Записки научных
семинаров ПОМИ
Том 293, 2002 г.

**Д. Ю. Григорьев**

# КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ И ТЕОРИЯ ИНВАРИАНТОВ

## 1. Введение.

Основная задача криптографии с открытым ключом состоит в том, чтобы построить криптосистему, имеющую следующие компоненты: открытый ключ $k_e$, секретный ключ $k_d$, известная всем кодирующая функция $f_e$ и декодирующая функция $f_d$. Если отправитель (назовем его Боря) хочет послать сообщение $m$ адресату (назовем его Аллой) по публичному (открытому) каналу связи, то Боря передает закодированное сообщение $u = f_e(m, k_e)$. Для декодирования Алла вычисляет исходное сообщение $m = f_d(u, k_d)$. Предполагается, что $k_d$ известен только Алле, в то время как $k_e$, $f_e$ известны всем, функция $f_d$ известна Алле (иногда она может быть известна всем). Другое важное требование криптосистемы состоит в том, чтобы постороннее лицо (назовем его Вова) не имел бы возможности найти $m$ по $u$ (не зная $k_d$).

Масса усилий была предпринята по построению криптосистем (некоторую литературу можно найти в [11, 13, 17]). Однако до настоящего момента не доказано надежности ни одной криптосистемы, и доказательство надежности остается одной из центральных открытых проблем. Все известные результаты о надежности касаются невозможности декодирования какой-то криптосистемы некоторыми фиксированными средствами, например, в рамках какой-то логической системы доказательств. Но что оказалось привлекательным в развитии криптографии с открытым ключом, – это то, что обнаружились ее связи с самыми различными разделами математики. Более того, во многих аспектах криптография с открытым ключом играет роль моста между математикой и информатикой. Наибольшее признание получили криптосистемы, основанные на идеях теории чисел, в частности РСА, протокол Диффи–Хеллмана или криптосистемы, использующие эллиптические кривые (описание этих криптосистем можно найти в книге [17], там же рассматриваются криптосистемы, привлекающие комбинаторно-алгебраические $NP$-трудные задачи).

В настоящей заметке вводятся криптосистемы, основанные на идеях теории инвариантов групп. Некоторые существующие криптосистемы используют группы (ниже мы приводим краткий обзор некоторых из них), но, на удивление, ранее не было известно приложений понятия инварианта представления группы, хотя оно хорошо подходит целям криптографии. Все же, применение инвариантов к криптографии наталкивается на ряд трудностей, поэтому цель настоящей заметки – ввести инварианты представлений групп в криптографию с открытым ключом, описать возможные криптосистемы, а также обсудить проблемы их надежности.

Итак, изложим общую идею использования групп (и их инвариантов) в криптографии с открытым ключом. Обозначим через $E$ множество закодированных сообщений и пусть группа $G : E \to E$ действует на $E$. Примерами $E$ могут служить множество слов в некотором алфавите, а также векторное пространство. Кроме того, выделено подмножество $M \subset E$ исходных (незакодированных) сообщений, являющееся трансверсальным по отношению к орбитам действия $G$, т.е. всякие два элемента из $M$ принадлежат различным орбитам.

Действие $G$ применяется для вероятностного кодирования [13, 14], которое более эффективно в плане "сокрытия информации", нежели детерминированное. Итак, для кодирования сообщения $m \in M$ Боря выбирает случайно элемент $g$ из группы $G$ и передает $gm \in E$ по открытому каналу. Задача Аллы состоит в декодировании $gm$, чтобы узнать $m$, используя ее секретный ключ. С другой стороны, Вова не должен уметь находить $m$ по $gm$.

