Записки научных
семинаров ПОМИ
Том 293, 2002 г.

Д. Ю. Григорьев, И. Н. Пономаренко

О НЕАБЕЛЕВЫХ ГОМОМОРФНЫХ КРИПТОСИСТЕМАХ С ОТКРЫТЫМ КЛЮЧОМ

1. Введение

Ниже группы задаются способом, зависящим от конкретной задачи. В частности, конструкция в параграфе 2 основана на группах $\mathbb{Z}_n^+$ и $\mathbb{Z}_n^*$, заданных натуральным числом n, в то время как в общей конструкции в параграфе 3 требуется лишь, чтобы можно было порождать элементы группы, и кроме того, чтобы можно было эффективно выполнять умножение и вычислять обратный элемент. В последнем случае группы можно задавать образующими и соотношениями, и даже порождающими алгоритмами (см. напр. [14]).

Известно довольно много криптосистем с открытым ключом, использующих группы (см., напр., [2, 11, 12, 16, 21, 22]), но только некоторые из них удовлетворяют свойству гомоморфности в смысле следующего определения (см. также [7, 23, 24]).

Определение 1.1. *Пусть H – конечная (нееденичная) группа, G – конечно порождённая группа и $f : G \to H$ – эпиморфизм. Предположим, что дано множество R представителей различных правых классов смежности группы G по (нормальной) подгруппе* $\ker(f)$, *и, кроме того, множество A слов в некотором алфавите и отображение $P : A \to G$ такое, что* $\operatorname{im}(P) = \ker(f)$. *Тройка $\mathcal{S} = (R, A, P)$ называется гомоморфной криптосистемой над H относительно f, если выполнены следующие условия:*

(H1) *имеются алгоритмы для случайного порождения элементов множеств A, G, H, а также для вычисления обратного элемента и произведения двух элементов в группах G и H, вероятностная сложность которых полиномиальна от (битового) размера N задания групп G, H и множества A;*

(H2) $|R| = |H|$ *и для всякого элемента $g \in R$ его образ $f(g)$ можно вычислить за полиномиальное от N время, также как для всякого элемента $h \in H$ его единственный прообраз*

$g \in R$, такой что $f(g) = h$;

(H3) *P – секретно-обратимое отображение.*

Замечание 1.2. Множество R задано явно списком своих элементов (из группы G). Следовательно, условие (H2) влечёт, что не ограничивая общности можно считать, что группа H задана своей таблицей умножения.

Условие (H3) означает (см., напр., [8]), что значения отображения P можно вычислять с полиномиальной от N вероятностной сложностью (в среднем), в то время как нахождение обратного отображения P^{-1} – трудная вычислительная задача, которая может быть решена с помощью дополнительной секретной информации (в настоящей работе под вероятностным алгоритмом будем понимать алгоритм типа Лас-Вегас [15]). В гомоморфной криптосистеме $\mathcal{S}$ элементы группы H (публично) кодируются вероятностным образом элементами группы G, все необходимые вычисления выполняются в группе G и результат декодируется в группу H. Более точно:

Открытый ключ: G, H, R, A, P, $f\big|_R$.

Секретный ключ: нахождение P^{-1}.

Кодирование: для каждой буквы $h \in H$ исходного сообщения найдём (единственный) элемент $r \in R$, для которого $f(r) = h$ (основываясь на условии (H2)), и случайный элемент $a \in A$; кодом h является элемент $P(a)r \in G$ (элемент a, также как и произведение $P(a)r$, вычисляется с помощью алгоритмов из условия (H1)).

Декодирование: для данного $g \in G$ найдём (единственный) элемент $r \in R$, а также элемент $a \in A$ (используя условие (H3)), для которых $rg^{-1} = P(a)$; тогда исходное сообщение, кодом которого является g, равно $f(g) = f(r)$ (элемент $f(r)$ вычисляется на основе условия (H2)).

