УДК 519

А. Н. Березин, Д. Ю. Гурьянов, Д. Н. Молдовян

ГОМОМОРФИЗМЫ КОНЕЧНЫХ ГРУПП ВЕКТОРОВ И ВЫБОР ПАРАМЕТРОВ КРИПТОСХЕМ НА ИХ ОСНОВЕ

Существуют обоснованные атаки на криптосхемы, основанные на недавно предложенной вычислительно трудной задаче, названной скрытой задачей поиска сопряженного элемента. Установлен гомоморфизм мультипликативной подгруппы конечного кольца векторов в мультипликативную группу конечного поля. При его использовании в некоторых случаях данная задача может быть разбита на две независимые: задачу поиска сопряженного элемента и задачу дискретного логарифмирования. Предложены два метода выбора параметров криптосхем для предотвращения атак на основе установленного гомоморфизма.

Мультипликативные группы векторов, гомоморфизм, скрытая задача поиска сопряженного элемента, криптография, криптосхемы с открытым ключом

Предложенная недавно [1] новая вычислительно трудная задача, называемая *скрытой задачей поиска сопряженного элемента*, задаваемая над конечными группами векторов, является перспективной в качестве нового криптографического примитива, стойкого к атакам на основе квантовых вычислений. Скрытая задача поиска сопряженного элемента является достаточно новой и малоизученной. При ее исследовании обнаружилась возможность снижения предполагаемой стойкости разбиением исходной задачи на две независимые: задачу поиска сопряженного элемента и задачу дискретного логарифмирования.

В данной статье описываются гомоморфизм **R*→F*** мультипликативной подгруппы конечного кольца векторов **R** в мультипликативную группу конечного поля $GF(p^s)$, над которым задаются векторы, и потенциально возможный гомоморфизм **R*→F′*** в мультипликативную группу **F′*** расширенного поля $GF(p^{sk})$, где $1 < k \le m$. Они налагают дополнительные ограничения на выбор параметров криптосхем, основанных на вычислениях в группах векторов. Предложены две возможные атаки на криптосхемы, основанные на скрытой задаче поиска сопряженного элемента, с использованием установленных гомоморфизмов. Разработаны требования к выбору параметров криптосхем для их предотвращения.

Гомоморфизмы конечных групп и колец. Рассмотрим конечное кольцо **R** m-мерных векторов над конечным полем $GF(p^s)$, где p^s – простое число (характеристика поля) и $s \ge 1$ – степень расширения поля. Предположим, **e**,**i**,...,**w** – некоторые m-мерные базисные векторы и $a,b,...,q \in GF(p)$ – координаты. Тогда векторы определяются как $a\mathbf{e}+b\mathbf{i}+...+q\mathbf{w}$, или как $(a,b,...,q)$. Слагаемые вида $\tau\mathbf{v}$, где $\tau \in GF(p)$ и $\mathbf{v} \in \{\mathbf{e},\mathbf{i},...,\mathbf{w}\}$, называются компонентами вектора. Сложение двух векторов осуществляется суммированием соответствующих координат:

$$(a,b,...,q)+(x,y,...,z)=(a+x,b+y,...,q+z).$$

Операция умножения векторов определяется по естественному правилу попарного перемножения всех компонент векторов-сомножителей по формуле

$$(a\mathbf{e}+b\mathbf{i}+...+q\mathbf{w})\circ(x\mathbf{e}+y\mathbf{i}+...+z\mathbf{w})=ax\mathbf{e}\circ\mathbf{e}+ay\mathbf{e}\circ\mathbf{i}+...+az\mathbf{e}\circ\mathbf{w}+$$
$$+bx\mathbf{i}\circ\mathbf{e}+by\mathbf{i}\circ\mathbf{i}+...+bz\mathbf{i}\circ\mathbf{w}+...+qx\mathbf{w}\circ\mathbf{e}+qy\mathbf{w}\circ\mathbf{i}+...+qz\mathbf{w}\circ\mathbf{w}.$$

В это выражение вместо каждого из произведений двух базисных векторов подставляется некоторый базовый вектор $\mathbf{v}$ или $\tau\mathbf{v}$ согласно специально задаваемой таблице умножения базисных векторов (ТУБВ). Таблица определяет ассоциативность операции $\circ$. Существуют различные типы ТУБВ, определяющие коммутативные* и некоммутативные кольца $\mathbf{R}$ [2].

