Криптосистемы в группах автоморфизмов групповых колец абелевых групп

С. К. РОСОШЕК

Томский государственный университет
e-mail: rososhek@list.ru

УДК 512.552

Ключевые слова: абелева группа, кольцо, групповое кольцо, автоморфизм, криптосистема.

Аннотация

В работе вводится новый класс криптосистем с открытым ключом, являющихся обобщением криптосистемы Эль-Гамала на группы автоморфизмов групповых колец абелевых групп. Приведена схема базового варианта такой криптосистемы и рассмотрены некоторые виды атак на неё.

Abstract

S. K. Rososhek, Cryptosystems in automorphism groups of group rings of Abelian groups, Fundamentalnaya i prikladnaya matematika, vol. 13 (2007), no. 3, pp. 157–164.

We introduce a new class of public-key cryptosystems generalizing ElGamal cryptosystems to automorphism groups of group rings of abelian groups. A scheme of the basic variant of such a cryptosystem is presented and some types of attacks to it are considered.

Введение

Среди криптосистем с открытым ключом в настоящее время наиболее распространёнными являются криптосистемы RSA, Эль-Гамала и Рабина. Их криптостойкость основана на вычислительной сложности следующих теоретико-числовых задач:

- 1) разложение натуральных чисел на простые множители;
- 2) вычисление дискретного логарифма в циклической группе, являющейся мультипликативной группой поля вычетов по модулю большого простого числа;
- 3) извлечение квадратного корня в кольце вычетов по модулю составного числа, являющегося произведением двух различных больших простых чисел.

Алгебраические структуры, в которых решаются перечисленные задачи, — это кольца вычетов или конечные поля. Цель данной работы — предложить другие алгебраические структуры. В качестве «среды обитания» для криптосистем

Фундаментальная и прикладная математика, 2007, том 13, № 3, с. 157–164.

© 2007 Центр новых информационных технологий МГУ,
Издательский дом «Открытые системы»

нового типа предлагается использовать такую алгебраическую конструкцию, как групповое кольцо KG , где K — кольцо, G — абелева группа. Идея использования группового кольца в криптографии заключается в том, что при варьировании кольца и группы рост порядка группового кольца носит экспоненциальный характер. Тогда легальный пользователь сможет при конструировании криптографических преобразований использовать полиномиальные вычисления в кольце и группе, а нелегальный пользователь вынужден решать трудные вычислительные задачи в групповом кольце.

Напомним необходимые определения для группового кольца. Пусть G — мультипликативная группа и K — произвольное ассоциативное кольцо с единицей. Рассмотрим множество KG , состоящее из всех формальных сумм вида

$$\sum_{g \in G} \alpha_g g \quad (\alpha_g \in K),$$

в которых лишь конечное число коэффициентов отлично от нуля. В дальнейшем с учётом криптографических приложений будем считать, что кольцо K и группа G конечны, откуда следует конечность группового кольца KG .

На множестве KG заданы сложение и умножение следующим образом: если

$$x = \sum_{g \in G} \alpha_g g, \quad y = \sum_{g \in G} \beta_g g -$$

элементы KG , то

$$x + y = \sum_{g \in G} (\alpha_g + \beta_g)g, \quad xy = \sum_{g \in G} \left(\sum_{h \in G} \alpha_h \beta_{h^{-1}g} \right)g.$$

Тогда относительно этих операций множество KG является ассоциативным кольцом с единицей, которое называется групповым кольцом группы G над кольцом K . Пусть K — конечное кольцо мощности n , G — циклическая группа порядка m , и пусть $K = \{a_0, \dots, a_{n-1}\}$, $G = \{g_0 = e, \dots, g_{m-1} = g^{m-1}\}$, тогда произвольный элемент KG можно записать в виде

$$z = \sum_{h \in G} a_h h = \sum_{i=0}^{m-1} a_{g_i} g_i.$$

Стандартные рассуждения показывают, что если K есть конечное коммутативное кольцо, G есть циклическая группа порядка m , то кольцо KG изоморфно фактор-кольцу кольца многочленов от неизвестного x с коэффициентами из кольца K по идеалу, порождённому многочленом $x^m - 1$. Удобно представить это кольцо как кольцо многочленов степени не более $m - 1$ от неизвестного x с коэффициентами из кольца K с операциями сложения и умножения многочленов по модулю многочлена $x^m - 1$, т. е. кольцевые операции в групповом кольце KG получают эффективную реализацию в виде обычных операций сложения и умножения многочленов с последующим взятием остатка от деления результата этих операций на многочлен $x^m - 1$.