Нетрудно видеть, что процедура кодирования может быть реализована эффективно с помощью открытых ключей. Однако, декодирование является секретным в следующем смысле. Для нахождения элемента r нужно, по существу, решить задачу определения принадлежности к подгруппе $\ker(f)$ группы G. Мы делаем предположение, что решение для любого элемента $g' \in \ker(f)$

этой задачи должно иметь “доказательство”, которое фактически является элементом $a \in P^{-1}(g')$. С другой стороны, возможность вычислять P^{-1} наделяет нас способностью эффективно выполнять алгоритм декодирования. Можно интерпретировать P как систему доказательств для $\ker(f)$ в смысле [3]. Более того, в случае, когда A – некоторая группа и P – гомоморфизм групп, мы имеем следующую точную последовательность гомоморфизмов групп:

$$A \xrightarrow{P} G \xrightarrow{f} H \to \{1\}$$

(напомним, что точность последовательности означает, что образ каждого гомоморфизма совпадает с ядром следующего).

В настоящей статье группа H, являющаяся алфавитом исходных сообщений, всегда конечна (и достаточно маленькая) и задаётся своей таблицей умножения, в то время как группа G закодированных сообщений может быть бесконечна, но всегда конечно порождена. Тем не менее, бесконечность группы G не является препятствием для кодирования (и декодирования), поскольку всякий элемент из H кодируется конечным словом из образующих группы G. В частности, в [6] для (бесконечной, в общем случае неабелевой) группы H, заданной m образующими и соотношениями, рассматривается естественный эпиморфизм $f : F_m \to H$ из свободной группы F_m с m образующими. Таким образом, для любого элемента из H можно строить его прообразы (т.е. коды) путём вставки в слово (являющееся уже построенным прообразом относительно f^{-1}) из F_m произвольного соотношения, определяющего H. Иначе говоря, декодирование f сводится к проблеме слов в группе H. Основное отличие от нашего подхода состоит в том, что мы рассматриваем свободные произведения групп теоретико-числовой природы, как-то Z_n^* (в отличие от групп, заданных образующими и соотношениями). Это даёт возможность представить некоторое обоснование трудности декодирования.

Определение 1.3. *Обозначим через $\mathcal{G}_{crypt}$ класс всех конечных групп H, для которых существует гомоморфная криптосистема над H.*

В контексте нашего определения гомоморфной криптосистемы основная цель настоящей статьи – доказать, что класс $\mathcal{G}_{crypt}$ содержит все неединичные разрешимые группы (см. теорему 3.6).

Сначала (в параграфе 2) мы показываем, что этот класс содержит все неединичные циклические группы.

Насколько авторам известно, все до сих пор построенные гомоморфные криптосистемы являются более или менее модификациями следующей. Пусть n – произведение двух различных простых чисел (битового) размера $O(\log n)$. Положим $G = \{g \in \mathbb{Z}_n^* : \mathbf{J}_n(g) = 1\}$, где $\mathbf{J}_n$ – символ Якоби по модулю n и $H = \mathbb{Z}_2^+$. Тогда для данного фиксированного неквадрата $g_0 \in G$ тройка (R, A, P), где

$$R = \{1, g_0\}, \quad A = \mathbb{Z}_n^*, \quad P(g) : g \mapsto g^2,$$

представляет собой гомоморфную криптосистему над H относительно естественного эпиморфизма $f : G \to H$ с ядром $\ker(f) = \{g^2 : g \in \mathbb{Z}_n^*\}$ (см. [9, 8]). Назовём её *криптосистемой квадратичных вычетов*. Можно доказать (см. [9, 8]), что в этом случае нахождение обратного P^{-1} не легче, чем разложение n на простые множители; с другой стороны, если известно разложение n, то P^{-1} можно вычислить за полиномиальное время.

