УДК 512.54

Метод линейного разложения анализа протоколов скрытой информации на алгебраических платформах

В.А. Романьков*

1 Введение

Классическими платформами для построения криптографических систем, схем и протоколов служат кольца вычетов (системы RSA, Гольдвассера-Микали и др.), мультипликативные группы конечных полей и группы эллиптических кривых над конечными полями (системы, схемы и протоколы, основанные на трудности вычисления дискретного логарифма: протоколы шифрования Диффи-Хеллмана, Масси-Омуры и ЭльГамаля, протоколы цифровой подписи, основанные на базовой схеме ЭльГамаля, и др.). См. [1], [2] или, например, [3], [4].

В то же время последние 15-20 лет знаменуются бурным развитием алгебраической криптографии, использующей в качестве платформ шифрования абстрактные алгебраические системы: алгебры, группы, лупы и т.п. См. по этому поводу монографии [5], [6], обзорные статьи [7], [8], [9], [10], [11], [12], коллекцию препринтов [13]. Классические протоколы Диффи-Хеллмана, Масси-Омуры, ЭльГамаля и др. получили свои аналоги прежде всего в криптографии, базирующейся на теории групп, в которой в качестве платформ построения систем, схем и протоколов рассматриваются абстрактные группы, как конечные, так и бесконечные. В настоящее время все чаще для этой роли предлагаются другие алгебраические системы. Очень часто (даже можно сказать, почти всегда) эти алгебраические системы имеют структуру конечномерного линейного пространства над конечным полем. Матричные группы стали использоваться в криптографии уже в 90-е годы 20-го столетия. Во многих работах отмечалось, что такие группы имеют соответствующие необходимые свойства и хорошо подходят для вычислений.

Предлагается новый метод вычисления скрытой информации целого ряда известных криптографических протоколов, построенных на алгебрах, группах, лупах и т.п. Основы метода и многочисленные его приложения представлены в монографии автора [14] и его статье [15]. Метод работает в случаях, когда платформа является линейным пространством над конструктивным полем или может быть вложена в такое пространство. Более

*Исследование выполнено за счёт гранта Российского научного фонда (проект №14-11-00085).

того, метод применим и в более общей ситуации конечномерного модуля над конструктивным нётеровым кольцом. При этом многие структурные свойства алгебраической системы, фигурирующей в качестве платформы, игнорируются. Также предполагается, что использованные при построении протокола операции являются эндоморфизмами подлежащего линейного пространства или модуля. Таковы сопряжения, домножения с разных сторон, эндоморфизмы колец, над которыми берутся модули и т.п. Показано, что в этом случае вопреки общепринятым представлениям (и многочисленным предположениям секретности) можно обойтись без решения соответствующих алгоритмических проблем поиска. Существует алгоритм, вычисляющий секретную информацию без решения алгоритмических проблем поиска, на трудности решения которых обычно основывается предположение секретности (стойкости) протокола. Это меняет общепринятое представление об обосновании стойкости протоколов. Эффективность атаки, основанной на методе линейной разложимости, конечно зависит от целого ряда факторов и требует специального анализа в каждом конкретном случае. В общем можно только утверждать, что атака осуществима за полиномиальное время от размеров данных входа, когда платформа уже представлена как естественное линейное пространство или модуль.

В [14] описан анализ методом линейного разложения криптографических систем, схем и протоколов, основанных на сопряжениях, умножениях и автоморфизмах из работ [16], [17], [18], [19], [20], [21], [22] и ряда других протоколов. В статье автора [15] и монографии [14] приведен анализ протоколов из [23], [24], [25], [26] и ряда других работ.

В разделе 3 приведен пример анализа одного из протоколов из [27], [28], использующий одну из вариации метода линейного разложения.