Во всех случаях наблюдается гомоморфизм мультипликативной подгруппы конечного кольца векторов $\mathbf{R}$ (т. е. мультипликативной группы векторов $\mathbf{R^*}$) в мультипликативную группу конечного поля $GF(p^s)$, над которым задаются векторы. Этот гомоморфизм обозначим как $\mathbf{R^*}\rightarrow\mathbf{F^*}$, где $\mathbf{F^*}$ – мультипликативная группа поля $GF(p^s)$. Следующее утверждение показывает существование этого гомоморфизма.

Утверждение 1. Главный определитель системы линейных уравнений для вычисления обратного вектора $\mathbf{A}^{-1}$ к заданному вектору $\mathbf{A}$ определяет гомоморфизм $\mathbf{R^*}\rightarrow\mathbf{F^*}$.

Доказательство. Предположим, что вектор $\mathbf{A}$ обратим. Тогда векторное уравнение вида

$$\mathbf{A}\circ\mathbf{X}=\mathbf{V};(a\mathbf{e}+b\mathbf{i}...+q\mathbf{w})\circ(a'\mathbf{e}+b'\mathbf{i}...+q'\mathbf{w})=(a''\mathbf{e}+b''\mathbf{i}...+q''\mathbf{w}) \quad (1)$$

с неизвестным значением X имеет единственное решение для произвольного вектора $\mathbf{V}$:

$$\mathbf{V}:\mathbf{X}=\mathbf{A}^{-1}\circ\mathbf{V}.$$

Выражение (1) может быть представлено в виде системы из m линейных уравнений (m – размерность векторов) над полем $GF(p^s)$ с m неизвестными, которыми являются координаты вектора $\mathbf{X}$:

$$\begin{cases}\xi_{11}a'+\xi_{12}b'+...+\xi_{1m}q'=a_1'',\\ \xi_{21}a'+\xi_{22}b'+...+\xi_{2m}q'=b_2'',\\ ...\\ \xi_{m1}a'+\xi_{m2}b'+...+\xi_{mm}q'=q_m''.\end{cases} \quad (2)$$

В получившейся системе уравнений (2) коэффициенты ξ полностью определяются при перемножении координат векторов $\mathbf{A}\circ\mathbf{X}$:

$$(a\mathbf{e}+b\mathbf{i}...+q\mathbf{w})\circ(a'\mathbf{e}+b'\mathbf{i}...+q'\mathbf{w})=aa'\mathbf{e}\circ\mathbf{e}+ab'\mathbf{e}\circ\mathbf{i}+...+qq'\mathbf{w}\circ\mathbf{w}.$$

Произведения базисных векторов заменяются согласно ТУБВ ($aa'\mathbf{e}\circ\mathbf{e}=\xi a'\mathbf{e}$). Эта замена определяет место коэффициента в системе уравнений.

Пусть Δ_A является главным определителем системы линейных уравнений (2), связанных с векторным уравнением (1) с неизвестным $\mathbf{X}$, тогда Δ_A полностью определяется координатами вектора $\mathbf{A}$ и коэффициентами выбранной таблицы умножения базисных векторов:

---

* Ko Kihyoung Lee Sang jin, Cha Jaecho on, Choi Do oho Cryptosystems based on non-commutativity : # WO2001KR01283. – 13 2 2003.

$$\Delta_A = \begin{vmatrix} \xi_{11} & \xi_{12} & \cdots & \xi_{1m} \\ \xi_{21} & \xi_{22} & \cdots & \xi_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \xi_{m1} & \xi_{m2} & \cdots & \xi_{mm} \end{vmatrix}. \qquad (3)$$