Существенным предположением (и недостатком) криптосистемы квадратичных вычетов, равно как и других криптосистем с открытым ключом, упомянутых ниже, является то, что их секретность (в смысле трудности декодирования посторонним лицом) основывается на фиксированной заранее системе доказательств P. В самом деле, не исключено, что постороннее лицо могло бы проверить принадлежность элемента группы G ядру $\ker(f)$ без использования P; в частности, в случае криптосистемы квадратичных вычетов это означало бы возможность проверки того, что элемент $g \in G$ является квадратом без предъявления квадратного корня элемента g. Однако, общее мнение состоит в том, что проверка того, что элемент является квадратом (или иной степенью) – трудная задача.

Упомянем, что криптосистема с открытым ключом из [19] над группой $H = \mathbb{Z}_n^+$ (при том же предположении на n, что и в криптосистеме квадратичных вычетов) относительно эпиморфизма $f : G \to H$, где $G = \mathbb{Z}_{n^2}^*$ и $\ker(f) = \{g^n : g \in G\}$, в которой $A = G$ и $P(g) = g^n$, не удовлетворяет условию (H3) определения 1.1 (поскольку $|G| \leqslant |H|^2$, можно обратить P за время, полиномиальное от $|H|$; по-видимому, трудно обратить P за время, полиномиальное от $\log n$). По той же причине криптосистема из [17] над группой $H = \mathbb{Z}_p^+$ относительно гомоморфизма $f : G \to H$, где

$G = \mathbb{Z}^*_{p^2q}$ и $\ker(f) = \{g^{pq} : g \in G\}$ (здесь p, q – различные простые числа одинакового битового размера), также не удовлетворяет определению 1.1 (помимо этого, в этой криптосистеме кодируется только часть группы H). Наконец, упомянем, что криптосистемы с открытым ключом над некоторыми диэдральными группами исследовались в [21].

Следует отметить, что альтернативное определение гомоморфного (в действительности, изоморфного) кодирования E (и декодирования $D = E^{-1}$) было предложено в [12]. В отличие от определения 1.1 кодирование $E : G \to G$ производится в том же множестве G (являющимся эллиптической кривой над кольцом $\mathbb{Z}_n$), рассматриваемом как множество исходных (незакодированных) сообщений. Если число n составное, то множество G не является группой, но на нем задана частично определённая бинарная операция, которая превращает G в группу, когда число n простое. Декодирование этой криптосистемы – трудная задача, близкая к разложению n на множители. В этом аспекте криптосистема из [12] сходна с криптосистемой РСА (см., напр., [8]), если последнюю интерпретировать как гомоморфизм (на самом деле, изоморфизм) $E : Z^*_n \to Z^*_n$, секретность которого связана с трудностью вычисления порядка группы Z^*_n.

Завершим введение упоминанием некоторых криптосистем с открытым ключом, также использующих группы, но не являющихся гомоморфными в смысле определения 1.1. Хорошо известна криптосистема, основанная на протоколе согласования ключей Диффи–Хеллмана (см. напр. [8]). Она использует циклические группы и связана с проблемой дискретного логарифма [14]; сложность этой криптосистемы изучалась в [4]. Некоторые обобщения этой криптосистемы на неабелевы группы (в частности, на группы матриц над некоторыми кольцами) были предложены в работе [18]; их секретность опирается на трудность вычисления аналога дискретного логарифма в группах внутренних автоморфизмов. Некоторые модификации систем Диффи–Хеллмана над группами кос описаны в [11]; здесь секретность предложенных функций связана с трудностью проблем распознавания сопряжённости и нахождения корней в группах кос. Упомянем также криптосистему из [16], использующую мономорфизм $\mathbb{Z}^+_m \to \mathbb{Z}^*_n$, с помощью которого элемент x кодируется элементом $g^x \pmod n$, где n, g – открытый ключ; декодирование в этой системе связано с проблемой дискретного логарифма и возможность его эффективной реализации в этом случае является следствием специального выбора параметров n и m (см. также [2]).

2. Гомоморфные криптосистемы над циклическими группами

В этом параграфе мы строим в явном виде гомоморфную криптосистему над циклической группой простого порядка m, декодирование которой основано на вычислении корней степени m в группе $\mathbb{Z}_n^*$ для подходящего натурального числа n. Эта криптосистема может рассматриваться как обобщение криптосистемы квадратичных вычетов над $\mathbb{Z}_2$. Ниже в этом параграфе мы обозначаем через $|n|$ битовый размер натурального числа n.