Легко проверяется следующее утверждение.

Пусть K — конечное коммутативное кольцо, G — циклическая группа порядка m . Если элемент $h \in KG$ имеет вид $h = \sum_{i=0}^{m-1} \alpha_i x^i$, где все α_i — нильпотентные элементы кольца K , то h — нильпотентный элемент кольца KG .

Пусть u — нильпотентный элемент кольца KG индекса k . Тогда $(1 - u) \times (1 + u + \dots + u^{k-1}) = 1 - u^k = 1$. Следовательно, $(1 - u)^{-1} = 1 + u + \dots + u^{k-1}$. Таким образом, если u — нильпотентный элемент индекса k кольца KG , то $\nu = 1 - u$ — обратимый элемент KG , причём $\nu^{-1} = \sum_{i=0}^{k-1} u^i$.

Теперь мы можем конструировать обратимые элементы кольца KG , для которых легко вычислить обратные элементы по следующей схеме.

1. Выбираем любые m нильпотентных элементов $\alpha_0, \dots, \alpha_{m-1}$ кольца K .
2. Составляем из них элемент $u = \sum_{i=0}^{m-1} \alpha_i x^i$ кольца KG , который будет нильпотентным элементом индекса k для некоторого натурального числа k .
3. Элемент $\nu = 1 - u$ является обратимым элементом кольца KG , причём $\nu^{-1} = \sum_{i=0}^{k-1} u^i$.

1. Базовая схема криптосистем на групповых кольцах

Все рассматриваемые кольца предполагаются ассоциативными кольцами с единицей, и автоморфизмы колец отображают единицу кольца в единицу. Кроме того, предполагается наличие полиномиальных алгоритмов как групповых и кольцевых операций, так и эффективных реализаций автоморфизмов колец и групп.

Рассмотрим следующую задачу. Пусть K — фиксированное кольцо (группа), L — некоторое множество автоморфизмов из группы $\text{Aut } K$ автоморфизмов кольца K , α — произвольный элемент из L . Предположим, что относительно автоморфизма α известно только его действие на некотором множестве элементов $x_1, x_2, \dots, x_s$ кольца K , т. е. известно некоторое множество пар (x_i, x_i^α) , $i = 1, 2, \dots, s$, $x_i \in K$, $x_i^\alpha \in K$ есть образ x_i при действии автоморфизма α . Требуется найти автоморфизм $\alpha' \in L$, такой что $x_i^{\alpha'} = x_i^\alpha$ для любого $i = 1, 2, \dots, s$. Обозначим эту задачу через $\Omega_s(L, K)$.

Заметим, что в общем случае, при отсутствии дополнительной информации относительно специфики кольца K и множества L , задача $\Omega_s(L, K)$ является вычислительно трудной, поскольку разрешима лишь путём полного перебора всех элементов множества L и для каждого элемента $\alpha' \in L$ проверки посредством полиномиального алгоритма условия $x_i^{\alpha'} = x_i^\alpha$ для любого $i = 1, 2, \dots, s$. При $s = 1$ задача $\Omega_s(L, K)$ внешне похожа на задачу вычисления дискретного

логарифма. Действительно, там требуется для заданного образующего α конечной циклической группы G и элемента $b = \alpha^x \in G$, где x — целое число, найти показатель степени x . На вычислительной сложности этой задачи держится стойкость криптосистемы Эль-Гамала.

Пусть K — конечное кольцо с некоммутативной группой автоморфизмов $\text{Aut } K$ (заметим, что кольцо K может быть при этом коммутативным), причём мощность $\text{Aut } K$ не меньше чем t_1 . Пусть G — конечная абелева группа с некоммутативной группой автоморфизмов $\text{Aut } G$, причём мощность $\text{Aut } G$ не меньше чем t_2 , где t_1, t_2 — наперёд заданные параметры безопасности.