Обычно, последние два свойства достигаются за счет подходящего выбора $G$. В широко распространенной криптосистеме квадратичных вычетов [13, 14] выбирают число $n = pq$ для больших простых чисел $p$, $q$ (которые представляют собой секретный ключ Аллы). В качестве группы $G$ рассматривается $(Z_n^*)^2$, множество $E = \{g \in Z_n^* : J_n(g) = 1\}$, где $J_n$ обозначает символ Якоби (по модулю $n$). Кроме того, выбирается квадратичный невычет $a \in E - G$, положим множество $M = \{1, a\}$. Открытый ключ состоит из $n$, $a$. Итак, чтобы закодировать 1, Боря случайно выбирает $g \in Z_n^*$, кодом 1 является $g^2 \in G \subset E$ (который Боря передает по каналу), кодом $a$ является $g^2a \in E$, тем самым $E = G \cup Ga$. Задача Аллы по декодированию состоит в том, чтобы проверить, является ли переданное Борей закодированное сообщение $b \in E$ квадратом. Алла может это проверить, зная $p$, $q$ и используя символы Лежандра–Якоби $J_p$, $J_q$. С другой стороны, имеется общее мнение, что Вова не может распознать, является ли $b$ квадратом, не зная $p$, $q$.

Описанная криптосистема квадратичных вычетов обобщается на класс криптосистем, называемых гомоморфными. Именно, пусть $f : E \to H$ – гомоморфизм групп, который является секретным ключом Аллы. Более того, имеется точная последовательность гомоморфизмов групп

$$B \xrightarrow{s} E \xrightarrow{f} H \to \{1\}$$

и множество $M \subset E$, трансверсальное (нормальной) подгруппе $G = \ker(f) \subset E$, иными словами, $f$ задает биективное соответствие между $M$ и $H$. При этом открытым ключом является пятерка $B$, $s$, $E$, $H$, $M$. Предполагается, что $s$ вычислимо с полиномиальной сложностью.

Описанная схема согласуется с приведенными выше понятиями и обозначениями: $G$ действует (посредством умножения слева) на $E$, и множество исходных (незакодированных) сообщений $M$ трансверсально к этому действию, причем $G$ задается здесь неявно как образ $G = s(B)$. Чтобы закодировать сообщение $m \in M$, Боря случайно выбирает $b \in B$ и передает по каналу сообщение $s(b)m \in E$. Алла декодирует $s(b)m$, применяя $f$, опираясь на то, что $f(s(b)m) = f(m)$. Вове декодировать затруднительно, не зная $f$. В описанной выше криптосистеме квадратичных вычетом имеем $H = \mathbb{Z}_2$, $B = E$, $s(b) = b^2$, и $f$ является эпиморфизмом квадратичного вычета.

В [9, 33] был поставлен вопрос: для каких групп $H$ могут быть построены гомоморфные криптосистемы (более общо, можно ли рассматривать гомоморфизмы колец вместо групп)? Для некоторых абелевых групп $H$ гомоморфные криптосистемы были построены в [4, 23–25, 27]. Для некоторых диэдральных групп $H$ гомоморфные криптосистемы предложены в [28]. В [15] гомоморфные криптосистемы описаны для произвольной разрешимой группы $H$. Имеется много работ о криптосистемах над эллиптическими кривыми (см., например, [17, 18]).

Общей чертой всех упомянутых выше гомоморфных криптосистем является то, что декодирование в них опирается на знание секретной пары чисел $p$, $q$. В настоящей заметке предлагается другой подход к декодированию (и кодированию), основанный на инвариантах $W : E \to F$, где $E$ – векторное пространство над полем $F$. Иными словами, $W$ постоянно на орбитах действия группы $G$. Алла может декодировать сообщение $gm$ путем вычисления $w(gm) = w(m)$ в предположении, что $W$ принимает различные значения на исходных (незакодированных) сообщениях из $M$.

Теория инвариантов (см., например, [7, 30, 31]) развита, главным образом, в ситуации, когда $G : E \to F$ – линейное представление, т.е. $E$ – $n$-мерное векторное пространство, $G \subset \mathrm{GL}(E)$ – подгруппа матриц над полем $F$, инвариант $w \in F[X_1, \ldots, X_n]$ – многочлен от $n$ переменных над $F$. Но, наверное, было бы полезно также изучить и другие действия групп и их инварианты.