Для чисел m, $N \in \mathbb{N}$ положим $\mathcal{T}_N = \{(p,q) : p, q \text{ простые}, |p| = |q| = N, \ p < q\}$ и

$$D_{N,m} = \{n \in \mathbb{N} : n = pq, \ (p,q) \in \mathcal{T}_N, \ m|p-1, \ \mathrm{GCD}\,(m, q-1) = 1\}.$$

Из теоремы Дирихле о простых числах в арифметических прогрессиях [5] вытекает, что для данного нечётного простого m множество $D_{N,m}$ не пусто для достаточно больших N.

Пусть $n \in D_{N,m}$ для некоторого натурального числа N и нечётного простого m. Тогда группа $G = \mathbb{Z}_n^*$ обладает (нормальной) подгруппой $G_0 = \{g^m : \ g \in G\}$, фактор-группа по которой изоморфна группе $H = \mathbb{Z}_m^+$. Обозначим через f соответствующий эпиморфизм из G на H. Отображение

$$P : G \to G, \quad g \mapsto g^m \tag{1}$$

является полиномиально вычислимым гомоморфизмом, образ которого совпадает с $\ker(f)$. Далее, всякий элемент множества

$$R_{m,n} = \{R \subset G : \ |f(R)| = |R| = m\}$$

есть система различных представителей классов смежности группы G по подгруппе G_0. Отметим, что, зная разложение $n = pq$, можно найти элемент $R \in R_{m,n}$ за вероятностное среднее время $|n|^{O(1)}$. Действительно, поскольку m – простое число, достаточно найти случайный элемент $s_p \in \mathbb{Z}_p^*$, такой что $s_p^{(p-1)/m} \neq 1$, а также элемент $s_q \in \mathbb{Z}_q^*$, затем, используя китайскую теорему об остатках, взять единственный элемент $s \in \mathbb{Z}_n^*$, для которого $s =$

$s_p \pmod p$, $s = s_q \pmod q$, и положить $R = \{s^i t_i^m : i = 0, \dots, m-1\}$ для произвольных $t_i \in \mathbb{Z}_n^*$.

Мы утверждаем, что тройка $\mathcal{S}_{N,m,n} = (R, A, P)$ с произвольно выбранным $R \in R_{m,n}$, $A = G$ и отображением P, определённым в соответствии с (1), является гомоморфной криптосистемой над группой H относительно эпиморфизма f, если выполнено следующее предположение:

Предположение (∗). Для нечётного простого m и $R \in R_{m,n}$ проблема $\mathcal{P}(m, R)$ нахождения в $\mathbb{Z}_n^*$ корня степени m, где $n \in D_{N,m}$, когда известен некоторый элемент $R \in R_{m,n}$, не проще, чем подобная проблема $\mathcal{P}(m)$, но без знания R.

Будем задавать группу G числом n, а группу H множеством её элементов. Тогда нетрудно проверить, что для тройки $S_{N,m,n}$ выполнены условия (H1) и (H2) определения 1.1 (образ определённого выше элемента $s^i t_i^m$ относительно гомоморфизма f равен $i \in \mathbb{Z}_m^+$). Условие же (H3) вытекает из следующей леммы.