Пусть A и B — участники сеанса связи по открытому каналу. Рассмотрим подробно все этапы конструирования криптосистемы на групповом кольце и её использования для защиты информации во время сеанса связи.

Этап 1 (генерация ключей). Участник A конструирует автоморфизм σ кольца K , порядок которого есть большое натуральное число $c \geq t_3$, а также автоморфизм ν группы G , порядок которого есть некоторое натуральное число $d \geq t_4$, где t_3, t_4 — наперёд заданные параметры безопасности. Пусть мощность централизатора $C(\sigma)$ автоморфизма σ в $\text{Aut } K$ не меньше чем t_5 , а мощность централизатора $C(\nu)$ автоморфизма ν в $\text{Aut } G$ не меньше чем t_6 , где t_5, t_6 — наперёд заданные параметры безопасности. Заметим, что циклическая подгруппа, порождённая автоморфизмом σ в группе $\text{Aut } K$, содержится в централизаторе $C(\sigma)$, а циклическая подгруппа, порождённая автоморфизмом ν в группе $\text{Aut } G$, содержится в централизаторе $C(\nu)$, причём эти включения будем предполагать строгими.

Участник A генерирует секретный ключ криптосистемы следующим образом:

- а) случайно выбирает автоморфизм $\tau \in C(\sigma)$, который не принадлежит циклической подгруппе, порождённой σ ;
- б) случайно выбирает автоморфизм $\omega \in C(\nu)$, который не принадлежит циклической подгруппе, порождённой ν ;
- в) задаёт автоморфизм φ группового кольца KG следующим образом: для любого $h \in KG$ вида $h = a_{g_1} + \dots + a_{g_n}$, где $G = \{g_1, \dots, g_n\}$, $a_{g_i} \in K$, $i = 1, \dots, n$, пусть

$$h^\varphi = (a_{g_1}^\tau g_1^\omega)_{\mu(1)} + \dots + (a_{g_n}^\tau g_n^\omega)_{\mu(n)},$$

где μ — случайная подстановка на множестве номеров слагаемых в записи элементов группового кольца, которая в силу коммутативности сложения не меняет сам элемент h^φ , а только форму его записи.

Тогда секретный ключ участника A есть автоморфизм φ .

Участник A вычисляет свой открытый ключ следующим образом:

- а) выбирает обратимый элемент $x \in KG$, для которого легко вычислить обратный элемент x^{-1} ;
- б) используя секретный ключ φ , вычисляет элемент $x^\varphi \in KG$.

Тогда открытый ключ участника A есть $(\sigma, \nu, x^{-1}, x^\varphi)$.

Этап 2 (алгоритм шифрования). После получения аутентичного открытого ключа участника A участник B для шифрования своего сообщения действует следующим образом:

- а) выбирает упорядоченную пару случайных чисел (i, j) ;
- б) задаёт сеансовый автоморфизм ψ кольца KG следующим образом: для любого $h = a_{g_1}g_1 + \dots + a_{g_n}g_n$, где $G = \{g_1, \dots, g_n\}$, $a_{g_1}, \dots, a_{g_n} \in K$, пусть

$$h = (a_{g_1}^{\sigma^i} g_1^{\nu^j})_{\xi(1)} + \dots + (a_{g_n}^{\sigma^i} g_n^{\nu^j})_{\xi(n)},$$

где ξ есть случайная подстановка на множестве номеров слагаемых;

- в) вычисляет $(x^{-1})^\psi$ и $(x^\varphi)^\psi$, используя открытый ключ участника A и автоморфизм ψ ;
- г) записывает исходный текст в виде $m \in KG$ и вычисляет $(m(x^\varphi)^\psi) \in KG$;
- д) в результате отправляет участнику A криптограмму $c = ((x^{-1})^\psi, m(x^\varphi)^\psi)$.

Заметим, что в каждом сеансе связи автоморфизм ψ нужно задавать заново.

Этап 3 (алгоритм дешифрования). Получив криптограмму c , участник A для дешифрования действует следующим образом:

- а) используя свой секретный ключ φ , вычисляет $((x^{-1})^\psi)^\varphi = z \in KG$;
- б) находит m , вычисляя $(m(x^\varphi)^\psi)z = m$.