Принимая во внимание, что инварианты $w$ известны явно и могут быть вычислены лишь для небольшого числа бесконечных серий линейных представлений $G \subset \mathrm{GL}(E)$ ([31]), мы предлагаем "запрятать" $G$, рассматривая ее сопряжение $a^{-1}Ga \subset \mathrm{GL}(E)$ для матрицы $a \in \mathrm{GL}(E)$, которая является секретным ключом Аллы. Тогда инвариант $e \to w(ae)$ сопряжения $a^{-1}Ga$ позволяет Алле декодировать сообщение $a^{-1}gam$, где $a^{-1}ga$ – элемент группы $a^{-1}Ga$, случайно выбранный Борей для кодирования сообщения $m$. Обычно группа $a^{-1}Ga$ (составляющая открытый ключ вместе с $E$ и $M \subset E$) задается семейством матриц из $\mathrm{GL}(E)$, являющихся ее образующими. Задание группы ее образующими – это достаточно сжатый способ. В частности, каждая известная простая группа имеет две образующих, кроме того, всякая конечная группа $G$ задается не более, чем $\log_2 |G|$ образующими. При вычислениях в группе $G$, заданной семейством образующих, не обязательно предполагать, что $G$ конечна (это так, в частности, когда поле $F$ конечно), поскольку для кодирования Боря случайно выбирает некоторое произведение образующих группы $a^{-1}Ga$. Вследствие этого, так же можно рассматривать семейство образующих, порождающих какую-то подгруппу группы $a^{-1}Ga$.

В последующих параграфах мы опишем класс криптосистем с открытым ключом, основанных на инвариантах групп, а также обсудим проблему их надежности, но сначала мы закончим введение обзором еще двух семейств криптографических конструкций, которые используют группы.

Другой задачей криптографии, наряду с построением криптосистем с открытым ключом, является протокол соглашения о ключе, (см., например, [11, 13, 17]). Теперь Алла и Боря хотят договориться об общем ключе, общаясь по открытому каналу. Распространенный подход к этой задаче состоит в том, что Алла и Боря независимо выбирают секретные коммутирующие операторы $f_A$, $f_B : E \to E$, соответственно, и кроме того, (публично) некоторое $e \in E$. Далее, Алла передает по каналу $f_A(e)$, Боря передает $f_B(e)$, и их общим ключом является $f_A(f_B(e)) = f_B(f_A(e))$. В первом из протоколов соглашения Диффи–Хеллмана (см. [13, 17]) в качестве коммутирующих операторов выбирались $f_A(e) = e^a$, $f_B(e) = e^b(\bmod p)$ для целых $a$, $b$. Таким образом, задача Вовы по декодированию протокола Диффи–Хеллмана связана с вычислением дискретного логарифма. Общее мнение состоит в том, что это трудно, сложность дискретного логарифма изучалась в [6, 22].

Указанный общий подход к задаче построения протокола соглашения о ключе рассматривался в следующей постановке (см. [3, 16, 26]). Пусть $E$ – группа с парой взаимно (поэлементно) коммутирующих подгрупп $E_A$, $E_B \subset E$. Тогда в качестве $f_A$ Алла выбирает сопряжение $e \to a^{-1}ea$ для случайного $a \in E_A$, Боря соответственно, $f_B(e) = b^{-1}eb$ для $b \in E_B$. В [16] роль $E$ играет группа кос, и трудность декодирования протокола соглашения связана с трудностью задачи сопряженности в группе кос.

В [2, 8, 10, 32] предлагается несколько криптосистем с открытым ключом, опирающихся на трудность проблемы равенства слов в подходящих группах.

Последнее семейство криптосистем с открытым ключом, которое мы упомянем, основывается на решетках (представляющих собой дискретные абелевы подгруппы пространства $\mathbb{R}^n$). Первая из таких конструкций предложена в [1]. Пусть $L \subset \mathbb{R}^n$ – $n$-мерная решетка, обладающая тем свойством, что она содержит (сопряженную) $(n-1)$-мерную подрешетку $L'$, чья линейная оболочка равна гиперплоскости $H$, так что выполнено следующее свойство. Гиперплоскости $H_i$, параллельные $H$, такие, что $\bigcup\limits_i H_i \supset L$, сильно отделены: именно, расстояние между любой парой соседних гиперплоскостей $H_i$, $H_{i+1}$ больше некоторого достаточно большого $d$. Иными словами, существует базис решетки $L$, состоящий из $n-1$ достаточно короткого вектора (их множество обозначим через $C$) из $L'$ и достаточно длинного вектора $c$, имеющего большую проекцию, ортогональную $H$.

