

О матричном шифровании (критика криптосистемы Ероша и Скуратова)

И.Л. Ерош и В.В.Скуратов предложили способ симметричного шифрования, разделения получателей и ряд других криптографических протоколов, основанных на циклической группы матриц над полем \mathbb{F}_2 . Показано, что шифр взламывается с полиномиальной сложностью, а задача Диффи-Хеллмана на группе матриц размера $n \times n$ сводится к задаче дискретного логарифмирования в поле характеристики 2, состоящем не более чем из 2^n элементов. Взлом соответствующего протокола осуществляется алгоритмом Копперсмита с малой сложностью.

Rostovtsev A.G.,
SPbSPU

On matrix encryption (critics of Erosh and Skuratov cryptosystem)

I.L. Erosh and V.V. Skuratov proposed symmetric cipher, addressed communication method using cyclic group of matrices over field \mathbb{F}_2 and some other cryptographic protocols. It is shown that cipher can be broken in polynomial time. Diffie—Hellman problem for $n \times n$ matrix can be reduced to discrete logarithm problem in field of characteristic two, that has at most 2^n elements. Corresponding protocol can be broken by Coppersmith's algorithm with small complexity.

1. Криптосистема Ероша и Скуратова

Криптография — «модная» дисциплина, положения которой обладают кажущейся внешней простотой. Однако работа в области криптографии требует глубоких профессиональных знаний в различных областях математики — алгебры, теории сложности, теории чисел, алгебраической геометрии. В основе безопасности шифров лежат сложные математические задачи. Решение такой задачи приводит к взлому шифра. Мера безопасности шифра называется стойкостью и определяется как сложность наилучшего алгоритма, решающего данную задачу. Общепризнанным требованием к шифрам является обеспечение заданного уровня стойкости по отношению к криптоанализу на основе известных и даже подобранных открытых текстов, которые задним числом можно купить, украсть или добыть иным способом [1]. При этом шифртексты по определению известны нарушителю.

Множество задач, положенных в основу безопасности криптосистем, постоянно растет, иногда предлагается в основу безопасности положить слабые задачи.

В статье И.Л. Ероша и В.В. Скуратова [2] предлагается строить блочные шифры на основе обратимых матриц над полем \mathbb{F}_2 из двух элементов. Если x , y — векторы, представляющие соответственно открытый и зашифрованный текст, а M — шифрующая матрица, то шифрование задается уравнением $y =$

Mx . Расшифрование задается уравнением $x = M^{-1}y$. Ключом шифрования является матрица M . В качестве обоснования такого способа шифрования приводится простота программной и аппаратной реализации и высокая скорость шифрования. Авторы полагают, что такое шифрование быстрее, чем шифрование с помощью обычного блочного шифра. Размер матрицы предлагается выбрать около 100×100 . Авторы предлагают алгоритм генерации невырожденной матрицы, содержащей примерно равное число нулей и единиц.

Невырожденные матрицы размера $n \times n$ над полем \mathbb{F}_2 образуют конечную группу. Пусть N — порядок группы. Авторы приводят оценку $N = 2^{n^2-2}$. Поскольку это число велико, авторы считают, что вычислить точное значение порядка группы сложно.

Для разделения получателей авторы предлагают в качестве шифрующих матриц использовать элементы циклической группы $\langle M \rangle$, образованной матрицей M . Пусть порядок циклической группы, образованной матрицей M , равен $m = \prod_{i=1}^k p_i$. Тогда пользователь i получает матрицу расшифрования

$M_i = M^{-p_i}$, а матрица шифрования равна M^{p_i} .

Для установления сеансовых ключей в системе авторы предлагают использовать протокол Диффи — Хеллмана в циклической группе матриц $\langle M \rangle$, где матрица M считается общедоступной. При этом пользователь A вырабатывает случайный показатель x , вычисляет матрицу M^x и посылает пользователю B , пользователь B вырабатывает случайный показатель y , вычисляет матрицу M^y и посылает пользователю A . Затем оба пользователя возводят полученные матрицы в свои степени и получают общую матрицу $M^{xy} = M^{yx}$. Поскольку число невырожденных матриц велико, авторы утверждают, что вычисление ключа имеет переборную сложность.

Перечислим еще раз утверждения авторов, касающиеся новизны и безопасности системы.

1. Шифрование с помощью линейного преобразования является новым.
2. Шифрование с помощью умножения матрицы размером примерно 100×100 на вектор позволяет обеспечить безопасность.
3. Найти точное значение порядка группы матриц сложно.
4. Сеансовый ключ, установленный протоколом Диффи—Хеллмана на циклической группе матриц размера порядка 100×100 , сложно вскрыть.

Покажем, что ни одно из этих утверждений не соответствует действительности.