Покажем корректность дешифрования. Сначала заметим, что по построению автоморфизмы φ и ψ коммутируют. Действительно, для любого $h \in KG$ вида $h = a_{g_1}g_1 + \dots + a_{g_n}g_n$ имеем

$$\begin{aligned} (h^\varphi)^\psi &= ((a_{g_1}^\tau g_1^\omega)_{\mu(1)} + \dots + (a_{g_n}^\tau g_n^\omega)_{\mu(n)})^\psi = \\ &= \left(((a_{g_1}^\tau)^{\sigma^i} \cdot (g_1^\omega)^{\nu^j}) \right)_{\xi(\mu(1))} + \dots + \left(((a_{g_n}^\tau)^{\sigma^i} \cdot (g_n^\omega)^{\nu^j}) \right)_{\xi(\mu(n))}, \\ (h^\psi)^\varphi &= \left(((a_{g_1}^{\sigma^i}) \cdot (g_1^{\nu^j}))_{\xi(1)} + \dots + ((a_{g_n}^{\sigma^i}) \cdot (g_n^{\nu^j}))_{\xi(n)} \right)^\varphi = \\ &= ((a_{g_1}^{\sigma^i})^\tau \cdot (g_1^{\nu^j})^\omega)_{\mu(\xi(1))} + \dots + ((a_{g_n}^{\sigma^i})^\tau \cdot (g_n^{\nu^j})^\omega)_{\mu(\xi(n))}. \end{aligned}$$

Так как τ коммутирует с σ и ω коммутирует с ν , то τ коммутирует с любой степенью σ , а ω коммутирует с любой степенью ν , следовательно, $(\sigma^i) \cdot \tau = \tau \cdot (\sigma^i)$ и $\omega \cdot (\nu^j) = (\nu^j) \cdot \omega$. Но тогда слагаемые у элементов $(h^\varphi)^\psi$ и $(h^\psi)^\varphi$ одни и те же, различие лишь в порядке записи слагаемых, и в силу коммутативности сложения в кольце сумма этих слагаемых одна и та же. Таким образом, $(h^\varphi)^\psi = (h^\psi)^\varphi$. Но тогда мы имеем

$$\begin{aligned} (m(x^\varphi)^\psi) \cdot z &= m \cdot (x^\varphi)^\psi \cdot ((x^{-1})^\psi)^\varphi = m \cdot x^{\varphi\psi} \cdot (x^{-1})^{\psi\varphi} = \\ &= m \cdot x^{\varphi\psi} \cdot (x^{-1})^{\varphi\psi} = m \cdot (x \cdot x^{-1})^{\varphi\psi} = m \cdot (1)^{\varphi\psi} = m \cdot 1 = m. \end{aligned}$$

Приведём теперь некоторые примеры колец, группы автоморфизмов которых удовлетворяют требуемым условиям.

Пример 1. Рассмотрим $K = M_2(\mathbb{Z}_5)$ — кольцо квадратных матриц второго порядка над полем вычетов по модулю 5. Учтём, что любой автоморфизм алгебры матриц внутренних. Пусть

$$A = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix},$$

тогда $A \in K^*$, где K^* — мультипликативная группа обратимых элементов кольца K , σ — внутренний автоморфизм кольца K , индуцированный матрицей A (т. е. для любого элемента B кольца K имеем $B^\sigma = A^{-1}BA$). Ясно, что степени автоморфизма σ индуцированы соответствующими степенями матрицы A . В нашем случае имеем, что циклическая подгруппа $\langle \sigma \rangle$, порождённая автоморфизмом σ , имеет порядок 5. Централизатор $C'(\sigma)$ автоморфизма σ в подгруппе $\text{Int } K$ внутренних автоморфизмов группы $\text{Aut } K$ всех автоморфизмов кольца K является подгруппой централизатора $C(\sigma)$ автоморфизма σ в группе $\text{Aut } K$. Поэтому в нашем случае можно ограничиться рассмотрением вместо $C(\sigma)$ подгруппы $C'(\sigma)$. Имеем

$$C'(\sigma) = \{\psi(A_{a,b}) \mid a \in \mathbb{Z}_5^*, b \in \mathbb{Z}_5\},$$

где $\psi(A_{a,b})$ — внутренний автоморфизм кольца K , индуцированный матрицей $A_{a,b}$ вида

$$A_{a,b} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix},$$

где $a \in \mathbb{Z}_5^*$, $b \in \mathbb{Z}_5$. Тогда порядок $C'(\sigma)$ равен 20, в то время как порядок $\langle \sigma \rangle$ равен 5.