Тогда криптосистема с открытым ключом из [1] рассматривает какой-либо случайный базис $C_1$ решетки $L$ в качестве открытого ключа, а базис $C \cup \{c\}$ – в качестве секретного ключа Аллы. Исходный бит 0 Боря кодирует посредством случайного вектора из $L$, а бит 1 – посредством случайного вектора из $\mathbb{R}^n$.

Для декодирования вектора $u$ Алла вычисляет величину

$$\ell = \big(u, c - P_H(c)\big) / \big\| c - P_H(c) \big\|^2,$$

где $P_H$ обозначает ортогональную проекцию на гиперплоскость $H$. Если число $\ell$ целое (это означает, что $u$ принадлежит одной из гиперплоскостей $H_i$), тогда Алла может объявить, что исходный бит равен 0 (в противном случае, 1). Фактически, таким способом Алла распознает элементы из $\bigcup\limits_i H_i$, а не из требуемой решетки $L$, поэтому ошибка случается, когда $u \in \bigcup\limits_i H_i - L$. Чтобы исправить эту ошибку, Боря слегка шевелит $u$, при этом каждая точка из $L$ окружается шариком подходящего радиуса $r$ так, чтобы покрыть $\bigcup\limits_i H_i$, но, с другой стороны, не покрыть все пространство $\mathbb{R}^n$. Более того, шевеления соседних гиперплоскостей $H_i$, $H_{i+1}$ должны быть сильно отделены, и как раз по этой причине было наложено требование на длинный вектор $c$. Наконец, Алла декодирует точки $u$ на расстоянии $r$ от объединения $\bigcup\limits_i H_i$ как 0, в противном случае – как 1. Все же, ошибка может произойти, когда $u$ лежит на расстоянии не более $r$ от объединения $\bigcup\limits_i H_i$, но тогда более вероятно, что в этом случае Боря закодировал 0 (а не 1). Таким образом, предполагаемая трудность декодирования Вовой описанной криптосистемы с открытым ключом основывается на трудности нахождения длинного вектора в решетке, заданной базисом $C_1$ (или, эквивалентно, нахождения короткого вектора в двойственной решетке), в предположении, что длинный вектор единственен в некотором подходящем строгом смысле.

Другая криптосистема с открытым ключом, использующая шевеления, была построена в [12]. Здесь исходное сообщение – точка решетки $L \subset \mathbb{R}^n$, и ее кодирование получается путем ее малого шевеления в $\mathbb{R}^n$. Тогда задача декодирования (Вовой) криптосистемы приводит к нахождению для данной вещественной точки ближайшего к ней вектора решетки $L$. Известно, что эта задача $NP$ – трудна, так же как и приближение к ней с точностью до постоянного множителя. Чтобы сделать возможным декодирование, Алла сперва выбирает случайно базис $c_1, \dots, c_n$ решетки $L$ специального вида (именно такой, что величина

$$\Big(\prod_i \|c_i\|\Big) / \Big|\det(c_i)\Big|$$

не слишком велика, базис с таким свойством называется “почти ортогональным”), который играет роль секретного ключа. Затем Алла меняет (с помощью случайного унимодулярного преобразования) базис $c_1, \dots, c_n$, полученный базис служит в качестве открытого ключа. Главное наблюдение состоит в том, что знание “почти ортогонального” базиса позволяет Алле найти для данного вектора ближайший вектор в $L$ в предположении, что шевеление было достаточно малым.

Итак, в обоих упомянутых методах, использующих решетки [1, 12], исходное сообщение “запрятано” посредством малого шевеления, это отличается от нашего подхода “запрятывать” сообщение путем сдвига на некоторый элемент данной группы.

## 2. Построение криптосистем с открытым ключом, основанных на инвариантах групп.

Пусть $G \subset \mathrm{GL}_n(F)$ – представление группы $G$, причем можно считать без ограничения общности, что поле $F$ алгебраически замкнуто, однако в вычислениях коэффициенты матриц из $G$ могут принадлежать некоторому подполю поля $F$. Например, коэффициенты могут лежать в конечном поле.

Допустим, что известен некоторый (непостоянный) инвариант $w$ ([7, 30]) представления $G$, т.е. многочлен $w \in F[X_1, \dots, X_n]$ такой, что для всякого элемента $g \in G$ и всякого вектора $v \in F^n$ имеем $w(gv) = w(v)$. Кроме того, фиксируем пару ненулевых различных векторов $v_0$, $v_1 \in F^n$.