Лемма 2.1. *Пусть $N \in \mathbb{N}$, m – нечётное простое число и $n \in D_{N,m}$. Тогда*

(1) *если известны простые числа p и q, такие что $n = pq$, то для каждого элемента $g \in \mathbb{Z}_n^*$ можно проверить, является ли он m-ой степенью, и если является, то найти корень m-ой степени из числа g за полиномиальное от N вероятностное время;*

(2) *проблема разложения числа n на множители сводима за полиномиальное вероятностное время к проблеме нахождения корня m-ой степени в $\mathbb{Z}_n^*$.*

Доказательство. В ходе доказательства будем использовать каноническое разложение $\mathbb{Z}_n^* = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Для проверки утверждения (1) воспользуемся алгоритмом Рабина [20], вычисляющим вероятностно за полиномиальное время корни многочлена над простым конечным полем. Именно, для данных простых p, q и $g \in \mathbb{Z}_n^*$ действуем следующим образом:

Шаг 1. Найдём элементы $g_p \in \mathbb{Z}_p^*$ и $g_q \in \mathbb{Z}_q^*$, такие что $g = g_p \times g_q$, т.е. $g_p = g \pmod p$, $g_q = g \pmod q$.

Шаг 2. Применяя алгоритм Рабина, найдём какие-либо корни $h_p \in \mathbb{Z}_p^*$ и $h_q \in \mathbb{Z}_q^*$ многочленов $x^m - g_p$ и $x^m - g_q$, соответственно.

Шаг 3. Выходом алгоритма объявляем $h = h_p \times h_q$.

Заметим, что описанный алгоритм успешно завершает работу тогда и только тогда, когда g является m-ой степенью; в противном случае алгоритм останавливается на шаге 2. Равенство $h^m = h_p^m \times h_q^m = g_p \times g_q = g$ завершает доказательство утверждения (1).

Для доказательства утверждения (2) предположим, что имеется алгоритм Q_n, вычисляющий с вероятностной полиномиальной сложностью какой-нибудь корень $Q_n(g)$ степени m из данного $g \in \mathbb{Z}_n^*$. Следующая процедура, использующая известное наблюдение из [8], показывает, как алгоритм Q_n помогает найти простые числа p и q.

Шаг 1. Выберем случайно $x \in \mathbb{Z}_n^*$.

Шаг 2. Положим $y = Q_n(x^m)$. Если $x = y$, возвращаемся к шагу 1.

Шаг 3. Выходом алгоритма объявляем $q = \mathrm{GCD}\,(x - y, n)$ и $p = n/q$.

Пусть $x = x_p \times x_q$ и $y = y_p \times y_q$, где $x_p, y_p \in \mathbb{Z}_p^*$ и $x_q, y_q \in \mathbb{Z}_q^*$. Из шага 2 вытекает, что $x_q^m = y_q^m$. С другой стороны, $\mathrm{GCD}\,(q-1, m) = 1$, поскольку $n \in D_{N,m}$. Поэтому $x_q = y_q \pmod q$ и, следовательно,

$$x = x_q = y_q = y \pmod q.$$

Таким образом, число $x - y \neq 0 \pmod n$ делится на q. Для завершения доказательства заметим, что поскольку $m = O(1)$, цикл, состоящий из шагов 1, 2, с большой вероятностью завершается после полиномиального числа итераций. □

К сожалению, мы не знаем, как применять лемму без использования предположения $(*)$, поскольку в нашем случае криптосистема с открытым ключом $\mathcal{S}_{N,m,n}$ включает множество $R \in R_{m,n}$. Тем не менее, в силу леммы мы имеем следующее утверждение.

Теорема 2.2. *В предположении $(*)$ тройка $\mathcal{S}_{N,m,n}$ для нечётного простого m является гомоморфной криптосистемой над $\mathbb{Z}_m^+$; в частности, класс $\mathcal{G}_{crypt}$ содержит все циклические группы простого порядка.* □

В завершение параграфа отметим, что криптосистему $\mathcal{S}_{N,m,n}$ можно было бы несколько модифицировать, чтобы избежать применения алгоритма Рабина для нахождения корней многочленов над конечными полями. В принципе для декодирования достаточно проверить, принадлежит ли данный элемент $g \in G$ группе G_0. Это, однако, легко сделать, принимая во внимание, что $g \in G_0$ тогда и только тогда, когда $g_p^{(p-1)/m} = 1 \,(\operatorname{mod} p)$, где g_p – компонента элемента g в сомножителе $\mathbb{Z}_p^*$ прямого произведения $G = \mathbb{Z}_p^* \times \mathbb{Z}_q^*$.