Если $\mathbf{V} = \mathbf{E}$, где $\mathbf{E}$ – единичный вектор, то имеем векторное уравнение вида $\mathbf{X} = \mathbf{A}^{-1} \circ \mathbf{E}$, т. е. Δ_A является главным определителем системы линейных уравнений для вычисления обратного вектора $\mathbf{A}^{-1}$. Обозначим матрицу коэффициентов системы линейных уравнений (2) как M_A из элементов (3):

$$M_A = \begin{Vmatrix} \xi_{11} & \xi_{12} & \cdots & \xi_{1m} \\ \xi_{21} & \xi_{22} & \cdots & \xi_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \xi_{m1} & \xi_{m2} & \cdots & \xi_{mm} \end{Vmatrix}.$$

Обозначим множество всех векторов, заданных над полем $GF(p^S)$, как $\{\mathbf{V}\}$. Для любого вектора, содержащегося в $\{\mathbf{V}\}$, уравнение (1) имеет единственное решение. Тогда $\Delta_A \neq 0$ и умножение вектора $\mathbf{A}$ на все векторы из множества $\{\mathbf{V}\}$ задает линейное преобразование T_A векторного пространства:

$$\mathbf{A} \circ \mathbf{V} = \dot{\mathbf{V}}; \; T_A : (a\mathbf{e} + b\mathbf{i} ... + q\mathbf{w}) \circ (\dot{a}\mathbf{e} + \dot{b}\mathbf{i} ... + \dot{q}\mathbf{w}) = (\zeta_1 \dot{a}\mathbf{e} + \zeta_2 \dot{b}\mathbf{i} ... + \zeta_m \dot{q}\mathbf{w}).$$

Действительно, для произвольных скалярных величин $\lambda_1 \in GF(p^S)$ и $\lambda_2 \in GF(p^S)$, произвольных векторов $\mathbf{V}_1$ и $\mathbf{V}_2$ справедливо равенство

$$\mathbf{A} \circ \; \lambda_1 \mathbf{V}_1 + \lambda_2 \mathbf{V}_2 \; = \lambda_1 \mathbf{A} \circ \mathbf{V}_1 + \lambda_2 \mathbf{A} \circ \mathbf{V}_2 .$$

Матрица M_A может быть поставлена в соответствие к T_A:

$$\begin{cases} \mathbf{A} \circ \mathbf{X} \Leftrightarrow \mathbf{T}_A : \mathbf{A} \circ \mathbf{V} \\ \mathbf{A} \circ \mathbf{X} \to M_A \end{cases} \Rightarrow T_A \to M_A .$$

Некоторый другой обратимый вектор $\mathbf{B}$ определяет линейное преобразование T_B, которое соответствует матрице коэффициентов M_B, связанной с задаваемой векторным уравнением $\mathbf{X} = \mathbf{B}^{-1} \circ \mathbf{V}$ системой линейных уравнений. Операция умножения векторов группы **R*** является ассоциативной, поэтому справедливо следующее выражение:

$$(\mathbf{A} \circ \mathbf{B}) \circ \mathbf{V} = \mathbf{A} \circ (\mathbf{B} \circ \mathbf{V}). \qquad (4)$$

Левая часть этого выражения представляет собой линейное преобразование T_{AB}, соответствующее матрице M_{AB}. Правая часть выражения (4) является произведением (суперпозицией) линейных преобразований $T_B * T_A$, поэтому

$$T_{AB} = T_B * T_A \Rightarrow M_{AB} = M_A M_B \Rightarrow \Delta(\mathbf{A} \circ \mathbf{B}) = \Delta_A \Delta_B .$$

Последнее выражение задает гомоморфизм **R*→F***, что и требовалось доказать.

Выбор параметров. Установленный гомоморфизм может быть положен в основу атаки первого типа на схемы открытого шифрования и открытого распределения ключей, основанных на задаче дискретного логарифмирования в скрытой коммутативной подгруппе, заданной над некоммутативными группами векторов. Данный гомоморфизм далее будем обозначать как $\Delta(\mathbf{A}) = \Delta_A$. В этих схемах используется открытый ключ вида $Y = Q^W G^X Q^{-W}$, где пара чисел x и w составляет секретный ключ, а $Y,Q,G \in$ **R***. Применение гомоморфизма **R*→F*** к уравнению вычисления открытого ключа дает следующее соотношение:

$$\Delta_Y = \Delta_Q{}^W \Delta_G{}^X \Delta_Q{}^{-W} = \Delta_G{}^X \Delta_Q{}^W \Delta_Q{}^{-W} = \Delta_G{}^X = \Delta_G{}^{x'}. \qquad (5)$$