Обычно предполагается, что можно порождать элементы из $G$. Для построения (вероятностной) криптосистемы с открытым ключом Алла случайно выбирает матрицу $a \in \mathrm{GL}(F)$ с тем свойством, что $w(av_0) \neq w(av_1)$ (очевидно, что почти всякая матрица $a$ обладает этим свойством).

**Открытый ключ:** $v_0$, $v_1$ и семейство элементов вида $h_i = a^{-1}g_i a \in \mathrm{GL}(F)$, где $g_i$ – случайно порожденные элементы группы $G$;

**Секретный ключ:** $a$;

**Кодирование:** бит 0 (или, соответственно бит 1) Боря кодирует вектором $u = h_{i_1} \cdots h_{i_\ell} v_0 \in F^n$ (соответственно, $u = h_{i_1} \cdots h_{i_\ell} v_1 \in F^n$ для случайно выбранных $i_1, \dots, i_\ell$.

**Декодирование:** по данному вектору $u \in F^n$ Алла вычисляет величину $w(au)$ и проверяет, равна ли она $w(av_0)$ (в этом случае исходное сообщение равно $v_0$, поскольку $w(av_0) = w(ah_{i_1} \cdots h_{i_\ell} v_0) = w(au)$) или она равна $w(av_1)$ (в этом случае исходное сообщение равно $v_1$).

**3. О надежности.**

Для декодирования описанной криптосистемы с открытым ключом Вова может попытаться построить инвариант $w'$ подгруппы $H$ сопряжения $a^{-1}Ga$ (здесь $H$ обозначает группу, порожденную образующими $h_i$). Можно считать, что группа $G \subset \mathrm{GL}(F)$ (размера экспоненциального от $n$ или даже бесконечного) известна, так же как и инвариант $w$. Вова может пытаться искать инвариант $w'$ в виде $w'(v) = w(bv)$ для неизвестной матрицы $b \in \mathrm{GL}_n(F)$. Пусть $d$ обозначает степень инварианта $w$ (как обычно в теории инвариантов, можно было бы ограничиться рассмотрением однородных инвариантов $w$). Подставляя $w'$ в заданные образующие $a^{-1}g_i a$ группы $H$, иными словами, $w(bv) = w(b(a^{-1}g_i a)v)$ для каждого $i$ (ясно, что подойдет любая такая матрица $b$), и приравнивая коэффициенты при всех мономах от $n$ координат вектора $v$, Вова получает систему полиномиальных уравнений степени $d$ от коэффициентов матрицы $b$. Следовательно, эта система содержит $\binom{n+d-1}{d}$ уравнений (для каждого $i$) степени $d$ от $n^2$ неизвестных, являющихся коэффициентами матрицы $b$.

Действуя другим способом, Вова может искать инвариант $w'$, рассматривая его как многочлен степени $d$ с $\binom{n+d-1}{d}$ неизвестными коэффициентами, удовлетворяющими уравнениям $w'(h_i v) = w'(v)$ для каждого $i$ и для всякого вектора $v \in F^n$. Это дает систему линейных уравнений от неизвестных коэффициентов (считая $v$ параметрическим вектором).

В любом случае, сложность каждого из двух описанных способов декодирования зависит от $\binom{n+d-1}{d}$, поэтому для обеспечения надежности следует брать представление группы $G$, у которого отсутствуют инварианты степени меньше $\mathrm{const}\cdot n$. С другой стороны, инвариант $w$ должен быть вычислим со сложностью, полиномиальной от $n$ (ниже мы приведем несколько таких примеров).

Задача нахождения инварианта кажется трудной и в общей ситуации мало что известно, помимо применения усредняющего оператора $|G|^{-1}\sum_{g\in G} g$ (в предположении, что группа $G$ конечна), ср. [31].

Рассмотрим еще два подхода к декодированию криптосистем, описанных в предыдущем параграфе.