3. Построение гомоморфных криптосистем с помощью свободных произведений

3.1. На протяжении всего параграфа множество всех слов в алфавите X обозначается через $W(X)$. Длина слова $w \in W(X)$ обозначается через $|w|$.

Пусть $G_1, \dots, G_m$ – семейство из $m \geqslant 1$ попарно непересекающихся конечных групп. Для $i = 1, \dots, m$ положим

$$X_i = G_i \setminus \{1_{G_i}\}, \quad \mathcal{R}_i = \{xyz \in W(X_i) : \; x, y, z \in X_i, \; z^{-1} = xy\}.$$

Тогда $G_i = \langle X_i; \mathcal{R}_i \rangle$, т.е. G_i – группа, заданная множеством образующих X_i, и множеством соотношений $\mathcal{R}_i$. Положим $X_G = \cup_{i=1}^m X_i$ и $\mathcal{R}_G = \cup_{i=1}^m \mathcal{R}_i$. Группа

$$G = G_1 * \dots * G_m = \langle X_G; \; \mathcal{R}_G \rangle$$

называется *свободным произведением* групп $G_1, \dots, G_m$ (см. [13]). Из определения следует, что каждый элемент группы G может быть представлен единственным (каноническим) словом из множества $W_G = W(X_G)$, в котором никакие две соседние буквы не принадлежат какому-то одному множеству X_i. Таким образом, в дальнейшем мы будем, не оговаривая особо, отождествлять элемент из G с соответствующим каноническим словом; иначе говоря $G = \{\overline{w} \in W_G : \; w \in W_G\}$, где $\overline{w}$ обозначает каноническое слово, соответствующее слову w. В частности, $\overline{g} = g$ для всех $g \in G$. Отождествляя ниже группы $G_1, \dots, G_m$ и G с соответствующими подмножествами множества W_G, мы, не умаляя общности, будем предполагать, что единицы всех этих групп совпадают с пустым словом.

Пусть K_i – группа и $f_i : G_i \to K_i$ – эпиморфизм, $i = 1, \dots, m$. Предполагая группы $K_1, \dots, K_m$ попарно непересекающимися, положим $K = K_1 * \dots * K_m$ и $W_K = W(X_K)$, где $X_K = \cup_{i=1}^m (K_i \setminus \{1_{K_i}\})$. Тогда естественная сюръекция $W_G \to W_K$, переводящая элементы из X_G в элементы из X_K с помощью эпиморфизмов f_i,

$i = 1, \dots, m$, индуцирует эпиморфизм

$$f^* : G \to K, \quad f^*|_{X_i} = f_i, \quad i = 1, \dots, m. \tag{2}$$

Более того, поскольку условия $f^*|_{X_i} = f_i$ определяют образы образующих элементов G, эпиморфизм f^* является единственным эпиморфизмом из G на K, удовлетворяющим этим условиям.

3.2. Изучим ядро эпиморфизма f^*. С этой целью предположим, что группа K_i – циклическая простого порядка и (R_i, A_i, P_i) – гомоморфная криптосистема над группой K_i относительно эпиморфизма $f_i : G_i \to K_i$, построенная в параграфе 2, $i = 1, \dots, m$. Пусть $w_1, w_2 \in W_G$ и $x \in G_i$ для некоторого i. *Элементарным преобразованием* слова $w_1 x w_2 \in W_G$ назовём замену элемента x словом $x_1 P_j(a_j) x_2$, где $x_1, x_2 \in G_i$, причём $x = \overline{x_1 x_2}$ и $a_j \in A_j$ для некоторого j:

$$w_1 x w_2 \quad \to \quad w_1(x_1 P_j(a_j) x_2) w_2. \tag{3}$$

Обозначим через W_0 множество всех слов из W_G, которые могут быть получены из пустого слова последовательностью элементарных преобразований и положим $G_0 = \{\overline{w} : \ w \in W_0\}$.