2 Метод линейного разложения

Пусть V – конечномерное векторное пространство над полем $\mathbb{F}$ с базисом $\mathcal{B} = \{v_1, \ldots, v_r\}$. Пусть $\mathrm{End}(V)$ – полугруппа всех эндоморфизмов пространства V. Предполагаем, что элементы $v \in V$ записываются как векторы относительно $\mathcal{B}$, а эндоморфизмы $a \in \mathrm{End}(V)$ записываются матрицами относительно $\mathcal{B}$. Для эндоморфизма $a \in \mathrm{End}(V)$ и элемента $v \in V$ через v^a обозначаем образ элемента v относительно a. Также для любых подмножеств $W \subseteq V$ и $A \subseteq \mathrm{End}(V)$ полагаем $W^A = \{w^a | w \in W, a \in A\}$, и обозначаем через $Sp(W)$ подпространство пространства V, порожденное W. Ниже обсуждается понятие сложности некоторых алгоритмов. Всюду в дальнейшем предполагается, что элементы поля $\mathbb{F}$ даны в некоторой конструктивной форме и формально определен "размер" этой формы. Более того, предполагается, что операции основного поля $\mathbb{F}$ эффективны, в частности их результаты могут быть вычислены за полиномиальное время от размеров элементов. Будем говорить, что такие поля *конструктивны*.

Для элемента $\alpha \in \mathbb{F}$ через $\|\alpha\|$, обозначается его размер. Полагаем также $\|v\| = \max \|\alpha_i\|$ для вектора $v = (\alpha_1, \ldots, \alpha_r) \in V$, и $\|a\| = \max\{\|\alpha_{ij}\|\}$ для матрицы $a = (\alpha_{ij}) \in \mathrm{End}(V)$.

Основная лемма. *Существует алгоритм, который по данным конечным подмножествам $W \subseteq V$ и $U \subseteq End(V)$ находит базис подпространства*

$Sp(W^{\langle U\rangle})$ (здесь $< U >$ обозначает подмоноид, порождённый U) в виде $w_1^{a_1}, \ldots, w_t^{a_t}$, где $w_i \in W$ и a_i – произведение элементов из U. Более того, число полевых операций, используемых алгоритмом, полиномиально от $r = \dim_{\mathbb{F}} V$ и мощностей подмножеств W и U.

Доказательство. Используя метод Гаусса, эффективно находим максимальную линейно независимую подсистему L_0 подмножества W. Справедливо равенство $Sp(L_0^{\langle U\rangle}) = Sp(W^{\langle U\rangle})$. Добавляя к системе L_0 один за другим элементы v^a, где $v \in L_0, a \in U$, и проверяя каждый раз линейную независимость расширенного множества, эффективно строим максимальную линейно независимую подсистему L_1 множества $L_0 \cup L_0^U$, содержащего L_0. Заметим, что $Sp(L_0^{\langle U\rangle}) = Sp(L_1^{\langle U\rangle})$, и что элементы в L_1 имеют вид w или w^a, где $w \in W$ и $a \in U$. Отсюда следует, что если $L_0 = L_1$, то L_0 – базис пространства $Sp(W^{\langle U\rangle})$. Если $L_0 \neq L_1$, то повторяем процедуру для $L_1 \setminus L_0$ и находим максимальную линейно независимую подсистему L_2 множества $L_1 \cup (L_1 \setminus L_0)^U$, расширяющую L_1. Продолжая таким образом, строим строго возрастающую цепочку $L_0 < L_1 < \ldots < L_i$ линейно независимых систем. Так как размерность r пространства V конечна, цепочка закончится на шаге $i \leq r$. В этом случае L_i – базис подпространства $Sp(W^{\langle U\rangle})$. Его элементы имеют требуемую форму.

Для верхней оценки числа полевых операций, используемых алгоритмом, заметим сначала, что число операций в методе Гаусса относительно матрицы размера $n \times r$ равно $O(n^2 r)$. Следовательно, требуется $O(n^2 r)$ шагов для построения L_0 из W, где $n = |W|$– число элементов в W. Заметим, что $|L_j| \leq r$ для любого j. Поэтому для нахождения L_{j+1} достаточно рассмотреть процесс исключения Гаусса относительно матрицы соответствующей $L_j \cup L_j^U$, имеющей размер не более, чем $r + r|U|$. Таким образом верхняя оценка на это число есть $O(r^3|U|^2)$. Так как происходит не более r итераций процесса , общая оценка выглядит как $O(r^3|U|^2 + r|W|^2)$. Лемма доказана.