Пример 2. Рассмотрим кольцо K из примера 1 (т. е. $K = M_2(\mathbb{Z}_5)$), и пусть группа G есть прямая сумма четырёх копий аддитивной группы $\mathbb{Z}_3^+$ поля вычетов по модулю 3. Тогда порядок кольца K равен $5^4 = 625$, порядок группы G равен $3^4 = 81$ и, следовательно, порядок группового кольца KG равен $625^{81} > (2^9)^{81} = 2^{729}$, т. е. даже при достаточно малых порядках кольца K и группы G порядок группового кольца KG очень велик. Заметим, что и автоморфизмов достаточно много: порядок $\text{Int } K$ равен порядку $\text{GL}_2(\mathbb{Z}_5)$, который равен $(5^2 - 1)(5^2 - 5) = 480$, порядок $\text{Aut } G$ равен порядку $\text{GL}_4(\mathbb{Z}_3)$, который равен $(3^4 - 1)(3^4 - 3)(3^4 - 3^2)(3^4 - 3^3) = 24\,261\,120$, а число только автоморфизмов KG , индуцированных автоморфизмами кольца K и группы G , равно $24\,261\,120 \cdot 480 = 11\,645\,337\,600$.

2. Некоторые атаки

Атака только с криптограммой

Криптоаналитик располагает открытым ключом $(\sigma, \nu, x^{-1}, x^\varphi)$ и криптограммой $c = ((x^{-1})^\psi, m \cdot (x^\varphi)^\psi)$. Предположим, что ему удалось по x^{-1} найти x , и тогда рассматривается пара (x, x^φ) . Имеем задачу $\Omega_1(L(\sigma, \nu), K)$ для пары

(x, x^φ) , где x — случайно выбранный обратимый элемент кольца KG , а φ — случайно выбранный элемент из множества $L(\sigma, \nu)$ автоморфизмов KG , причём $L(\sigma, \nu)$ состоит из автоморфизмов, индуцированных парами (σ', ν') , где $\sigma' \in (C(\sigma) \setminus \langle \sigma \rangle)$, $\nu' \in (C(\nu) \setminus \langle \nu \rangle)$. Но тогда единственная возможность найти секретный ключ φ — это случайный выбор элемента $\varphi' \in L(\sigma, \nu)$ и проверка условия $x^{\varphi'} = x^\varphi$. Поскольку при соответствующем выборе значений параметров безопасности $|L(\sigma, \nu)|$ может быть большим числом, в этом случае нахождение φ является вычислительно трудной задачей.

Атака на сеансовый автоморфизм ψ

Ещё одна атака состоит в попытке сначала найти автоморфизм ψ , а затем решить относительно m уравнение $m \cdot (x^\varphi)^\psi = h$, где $(x^\varphi)^\psi$ вычисляется из открытого ключа, если известен автоморфизм ψ , а элемент $h = m \cdot (x^\varphi)^\psi$ известен из криптограммы. Для нахождения ψ криптоаналитику нужно найти σ^i и ν^j , посредством которых был построен автоморфизм ψ . При нахождении σ^i можно учесть тот факт, что любой автоморфизм группы отображает единицу в единицу. Тогда из коэффициентов при единице группы G для x^{-1} и $(x^{-1})^\psi$ получаем пару элементов кольца K вида $(a_e, a_e^{\sigma^i})$, т. е. имеем задачу $\Omega_1(L, K)$, где $L = \langle \sigma \rangle$. При выборе в качестве σ автоморфизма большого порядка с большим централизатором $C(\sigma)$ нахождение автоморфизма $\sigma' \in \langle \sigma \rangle$, такого что $a_e^{\sigma'} = a_e^{\sigma^i}$, является вычислительно трудной задачей ввиду необходимости полного перебора всех степеней автоморфизма σ с последующей проверкой для каждой степени $\sigma' = \sigma^k$, $k = 1, 2, \dots$, условия $a_e^{\sigma^i} = a_e^{\sigma'}$.