Лемма 3.1. *Во введённых выше обозначениях имеем:* $\ker(f^*) = G_0$.

Доказательство. Пусть сначала $w = w_1 x w_2$, где $w_1, w_2 \in W_G$ и $x \in G_i$ для некоторого i. Предположим, что слово $w' \in W_G$ получается из слова w элементарным преобразованием (3). Тогда слова $\overline{w}, \overline{w'}$ принадлежат или не принадлежат группе $\ker(f^*)$ одновременно. Действительно,

$$f^*(\overline{w'}) = f^*(\overline{w}_1 \overline{x}_1 \overline{P_j(a_j)} \overline{x}_2 \overline{w}_2) = f^*(\overline{w}_1) f^*(\overline{x}_1) f^*(\overline{x}_2) f^*(\overline{w}_2) =$$
$$f^*(\overline{w}_1) f^*(\overline{x}) f^*(\overline{w}_2) = f^*(\overline{w_1 x w_2}) = f^*(\overline{w}). \tag{4}$$

Отсюда индукцией по числу элементарных преобразований, использованных для получения элемента из G_0, получается включение $\ker(f^*) \supseteq G_0$.

Обратно, пусть $w' \in \ker(f^*)$. Индукцией по $|w'|$ покажем, что $w' \in G_0$. База индукции $|w'| = 0$ очевидна. Предположим, что $|w'| > 0$. Тогда $w' = w_1 x w_2$ для подходящих слов w_1, $w_2 \in W_G$ и $x \in \ker(f_i)$ для некоторого i. Действительно, предположив противное, получаем в силу каноничности слова w', что $\overline{w'} = w'$, и потому $|w'| = |f^*(w')|$, откуда $|f^*(w')| > 0$, что противоречит тому, что $w' \in \ker(f^*)$. Таким образом, слово w' получается из слова $w = w_1 w_2 \in W_G$ элементарным преобразованием вида (3). Поскольку $w' \in \ker(f^*)$, из 3.1 вытекает, что $\overline{w} \in \ker(f^*)$. С другой стороны, $|\overline{w}| \leqslant |w| < |w'|$. Отсюда по индукционному предположению заключаем, что $\overline{w} \in G_0$. Следовательно, $w' \in G_0$. Так что $\ker(f^*) \subseteq G_0$. □

Пусть $g \in \ker(f^*)$. Тогда из леммы 3.1 следует, что g может быть получено из пустого слова последовательностью элементарных преобразований вида (3). Более того, из доказательства леммы вытекает существование такой последовательности из не более, чем $|g|$ элементарных преобразований. Всякую такую последовательность назовём *доказательством* для g (более точно, доказательством принадлежности $g \in \ker(f^*)$, ср. условие (H3) определения 1.1). Нетрудно видеть, что любое элементарное преобразование вида (3) однозначно определяется следующими данными: позицией буквы $x \in G_i$, словом $x_1 x_2 x^{-1} \in \mathcal{R}_j$ и элементом $a_j \in A_j$. Поэтому всякое доказательство принадлежности g к $\ker(f^*)$ может быть представлено словом в алфавите $\mathbb{N} \times \mathcal{R}_G \times (\cup_i A_i)$. Можно проверить, что длина этого слова ограничена сверху полиномом от $|g|$.

Обозначим через A^* множество всех доказательств для элементов из $\ker(f^*)$. Следует отметить, что A^* включает только "короткие" (т.е. содержащие не более $|g|$ элементарных преобразований) доказательства для $g \in \ker(f^*)$, но не содержит "доказательств" для всех слов из W_0. Нетрудно показать, что случайный элемент из A^* данной длины может быть порождён за время полиномиальное от этой длины. Действительно, ввиду (3), достаточно случайно выбрать позиции в текущем слове и, кроме того, элементы из A_i для $i = 1, \ldots, m$. Для этого можно воспользоваться порождающим алгоритмом из условия (H1) определения 1.1 для гомоморфных криптосистем (R_i, A_i, P_i) над K_i.