2. Шифрование с помощью матриц не является ни новым, ни безопасным.

Шифрование с помощью матриц рассматривается в работе А. Конхейма [3] и поэтому новым не является. В этой же работе показано, что такое шифрование не может обеспечить безопасность.

Пусть матрица M имеет размер $n \times n$ и нарушитель знает несколько открытых текстов \mathbf{x}_i и соответствующих зашифрованных текстов \mathbf{y}_i . Линейность шифра приводит к тому, что выполняется равенство $M(\mathbf{x}_i + \mathbf{x}_j) = M\mathbf{x}_i + M\mathbf{x}_j$. Таким образом, сумму открытых текстов соответствует сумма зашифрованных текстов. Если среди открытых текстов содержится n линейно независимых, то нарушитель методом гауссова исключения может найти линейные комбинации текстов, соответствующие векторам $(1, 0, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$, \dots , $(0, 0, \dots, 0, 1)$. Тогда соответствующие линейные комбинации шифртекстов дадут столбцы шифрующей матрицы. Сложность гауссова исключения не превышает $O(n^3)$. Поэтому для $n = 100$ вскрытие ключа осуществляется со сложностью порядка 10^6 , то есть практически мгновенно. Таким образом, предложенный способ шифрования не обеспечивает безопасность.

3. Порядок группы матриц и циклической подгруппы можно вычислить

Теорема 1. Порядок группы невырожденных матриц размера n над \mathbb{F}_2 равен

$$N = \prod_{i=0}^{n-1} (2^n - 2^i). \quad (1)$$

Доказательство. Следующий алгоритм позволяет построить любую невырожденную матрицу. Первая строка невырожденной матрицы может быть любым ненулевым вектором длины n бит, всего $2^n - 2^0$ вариантов. Вторая строка — любой, кроме нулевой и первой, всего $2^n - 2^1$ вариантов. Третья строка — любой, кроме нулевой, первой, второй и их суммы, всего $2^n - 2^2$ вариантов. Далее по индукции. Число вариантов для последней строки — $2^n - 2^{n-1}$. **□**

Порядок циклической подгруппы является делителем числа N . Согласно (1) нечетные делители порядка группы имеют вид $2^k - 1$. Если $k = lm$, то $2^k - 1$ делится на $2^l - 1$ и на $2^m - 1$. Поэтому достаточно рассмотреть разложение чисел $2^k - 1$ только для простых k . Разложение на множители таких чисел для предложенного авторами размера задачи не составляет труда и выполняется на персональном компьютере за доли секунды с использованием стандартных математических пакетов. Поскольку количество простых чисел, не превышающих n , невелико, для задач большего размера можно использовать таблицу разложений чисел $2^k - 1$ для простых k . Таким образом, можно найти разложение порядка группы

$$N = \prod_i p_i^{\alpha_i} \quad (2)$$

на простые множители p_i . Отметим, что число различных простых делителей невелико и близко к числу $O(\log(\log N))$.

Покажем, что порядок циклической группы, образованной данной матрицей M , можно легко вычислить. По определению $M^N = E$ — единичная матрица. Вычисление порядка группы будем проводить следующим алгоритмом.

1. Вычислим матрицы $M_i = M^{\frac{N}{p_i^{\alpha_i}}}$ методом возведений в квадрат и умножений для всех индексов i , входящих в разложение (2). В найденном множестве матриц выбираем подмножество S матриц, отличных от единичной. Тогда множество индексов i матриц из S даст список простых делителей порядка группы. Сложность вычисления множества S не превышает $O(\log N)$.
2. Возводим матрицы $M_i \in S$ в степени p_i, p_i^2, \dots до получения единичной матрицы. Пусть единичная матрица получается при возведении M_i в степень $p_i^{\beta_i}$. Тогда порядок циклической группы, образованной матрицей M , равен $\# \langle M \rangle = m = \prod_i p_i^{\beta_i}$. Сложность этого этапа не выше $O(\log(\log N))$.

Сложность алгоритма в целом не превышает $O(\log N)$. Поэтому порядок циклической группы матриц и его разложение на простые множители эффективно вычислимы. Отсюда следует, что утверждение авторов, будто вычисление порядка циклической группы матриц — переборная задача, неверно.

4. Сеансовый ключ легко вскрывается

В третьей части статьи предлагается протокол Диффи—Хеллмана для установления сеансового ключа на основе циклической группы матриц. Для обеспечения приемлемой стойкости порядок циклической группы, образованной матрицей M должен быть не просто «большим», как утверждается в статье, а большим простым числом, так как в противном случае сеансовый ключ находится легко алгоритмом Сильвера—Полига—Хеллмана (см. [4]). Таким образом, все простые делители порядка группы, кроме максимального, являются балластом и не влияют на стойкость.