Следствие. *При сделанных ограничениях на поле $\mathbb{F}$ алгоритм из Основной леммы полиномиален относительно размера входа, т.е. относительно $r = \dim_{\mathbb{F}} V$, $|W|$, $|U|$ и $\max\{\|w\|, \|u\| \mid w \in W, u \in U\}$.*

Проиллюстрируем, как может проводиться атака методом линейного разложения.

Базовая модель. Пусть теперь U_1 и U_2 – два конечных подмножества в $\mathrm{End}(V)$ таких, что каждый элемент из U_1 перестановочен с любым элементом из U_2. Пусть A и B – подмоноиды в $\mathrm{End}(V)$, порожденные U_1 и U_2, соответственно. Пусть $a \in A, b \in B$ и $v \in V$. Мы предполагаем, что U_1, U_2 и векторы v, v^a, v^b открыты, в то время, как эндоморфизмы a и b секретны.

Утверждение. *Для данных U_1, U_2, v, v^a, v^b вектор $v^{ab} = v^{ba}$ находится за полиномиальное время.*

Доказательство. В самом деле, по данным U и v Основная лемма (и ее Следствие) позволяют сконструировать за полиномиальное время базис подпространства $Sp(v^A)$, где A – подмоноид, порожденный U, в виде $v^{a_1}, \ldots, v^{a_t}$, где $a_i \in A$ даны как некоторые произведения элементов из U. Используя процесс Гаусса, выразим v^a, как линейную комбинацию элементов этого базиса:

$$v^a = \Sigma_{i=1}^t \alpha_i v^{a_i}, \quad \alpha_i \in \mathbb{F}.$$

Это позволяет вычислить v^{ab} следующим образом:

$$v^{ab} = (v^a)^b = (\Sigma_{i=1}^t \alpha_i v^{a_i})^b =$$

$$\Sigma_{i=1}^t \alpha_i v^{a_i b} = \Sigma_{i=1}^t \alpha_i v^{b a_i} = \Sigma_{i=1}^t \alpha_i (v^b)^{a_i}. \quad (1)$$

Действительно, поскольку вектор v^b, матрицы a_i и коэффициенты α_i известны, правая часть равенства 1 непосредственно вычислима. Утверждение доказано.

В заключение отметим, что у нас не было необходимости вычислять ни a, ни b, чтобы вычислить вектор v^{ab}. Отметим также, что в Утверждении не нужно знать U_2, достаточно знать только, что для $b \in \mathrm{End}(V)$ справедливо равенство $[b, U_1] = 1$, т.е. он перестановочен с любым элементом из U_1.

3 Пример использования метода линейного разложения

Рассмотрим протоколы Харли из [27], [28].

1) Матричный аналог протокола Масси-Омуры: передача сообщения.

Установка:

$G \leq \mathrm{GL}_n(\mathbb{F})$ – коммутативная подгруппа – открытые данные.

Алгоритм:

1. Алиса должна передать $x \in \mathbb{F}^n$ Бобу, она выбирает $A \in G$, вычисляет и передает xA.
2. Боб выбирает $B \in G$, вычисляет и передает xAB.
3. Алиса вычисляет и передает $(xAB) \cdot A^{-1} = xB$.
4. Боб вычисляет $(xB) \cdot B^{-1} = x$.

2) Протокол аутентификации с возможностью использовать как цифровую подпись. .

Установка:

$G \leq \mathrm{GL}_n(\mathbb{F})$ – коммутативная подгруппа – открытые данные.

Алгоритм:

1. Боб выбирает $y \in \mathbb{F}^n$, $B \in G$, вычисляет и передает yB.
2. Алиса выбирает $x \in \mathbb{F}^n$, $A_1, A \in G$, вычисляет и передает (xA, yBA_1).
3. Боб выбирает $B_1, B_2 \in G$, вычисляет и передает (xAB_1, yA_1B_2).
4. Алиса вычисляет (xB_1, yB_2) и передает $xB_1 - yB_2$.
5. Боб находит $x - yB_2B_1^{-1}$ и вычисляет x.

Боб может использовать yB для сообщений с другими пользователями.