Отношение (5) представляет собой уравнение над полем $GF(p^s)$. Возможны 3 случая нахождения значения x' из последнего уравнения:

1. Порядок значения $\Delta_G \in GF(p^s)$ равен порядку элемента G. В этом случае секретное значение x' можно найти решив задачу дискретного логарифмирования в $GF(p^s)$. Тогда секретный элемент X можно найти решением задачи поиска сопряженного элемента. Таким образом, решение скрытой задачи поиска сопряженного элемента сводится к двум независимым известным вычислительно трудным задачам, и атака может считаться успешной.

2. Порядок значения $\Delta_G \in GF(p^s)$ меньше порядка элемента G. В этом случае часть информации о секретном ключе может быть найдена решением задачи дискретного логарифмирования в поле $GF(p^s)$. Решив уравнение $\Delta_Y = \Delta_G{}^{x'}$, можно найти значение $x' \equiv x \bmod q'$, где q' – порядок элемента $\Delta_G \in GF(p^s)$. Если значение q' достаточно велико, то решение задачи дискретного логарифмирования, задаваемое уравнением (5), позволит определить значительную часть секретного ключа.

3. Гомоморфизм отображает элемент G в единичный элемент поля $GF(p^s)$, и уравнение (5) вырождается в тривиальное уравнение $1 = 1^{x'}$, из которого не может быть получено никакой информации о секретном значении. Тогда рассматриваемая атака не снижает сложность скрытой задачи поиска сопряженного элемента.

Таким образом, способом предотвращения такой атаки является использование в качестве параметра G вектора, имеющего порядок, который не является нетривиальным делителем числа $p^s - 1$. В этом случае уравнение (5) не позволяет получить какой-либо информации о значении x, поскольку значения Δ_Y и Δ_G равны единичному элементу поля $GF(p^s)$ и выражение (5) принимает вид $1 = 1^{x'}$. Тогда справедливо следующее утверждение.

Утверждение 2. Если вектор **G** имеет порядок ω_G, такой, что НОД$(\omega_G, p^s - 1) = 1$, то $\Delta(G) = 1$.

Доказательство. Пусть E – единичный элемент группы **R***. Предположим, что $\Delta(G) \neq 1$. По условию $G^{\omega_G} = E \Rightarrow \Delta G^{\omega_G} = \Delta(E) = 1$. Тогда $\Delta G^{\omega_G} = \Delta G^{\omega_G} = 1$ и $\Delta G^{p^s - 1} = 1$. Из последних двух соотношений и предположения $\Delta_G \neq 1$ следует, что НОД $\omega_G, p^s - 1 \neq 1$, поскольку ω_G и $p^s - 1$ кратны порядку элемента $\Delta(G)$ мультипликативной группы поля $GF(p^s)$. Полученное противоречие доказывает утверждение 2.

Воспользуемся утверждением 2 для выбора элемента G в конечной некоммутативной группе четырехмерных векторов. Ее порядок определяется формулой $\Omega = p(p-1)(p^2-1)$ [3]. В этом случае можно сформировать 90-битное простое число $p = 2q - 1$, такое, что число q – простое. Тогда можно сгенерировать вектор, имеющий простой порядок, удовлетворяющий условию НОД$(\omega_G, p-1) = 1$. Если группа соответствует $m \times m$-матрицам и m-мерным векторам, выбор векторов **G**, удовлетворяющих утверждению 2, относительно прост. Такой выбор предотвращает атаки, использующие рассматриваемый гомоморфизм.

По аналогии с атакой, основанной на гомоморфизме **R*→F***, можно предложить атаку второго типа на основе потенциально возможного гомоморфизма **R*→F′***, где **F′*** – мультипликативная группа расширенного поля $GF(p^{sk})$, $1 < k \leq m$.

Наиболее простым является случай $m = 4$, когда формула для порядка **R*** группы: $\Omega = p(p-1)(p^2-1)$.