При первом подходе Вова пытается найти матрицу $a$ (или любую другую матрицу $b \in \mathrm{GL}_n(F)$ такую, что $bHb^{-1} \subset G$). Ясно, что можно предполагать без ограничения общности, что группа $H$ сопряжена с самой группой $G$ (а не с какой-то ее подгруппой), выбирая в качестве $g_i$ образующие группы $G$ (случайно выбранное достаточно большое семейство $g_i$ порождает $G$ с большой вероятностью). Проблема проверки существования матрицы $b$ (и ее нахождения, если она существует) такой, что $bHb^{-1} = G$, называется *проблемой сопряженности* матричных групп. К этой проблеме можно свести проблемы сопряженности групп перестановок, как сообщил автору Ю. Лакс [21]. В свою очередь, в [20] сформулирована гипотеза о трудности проблемы сопряженности групп перестановок. Кроме того, к проблеме сопряженности групп перестановок сводится проблема изоморфизма графов [20]. Итак, первый подход к декодированию криптосистем с открытым ключом, описанных в предыдущем параграфе, приводит Вову, в частности, к проблеме изоморфизма графов.

При втором подходе Вова пытается найти матрицу $h \in H$ такую, что $hu = v_0$ (или, соответственно, $hu = v_1$). Эта проблема называется *проблемой о переносе векторов*, и в [20] сформулирована гипотеза о ее трудности в частном случае, когда $H$ – группа перестановок. Аналогично, к ней сводится проблема изоморфизма графов.

Упомянем, что частный случай проблемы о переносе векторов, когда (множество закодированных сообщений) $F^4$ рассматривается как пространство $2\times 2$ матриц, и группа $H = \mathrm{SL}_2(\mathbb{Z})\times\mathrm{SL}_2(\mathbb{Z})$ действует на $F^4$ по правилу $v \to h_1 v h_2$, где $(h_1, h_2)\in H$, является $NP$-трудным для сложности в среднем [5]. В этой связи заметим, что доказательство трудности декодирования криптосистемы с открытым ключом относительно более сильного понятия сложности в среднем было бы более интересно, чем относительно обычной сложности в худшем случае (ср. [19]).

Итак, оба подхода к декодированию описанных выше криптосистем с открытым ключом связаны с проблемой изоморфизма графов. Но, конечно, трудность доказательства сведе́ния проблемы изоморфизма графов к декодированию криптосистем лежит, в частности, в необходимости построения группы $G$ и ее представления, таких, что проблема изоморфизма графов могла бы быть сведена к проблемам сопряженности и переноса векторов для $G$. Было бы интересно выяснить, сводится ли действительно проблема изоморфизма графов к декодированию описанных выше криптосистем.

Упомянем также, что выглядящая внешне похожим образом задача эквивалентности (сопряженности) представлений групповых алгебр $F[G]$, $F[H]$ (в отличие от сопряженности самих групп), другими словами, нахождение матрицы $a \in \mathrm{GL}_n(F)$ такой, что $a^{-1}F[H]a = F[G]$, может быть эффективно решена над алгебраически замкнутым полем $F$ [29], основываясь на структурных теоремах Шура и Веддерберна.

Очевидное замечание состоит в том, что для обеспечения большей надежности криптосистем с открытым ключом было бы разумно часто менять секретные и (тем самым) открытые ключи $a$ и $a^{-1}g_i a$.

Приведем теперь несколько простых примеров криптосистем с открытым ключом, использующих инварианты классических групп [7, 30].

**Пример 1.** ([30]) В качестве группы $G$ возьмем подгруппу группы $\mathrm{GL}_n$, порожденную симметрической группой $S_n$ перестановок стандартного базиса $e_i$, $1 \leqslant i \leqslant n$, а также всеми матрицами $t$ такими, что $te_i = c_i e_i$, где $c_i^m = 1$, $1 \leqslant i \leqslant n$, $(c_1, \dots, c_n)^\ell = 1$ для некоторых $\ell | m$. Тогда в качестве инварианта $w$ можно взять степенную сумму $x^m + \cdots x_n^m$. Мы сознательно рассматриваем расширение симметрической группы, чтобы избежать наличие инвариантов малых степеней (см. дискуссию в начале этого параграфа).

**Пример 2.** Определим представление специальной линейной группы $G = \mathrm{SL}_n(F)$ на симметрическом квадрате $S^2F^n$, другими словами, на симметрических матрицах (или квадратичных формах) формулой $v \to mvm^\intercal$, где $m \in G$ и $\intercal$ обозначает транспонирование. Тогда в качестве $w$ можно взять $\det(v)$.