Криптографический анализ:

Проведем анализ более сложного протокола 2). Анализ протокола передачи сообщения аналогичен.

1. Строим базис пространства $(yBA_1)G : yBA_1C_1, ..., yBA_1C_r$.
2. Разлагаем: $yB = \sum_{i=1}^{r} \alpha_i yBA_1C_i, \alpha_i \in \mathbb{F}$.
3. Подставляем вместо yBA_1 вектор $yA_1B_2 : \sum_{i=1}^{r} \alpha_i yA_1B_2C_i = yB_2$.
4. Строим базис пространства $(xAB_1)G : xAB_1D_1, ..., xAB_1D_t$.
5. Разлагаем: $xA = \sum_{i=1}^{t} \beta_i xAB_1D_i, \beta_i \in \mathbb{F}$.
6. Подставляем вместо xAB_1 вектор $xB_1 - yB_2 : \sum_{i=1}^{t} \beta_i (xB_1 - yB_2)D_i = x - yB_2B_1^{-1}$.
7. Еще раз подставляем вместо xAB_1 вектор $yB_2 : \sum_{i=1}^{t} \beta_i yB_2D_i = yB_2B_1^{-1}$.
8. Вычисляем x.

Замечание. Часто группа (или другая алгебраическая система), выбранная в качестве платформы для криптографического протокола, задана абстрактно. Например, она конечная, полициклическая, группа кос Артина или другая группа, допускающая точное представление матрицами над конструктивным полем. Тогда для применения метода линейного разложения необходимо использовать её эффективное вложение в кольцо матриц. Но тогда и результат будет иметь матричный вид. Для получения результата в исходном представлении нужно уметь переходить к прообразам матричных элементов. Если существует эффективная процедура записи образа произвольного элемента через образы порождающих элементов группы, то прообраз эффективно вычисляется как соответствующее слово от порождающих элементов исходной группы. Существует много работ, в которых строятся эффективные алгоритмы нахождения такого сорта. См., например, обзорные статьи [29] и [30], а также и библиографию в них. Приведу цитату из [29]: "A costructive membership test not only answers the question whether or not a given element belongs to a given group but in the case of positive answer, it also provides a straight-line program that constructs the given element from the given generators of the group."Это как раз то, что нужно для перехода к прообразам, о необходимости которого говорилось выше.

Список литературы

[1] *W. Diffie, M.E. Hellman,* New directions in cryptography, IEEE Transaction Information Theory, **22** (1976), 644-654.

[2] *T. ElGamal,* A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, **IT-31**, №4 (1985), 469-472.

[3] *М.М. Глухов, А.В. Черемушкин, И.А. Круглов, И.А. Пичкур,* Введение в теоретико-числовые методы криптографии, Санкт-Петербург, Лань, 2011.

[4] *В.А. Романьков,* Введение в криптографию, Курс лекций, М., Форум, 2012.

[5] *A.G. Miasnikov, V. Shpilrain, A. Ushakov,* Group-based Cryptography, Advanced Courses in Math., CRM Barselona, Basel, Birkhauser, 2008.

[6] *A.G. Miasnikov, V. Shpilrain, A. Ushakov,* Non-commutative Cryptography and Complexity of Group Theoretic Problems, Mathematical Surveys and Monographs, Providence R.I., Amer. Math. Soc., 2011.

[7] *P. Dehornoy,* Braid-based cryptography, In: Group theory, statistics and cryptography, Contemp. Math., **360**, Providence R.I., Amer. Math. Soc., 2004, 5-33.

[8] *V. Shpilrain, G. Zapata,* Combinatorial group theory and public key cryptography, Applicable Algebra in Engineering Communication and Computing, **17** (2006), 291-302.

[9] *Shpilrain V., Zapata G.* Using decision problems in public key cryptography, Groups. Complexity. Cryptology, **1** (2009), 33-40.

[10] *В.А. Романьков,* Диофантова криптография на бесконечных группах, Прикл. дискр. мат., №2 (2012), 15-42.

[11] *B. Fine, M. Habeeb, D. Kahrobaei, G. Rosenberger,* Survey and open problems in non-commutative cryptography, JP Journal of Algebra, Number Theory and Applications, **21** (2011), 1-40.