Для нахождения автоморфизма ν^j группы G , в отличие от σ^i , не удаётся свести задачу Ω_1 с группового кольца KG к группе G , поскольку случайная перестановка слагаемых при действии автоморфизма ψ не позволяет получить ни одной пары вида $(g_k, g_k^{\nu^j})$. Поэтому криптоаналитику приходится случайным образом выбирать пару (σ', ν') , где $\sigma' \in \langle \sigma \rangle$, $\nu' \in \langle \nu \rangle$, по этой паре задавать автоморфизм ψ' кольца KG и проверять условие $(x^{-1})^{\psi'} = (x^{-1})^\psi$ в этом кольце. Но так как $|\langle \sigma \rangle|$ — большое число, то мощность множества всех выбираемых пар вида (σ', ν') тоже является большим числом, даже если $|\langle \nu \rangle|$ большим числом не является (уменьшение порядка группы G до некоторого допустимого числа позволит уменьшить битовую длину представления данных в виде элементов группового кольца). Следовательно, и в этом случае атака не представляет реальной угрозы.

Атака с известным исходным текстом

В этом случае криптоаналитик располагает исходным текстом m и криптограммой $c = ((x^{-1})^\psi, m \cdot (x^\varphi)^\psi)$. Тогда есть две пары вида (y, y^ψ) , а именно $(x^{-1}, (x^{-1})^\psi)$ и $(x^\varphi, (x^\varphi)^\psi)$, поскольку при известном m можно найти $(x^\varphi)^\psi$ из уравнения $m \cdot (x^\varphi)^\psi = h$. Получается задача $\Omega_2(L, KG)$ для нахождения

сеансового автоморфизма ψ , где L — множество автоморфизмов кольца KG , индуцированных парами вида (σ', ν') , $\sigma' \in \langle \sigma \rangle$, $\nu' \in \langle \nu \rangle$. Но при соответствующем выборе параметров безопасности эта задача, так же как и задача $\Omega_1(L, KG)$, является вычислительно трудной.

Атака с выбранным исходным текстом

В этом случае криптоаналитик может выбирать исходный текст и получать для него криптограмму. Тогда он может действовать следующим образом. Из равенства $(x^{-1})^\psi = (x^\psi)^{-1}$ он находит x^ψ , а затем и $y = x \cdot (x^\psi)$. Тогда выбор $m = x^\varphi$ даёт

$$x^\varphi \cdot ((x^\varphi)^\psi) = x^\varphi \cdot ((x^\psi)^\varphi) = (x \cdot (x^\psi))^\varphi.$$

Следовательно, кроме (x, x^φ) , получается ещё одна пара (y, y^φ) . Но задача $\Omega_2(L, KG)$ для нахождения автоморфизма φ , где L — множество автоморфизмов кольца KG , индуцированных парами вида (σ', ν') , $\sigma' \in (C(\sigma) \setminus \langle \sigma \rangle)$, $\nu' \in (C(\nu) \setminus \langle \nu \rangle)$, также является вычислительно трудной задачей при соответствующем выборе параметров безопасности.

Заметим, что конструирование конкретных криптосистем на групповых кольцах ставит следующие задачи:

- а) разработать быстрый алгоритм умножения в групповом кольце;
- б) разработать эффективные алгоритмы построения автоморфизмов колец с большими порядками и централизаторами, в том числе и регулярных автоморфизмов с указанными свойствами;
- в) найти такие классы колец K и групп G , для которых криптосистема на групповом кольце KG была бы сбалансирована относительно безопасности (увеличение параметров безопасности) и экономичности (уменьшение битовой длины представления данных).

Литература

- [1] Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. Н. Основы криптографии. — М.: Гелиос, 2001.
- [2] Каш Ф. Модули и кольца. — М.: Мир, 1981.
- [3] Ламбек И. Кольца и модули. — М.: Мир, 1971.
- [4] Фейс К. Алгебра: кольца, модули и категории. — М.: Мир, 1977. — Т. 1.
- [5] Фейс К. Алгебра: кольца, модули и категории. — М.: Мир, 1979. — Т. 2.

Статья поступила в редакцию в мае 2006 г.