**Пример 3.** Теперь группа $G = \mathrm{GL}_n(F)$ действует на прямой сумме $F^{2n^2} = F \oplus \ldots \oplus F^n$ $2n$ копий пространства $F^n$ по формуле $m(\rho_1, \ldots, \rho_{2n}) = (m\rho_1, \ldots, m\rho_{2n})$. Рассмотрим два разбиения $I_1 \cup J_1 = I_2 \cup J_2 = \{1, \ldots, 2n\}$ на $n$-элементные подмножества $|I_1| = |J_1| = |I_2| = |J_2| = n$. Через $\det_{I_1}$ обозначим определитель $n \times n$ минора, состоящего из $n$ векторов $p_i$ для $i \in I_1$. Тогда в качестве $w$ можно взять рациональный инвариант

$$\frac{\det_{I_1} \det_{J_1}}{\det_{I_2} \det_{J_2}}.$$

В описанной в предыдущем параграфе криптосистеме с открытым ключом мы рассматривали полиномиальные инварианты $w$, но почти дословно можно было бы рассмотреть и рациональные инварианты $w \in F(X_1, \ldots, X_n)$, с той лишь оговоркой, разумеется, что Алла должна выбирать векторы $v_0$, $v_1 \in F^{2n^2}$ и матрицу $a \in \mathrm{GL}_{2n^2}(F)$ таким образом, чтобы значения $w(av_0)$, $w(av_1)$ были определены.

Можно еще построить подобные примеры, использующие прямое, тензорное, симметрическое, внешнее произведения представлений групп.

Состояние дел в настоящее время в криптографии не позволяет доказывать надежность криптосистем с открытым ключом, это обычно вопрос веры в трудность некоторой подходящей вычислительной задачи, а также опыта (поэтому имеется много статей по криптографии с открытым ключом, включая настоящую, не содержащих теорем). Напротив, можно ожидать "разочаровывающего" декодирования каких-то частных криптосистем. Это не исключено ни для какой из описанных, в примерах выше, криптосистем с открытым ключом (избегая при этом решения проблемы изоморфизма графов, см. замечание выше). С другой стороны, декодирование могло бы привести, возможно, к интересным алгоритмам в теории представлений групп. Итак, можно смотреть на приведенные примеры (а также на конструкцию из предыдущего параграфа в целом) лишь как на предложение исследовать криптосистемы с открытым ключом, основанные на теории инвариантов.

**Благодарности.** Автор хотел бы поблагодарить Институт Высших Исследований (Франция), во время пребывания в котором эта работа была задумана, а также Л. Левина и Ю. Лакса за интересные обсуждения.

## Литература


1. M. Ajtai, C. Dwork, *A public-key cryptosystem with worst-case/average case equivalence.* — Proceedings of the 29th Annual ACM Symposium on Theory of Computing (1997), pp. 284–293.
2. I. Anshel, M. Anshel, *From the Post-Markov theorem through decision problems to public-key cryptography.* — Amer. Math. Monthly, **100** (1993), 835–844.
3. I. Anshel, M. Anshel, D. Goldfeld, *An algebraic method for public-key cryptography.* — Math. Res. Lett., **6** (1999), 287–291.
4. J. Benaloh, *Dense probabilistic encryption.* — First Ann. Workshop on Selected Areas in Cryptology (1994), pp. 120–128.
5. A. Blass, Y. Gurevich, *Matrix transformation is complete for the average case.* — SIAM J. Comput., **24** (1995), 3–29.
6. D. Coppersmith, I. Shparlinski, *On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping.* — J. Cryptology, **13** (2000), 339–360.
7. J. Dieudonné, J. Carrell, *Invariant theory, Old and New.* Academic Press (1971). Перевод: Ж. Дьедонне, Д. Кэррел, Теория инвариантов, Старое и Новое “Мир” (1975).
8. Do Long Van, A. Jeyanthi, R. Siromony, K. Subramanian, *Public key cryptosystems based on word problems.* — ICOMIDC Symp. Math. of Computations, Ho Chi Minh City, April (1988).
9. J. Feigenbaum, M. Merritt, *Open questions, talk abstracts, and summary of discussions.* — DIMACS series in discrete mathematics and theoretical computer science, **2** (1991), 1–45.
10. M. Garzon, Y. Zalcstein, *The complexity of Grigorchuk groups with application to cryptography.* — Theoret. Comput. Sci., **88** (1991), 83–98.
11. O. Goldreich, *Modern cryptography, probabilistic proofs and pseudorandomness.* Springer (1998).
12. O. Goldreich, S. Goldwasser, S. Halevi, *Public-key cryptosystems from lattice reduction problems.* — Lecture Notes in Comput. Sci., **1294** (1997), 112–131.
13. S. Goldwasser, M. Bellare, http://www-cse.ucsd.edu/users/mihir/papers/gb.html (2001), Lecture Notes on Cryptography.
14. S. Goldwasser, S. Micali, *Probabilistic encryption.* — J. Comput. System Sci., **28** (1984), 270–299.
15. Д. Ю. Григорьев, И. Н. Пономаренко, *О неабелевых гомоморфных криптосистемах с открытым ключом.* — Зап. научн. семин ПОМИ, **293** (2002), 39–58.