[12] *V. Shpilrain, A. Ushakov,* The conjugacy search problems in public key cryptography: unecessary and insufficient, Applicable Algebra in Engineering Communication and Computing, **17** (2006), 285-289.

[13] *V. Shpilrain,* www.grouptheory.info/PersonalPages/Shpilrain, Vladimir/Cryptology ePrint Archive

[14] *В.А. Романьков,* Алгебраическая криптография, Омск, ОмГУ, 2013.

[15] *В.А. Романьков,* Криптографический анализ некоторых схем шифрования использующих автоморфизмы, Прикл. дискр. мат. №3 (2013), 36-51.

[16] *K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang, C. Park,* New public-key cryptosystem using braid groups, In: Advances in Cryptology - CRYPTO 2000, **1880** of Lecture Notes Comp. Sc., Berlin, Springer, 2000, 166-183.

[17] *M. Habeeb, D. Kahrobaei, C. Koupparis, V. Shpilrain,* Public key exchange using semidirect product of (semi)groups, Preprint: arXiv math.: 1304.6572v1[cs.CR], 24 Apr. 2013, 1-12.

[18] *D. Kahrobaei, B. Khan,* A Non-Commutative Generalization of ElGamal Key Exchange using Polycyclic Groups, In: Global Telecommunication Conference, 2006, GLOBECOM'06, IEEE, 1-5.

[19] *D. Kahrobaei, C. Koupparis, V. Schpilrain,* Public key exchange using matrices over group rings, Groups. Complexity. Cryptology, **5** (2013), 13-52.

[20] *A. Mahalanobis,* The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups, Israel J. Math., **165** (2008), 161-187.

[21] *V. Shpilrain, A. Ushakov,* A new key exchange protocol based on the decomposition problem, In: Algebraic Methods in Cryptography, Contemp. Math., **418**, 2006, Providence R.I., Amer. Math. Soc., 161-167.

[22] *L. Wang, L. Wang, Z. Cao, E. Okamoto, J. Shao,* New constructions of public-key encryption schemes from conjugacy search problems, In: Information security and cryptology, **6584**(2010), Lecture Notes Comp. Sc., Berlin, Springer, 1-17.

[23] *А.В. Грибов, П.А. Золотых, А.В. Михалев,* Построение алгебраической криптосистемы над квазигрупповым кольцом, Матем. вопр. криптографии, **1**, №4 (2010), 23-33.

[24] *В.Т. Марков, А.В Михалев, А.В. Грибов, П.А. Золотых, С.С. Скаженик,* Квазигруппы и кольца в кодировании и построении криптосхем, Прикл. дискр. мат. 2012. №4 (2012), 32-52.

[25] *С.К. Росошек,* Криптосистемы групповых колец, Вестник Томского государственного университета, №6 (2003), 57-62.

[26] *С.К. Росошек,* Криптосистемы в группах автоморфизмов групповых колец абелевых групп, Фунд. и прикл. мат., **13**, №3 (2007), 157-164.

[27] *B. Hurley, T. Hurley,* Group ring cryptography, arXiv: 1104.17.24v1 [math.GR] 9 Apr 2011, 1-20.

[28] *T. Hurley,* Cryptographic schemes, key exchange, public key, arXiv: 1305.4063v1 [cs.CR] May 2013, 1-19.

[29] *L. Babai, R. Beals, A. Seress,* Polynomial-time theory of matrix groups, STOC'09, May-June 2, 2009, Bethesda, Maryland, USA, 55-64.

[30] *A. Detinko, B. Eick, D. Flannery,* Computing with matrix groups, In: London Math. Soc. Lect. Notes Ser., **387** (2011), 256-270.

Адреса авторов:

РОМАНЬКОВ ВИТАЛИЙ АНАТОЛЬЕВИЧ,

Омский гос. ун-т им. Ф. М. Достоевского, пр. Мира, 55-А, г. Омск, 644077, РОССИЯ;

Омский гос. техн. ун-т, пр. Мира, 11, г. Омск, 644050, РОССИЯ;

e-mail: romankov48@mail.ru