Тогда наилучшим выбором является использование матриц размера $n \times n$, где число n является простым, а число $2^n - 1$ имеет большой простой делитель.

Покажем, что предложенный в работе [2] подход к построению протокола Диффи—Хеллмана неэффективен. Для вычисления ключа достаточно решить задачу дискретного логарифмирования в группе матриц: найти показатель x такой, что $L = M^x$.

Теорема 2. Степени невырожденной матрицы X над \mathbb{F}_2 образуют коммутативное кольцо характеристики 2 с единицей.

Доказательство. Умножение матриц ассоциативно и дистрибутивно относительно сложения. Поэтому матрицы образуют кольцо. В силу равенства $M + M = 0$ для всех M характеристика кольца равна 2. Из (1) получаем $X^N = 1$ —

единичная матрица. Коммутативность кольца указанных матриц следует из равенства $X^i X^j = X^j X^i = X^{i+j}$ и дистрибутивности умножения матриц относительно сложения. **□**

Теорема 3. Если матрица X размера $n \times n$ имеет нечетный порядок, равный $2^n - 1$, то кольцо матриц, образованное матрицей X , изоморфно полю из 2^n элементов.

Доказательство. Матрица X над полем \mathbb{F}_2 является корнем полинома $X^{2^n} + X$. Этот полином раскладывается на простые множители над полем \mathbb{F}_2 . Из теории конечных полей известно, что эти простые множители состоят в точности из неприводимых полиномов степени n и неприводимых полиномов, степень которых делит n . Тогда матрица X является корнем в точности одного из неприводимых полиномов $p(X)$ степени n . Поскольку $p(X)$ не раскладывается на множители, то он образует максимальный идеал, кольцо классов вычетов по которому изоморфно полю из 2^n элементов. **□**

Кольцо матриц, порожденное матрицей X , представляет собой множество матричных полиномов вида $\mathbb{F}_2[X] = \left\{ \sum_{i \geq 0} a_i X^i \right\}$ и является конечным. Из элементов этого кольца можно строить частные $\frac{A}{B} = AB^{-1}$, где B — обратимая матрица. Домножая равенство $AB = BA$ справа и слева на B^{-1} , получим равенство $B^{-1}ABB^{-1} = B^{-1}BAB^{-1}$, откуда $B^{-1}A = AB^{-1}$. Присоединение частных к исходному кольцу дает коммутативное кольцо частных R_X .

Следствие 4. Если матрица X размера $n \times n$ имеет нечетный порядок r , делящий число $2^n - 1$ и не делящий ни одно из чисел $2^k - 1$, $k < n$, то кольцо частных R_X изоморфно полю из 2^n элементов, а циклическая группа, образованная матрицей X , изоморфна мультипликативной подгруппе поля.

Следовательно, при анализе безопасности предлагаемого криптоалгоритма вместо циклической группы матриц можно рассматривать изоморфную ей группу $\mathbb{F}_{2^k}^*$ или ее подгруппу. Дискретный логарифм в группе $\mathbb{F}_{2^k}^*$ вычисляется сравнительно легко алгоритмом Копперсмита [5], сложность которого равна $S = O\left(\exp\left(\sqrt[3]{\frac{32}{9} \ln 2^n (\ln \ln 2^n)^2}\right)\right)$. По этой причине задача логарифмирования в данной группе уже 20 лет как не используется криптографами.

Применительно к предложенному размеру задачи $n = 100$ стойкость составит $1,35 \cdot 10^7$ арифметических операций в поле из 2^{100} элементов, то есть ключ может быть вскрыт за доли секунды или за несколько секунд.

В работе [2] предлагается строить цифровую подпись на основе данного шифра. Цифровая подпись по определению предполагает, что получатель

подписанного сообщения не должен иметь возможность сам сформировать правильную подпись. Очевидно, что поскольку получатель может найти ключ отправителя, то цифровую подпись невозможно сформировать указанным методом.

Литература

1. Дж. Месси. Введение в современную криптологию / ТИИЭР, т.76, №5, с. 25.
2. И.Л. Ерош, В.В. Скуратов. Адресная передача сообщений с использованием матриц над полем $GF(2)$ / Проблемы информационной безопасности. Компьютерные системы. 2004, №1, с. 72–78.
3. Konheim A. Cryptography. A Primer. — J. Wiley & Sons, New York, 1981.
4. Menezes A., Oorschot P. van, Vanstone S. Handbook of applied cryptography. — CRC Press, 1997.
5. Coppersmith D. Fast evaluation of logarithms in fields of characteristic two // IEEE Transactions on Information Theory, v. IT-30, 1984, pp. 587–594.