Из данной формулы легко видеть, что множитель $(p-1)$ указывает на потенциальную возможность гомоморфизма **R*→F***, а множитель (p^2-1) – на потенциальную возможность гомоморфизма **R*→F′*** при $k = 2$ (единственно возможное значение $k > 1$). Если такой гомоморфизм найден, это будет означать, что некоммутативные группы четырехмерных векторов не могут обеспечить достаточную стойкость криптосхем с открытым ключом вида $Y = Q^w \circ G^x \circ Q^{-w}$ при сравнительно малых значениях размера порядка поля $GF(p^s)$, над которым задаются векторы.

Для предотвращения атаки второго типа с использованием потенциально возможного гомоморфизма существуют 2 метода.

Первый метод состоит в использовании элемента G, имеющего порядок p. Тогда гомоморфизм **R*→F′*** отображает элемент G в единичный элемент поля $GF(p^{sk})$.

Второй метод заключается в использовании необратимых элементов N конечного кольца **R**, содержащего мультипликативную группу **R***. В качестве G используется необратимый элемент N, такой, что множество $\{N, N^2, ..., N^j, ...\}$ содержит достаточно большое число разных элементов $N^i \in \mathbf{R}$.

Применение гомоморфизма **R*→F′*** к уравнению $Y = X \circ N^X \circ X^{-1}$ дает $\Delta_Y = 0$, так как $\Delta_N = 0$. Следовательно, этот метод также эффективен для предотвращения атаки второго типа.

Таким образом, рассмотрение мультипликативных гомоморфизмов некоммутативных конечных колец **R** является важным пунктом исследований сложности скрытой задачи поиска сопряженного элемента, определенного над кольцом **R**, которое относится к оценке безопасности криптосистем, на основе данной задачи. Установлен и доказан общий мультипликативный гомоморфизм **R*→ F*** векторных конечных колец в поле $GF(p^s)$. Если кольцо m-мерных векторов представляется полем $GF(p^s)$ [4], гомоморфизм **R*→F*** совпадает с нормальным гомоморфизмом.

Рассмотрены атаки на его основе, позволяющие вычислить секретный ключ по частям. Сформулированы ограничения на выбор вектора **G**, предотвращающие атаки на основе сформулированного гомоморфизма.

При разработке конкретных криптосхем их параметры выбираются в зависимости от порядка Ω мультипликативной группы **R*** кольца **R**. В случае m-мерных векторов параметры кольца могут быть выбраны так, что безопасный размер открытого ключа примерно $4|q| \approx 320$ бит для малых $(m = 4)$ и больших $(m = 8,16,32)$ значений m.

Работа поддержана грантом РФФИ № 11-07-00004-а.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. СПб.: БХВ-Петербург, 2010.

2. Moldovyan D. N. Non-commutative finite groups as primitive of public-key cryptoschemes // Quasigroups and Related Systems. 2010. № 18. С. 165–176.

3. Молдовяну П. А., Молдовян Д. Н., Дернова Е. С. Гомоморфизмы и многомерная цикличность конечных групп векторов в синтезе алгоритмов ЭЦП // Вопр. защиты информации. М.: ФГУП "ВИМИ", 2009. № 3 (82). С. 2–7.

4. Молдовян Д. Н. Конечные некоммутативные группы как примитив криптосистем с открытым ключом // Вопр. защиты информации. М.: ФГУП "ВИМИ", 2010. № 1. С. 61–65.

A. N. Berezin, D. U. Guriyanov, D. N. Moldovyan

HOMOMORPHISMS OF FINITE GROUPS OF VECTORS AND CHOOSING THE PARAMETERS OF CRYPTOSCHEMES BASED ON THEM

There are considered attacks on cryptoschemes based on the recently proposed hard computational problem called hidden conjugacy search problem (HCSP). It is shown that in some cases the HCSP can be reduced to two independent problems, discrete logarithm and conjugacy search problem. Such attacks use homomorphisms of the multiplicative subgroup of finite rings of vectors into multiplicative group of the finite field. To prevent the attacks two variants for choosing the parameters of cryptoschemes have been proposed.

Vector multiplicative groups, homomorphism, hidden conjugacy search problem, cryptography, public-key cryptoschemes