16. K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park,, *New public-key cryptosystem using braid groups.* — Lecture Notes in Comput. Sci., **1880** (2000), 166–183.
17. N. Koblitz, *Algebraic aspects of cryptography.* — Algorithms and Computation in Mathematics, **3**, Springer (1998).
18. K. Koyama, U. Maurer, T. Okamoto, S. Vanstone, *New public-key schemes based on elliptic curves over the ring* $\mathbb{Z}_n$. — Lecture Notes in Comput. Sci., **576** (1991), 252–266.
19. L. Levin, *Average case complete problems.* — SIAM J. Comput., **15** (1986), 285–286.
20. E. Luks, *Permutation groups and polynomial-time computations.* — DIMACS Series in Discr. Math. and Theor. Comput. Sci., **11** (1993), 139–175.
21. E. Luks, *Personal communication.* — (2002).
22. U. Maurer, S. Wolf, *Lower bounds on generic algorithms in groups.* — Lecture Notes in Comput. Sci., **1403** (1998), 72–84.
23. D. Naccache, J. Stern, *A new public-key cryptosystem.* — Lecture Notes in Comput. Sci., **1233** (1997), 27–36.
24. D. Naccache, J. Stern, *A new public-key cryptosystem based on higher residues.* — Proc. 5th ACM Conference on Computer and Communication Security 1998, pp. 59–66.
25. T. Okamoto, S. Uchiyama, *A New Public-Key Cryptosystem as Secure as Factoring.* — Lecture Notes in Comput. Sci., **1403** (1998), 308–317.
26. S.-H. Paeng, D. Kwon, K.-C. Ha, J. H. Kim, *Improved public key cryptosystem using finite non-abelian groups.* — Preprint NSRI, Korea.
27. P. Paillier, *Public-Key Cryptosystem Based on Composite Degree Residuosity Classes.* — Lecture Notes in Comput. Sci., **1592** (1999), 223–238.
28. D. Rappe, *Algebraisch homomorphe Kryptosysteme.* — Diplomarbeit, Universität Dortmund (2000).
29. L. Ronyai, *Computations in associative algebras.* — Groups and Computation, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., **11**, AMS (1993), 221–243.
30. T. Springer, *Invariant theory.* — Lecture Notes in Mathematics, **585**, Springer (1977). Перевод: Т. Спрингер, Теория инвариантов, "Мир", (1981).
31. B. Sturmfels, *Algorithms in invariant theory.* — Texts and Monographs in Symbolic Computation, Springer (1993).
32. N. Wagner, M. Magyarik, *A public-key cryptosystem based on the word-problem.* — Lect. Notes in Comput. Sci., **196** (1985), 19–36.
33. A. Yao, *How to generate and exchange secrets.* — Proceedings of the 27th annual IEEE Symposium on Foundations of Computer Sciences (1986), pp. 162–167.

Grigoriev D. Public-key cryptography and invariant theory.

Public-key cryptosystems are suggested based on invariants of groups. We give also an overview of known cryptosystems which involve groups.

IRMAR, Université de Rennes
Beaulieu, 35042, Rennes, France
http://maths.univ-rennes1.fr/~dima

Поступило 15 сентября 2002 г.