×3), то он может определить индуцированную матрицу $\mathbf{S}^*$. Отсюда мораль при каждом пересылке надо менять матрицу $\mathbf{S}$.

Если секретная матрица для всякой пересылке меняется, то надо получить матрицу $\mathbf{S}$ из информации, которая доступна только один раз. Ему точно известно, что матрица $\mathbf{S}$ выражается как многочлен от матрицы $\mathbf{S}$. Поскольку рассматриваются матрицы размера 3×3, то любая матрица может быть представлена в виде

$$\mathbf{S}=x\mathbf{E}+y\mathbf{A}+z\mathbf{A}^2$$

Или в явном виде

$$\mathbf{S}=x\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}+y\begin{pmatrix}2&-1&3\\-3&1&5\\2&0&4\end{pmatrix}+z\begin{pmatrix}13&-3&13\\1&4&16\\12&-2&22\end{pmatrix}=$$

$$\begin{pmatrix}x+2y+13z & -y-3z & 3y+13z\\ -3y+z & x+y+4z & 5y+16z\\ 2y+12z & -2z & x+4y+22z\end{pmatrix}$$

Отсюда можно получить матрицы для вычисления определителей миноров.

$$\begin{pmatrix}x+2y+13z & -y-3z\\ -3y+z & x+y+4z\\ 2y+12z & -2z\end{pmatrix}\begin{pmatrix}x+2y+13z & 3y+13z\\ -3y+z & 5y+16z\\ 2y+12z & x+4y+22z\end{pmatrix}\begin{pmatrix}-y-3z & 3y+13z\\ x+y+4z & 5y+16z\\ 2z & x+4y+22z\end{pmatrix}$$

Первое уравнение, которое получается при анализе исходного примера

$$11[(x+2y+13z)(x+y+4z)-(-y-3z)(-3y+z)]+$$
$$8[(x+2y+13z)(3y+13z)-(3y+13z)(-3y+z)]+$$
$$-5[(-y-3z)(5y+16z)-(x+y+4z)(3y+13z)]=1043932$$

Естественно скобки придется раскрыть.

Данное уравнение является нелинейным уравнением второго порядка для трех переменных. Естественно к нему нужно добавить еще два уравнения. В результате получается система из трех уравнений для трех неизвестных. Известно, что задача решения полиномиальных уравнений над целыми числами является трудной

Этот же пример можно рассматривать над кольцом Z_p.

Заключение.

Достоинства

Для всякой матрицы существует много вариантов построения модулей. Это означает, что тип модуля можно выписать в открытом ключе.

Кроме того, для реализации трех проходного протокола отправляющий сообщения может предложить свой вариант модуля. Для владельца открытого ключа не важно, какой модуль выбран.

Недостатки

Основная, пока нерешенная проблема, заключается в эффективной реализации данного варианта криптографических примитивов.

Благодарю за внимание.

Вопросы?