Лемма 3.2. *Образ отображения $P^* : A^* \to G$, определённого формулой $P^*(a) = g$, где a – доказательство принадлежности g к $\ker(f^*)$, равен $\ker(f^*)$. Кроме того, справедливы следующие утверждения:*

(i1) *для данного $a \in A^*$ элемент $P^*(a)$ можно вычислить за время полиномиальное от $|a|$,* (i2) *если для каждого* $i = 1, \dots, m$ *имеется оракул* Q_i, *который для любого элемента* $g_i \in \ker(f_i)$ *строит некоторый элемент* $a_i \in P_i^{-1}(g_i)$, *то для данного* $g \in \ker(f^*)$ *можно найти его доказательство* $a \in A^*$, *используя не более* $|g|^2$ *обращений к оракулам* Q_i *для построения элементов из* $P_i^{-1}(g_i)$, $g_i \in \ker(f_i)$, $i = 1, \dots, m$,

(i3) *для каждого* $i = 1, \dots, m$ *и* $g \in \ker(f_i)$ *задача нахождения какого-нибудь элемента из* $P_i^{-1}(g)$ *сводится за полиномиальное время к задаче нахождения какого-нибудь элемента из* $(P^*)^{-1}(g)$.

Доказательство. Равенство $\operatorname{im}(P^*) = \ker(f^*)$ следует из леммы 3.1. Утверждение (i1) вытекает из того, что всякое элементарное преобразование вида (3) слова $g \in W_G$ сводится к вычислению $P_j(a_j)$, которое осуществимо за полиномиальное от $|a_j| \leqslant |a|$ время. Для доказательства утверждения (i2) можно применить следующую процедуру, выясняющую принадлежность слова $w \in W_G$ к множеству W_0.

Шаг 1. Используя умножение в группах G_i, $i = 1, \dots, m$, найдём каноническое слово $\overline{w}$ слова w.

Шаг 2. Обращаясь к оракулам Q_i, $i = 1, \dots, m$, удалим каждую букву $x \in \ker(f_i)$ из (текущего) слова $\overline{w}$. Если при этом была удалена хотя бы одна буква, то возвращаемся к шагу 1.

Шаг 3. Если полученное в результате слово пусто, то $w \in W_0$.

В действительности, описанная процедура представляет собой алгоритмическую версию леммы 3.1. Для построения доказательства принадлежности произвольного слова $g \in W_G$ к $\ker(f^*)$ достаточно применить эту процедуру к g и собрать вместе все промежуточные результаты шагов 1 и 2. Поскольку их количество не превосходит $|g|$, и на шаге 2 число обращений к оракулам Q_i также не превосходит $|g|$, утверждение (i2) доказано.

Для доказательства утверждения (i3) зафиксируем $i \in \{1, \dots, m\}$ и $g \in G_i$. Поскольку, очевидно, что $g \in \ker(f_i)$ тогда и только тогда, когда $g \in \ker(f^*)$, легко проверить принадлежность g к $\ker(f_i)$ с помощью алгоритма для задачи нахождения $(P^*)^{-1}$. Более того, если $g \in \ker(f_i)$, этот алгоритм находит доказательство из A^* для элемента g. Зная вид этого доказательства, выделим множество T, состоящее из всех элеметов $a_j \in A_i$, встречающихся в элементарных преобразованиях вида (3), входящих в это доказательство. Тогда $g = \prod_{a_j \in T} P(a_j)$. Принимая во внимание, что множество A_i является абелевой группой, а отображение $P_i : A_i \to G_i$ – гомоморфизмом, мы заключаем, что элемент $a = \prod_{a_j \in T} a_j$ является доказательством для g. Лемма доказана.$\square$

Опишем теперь некоторое специальное множество различных представителей правых классов смежности группы G по подгруппе $\ker(f^*)$. Положим $W_R = W(\cup_i R_i)$. Тогда $W_R \subset W_G$ и множество

$$R^* = G \cap W_R \tag{5}$$

является множеством различных представителей правых классов смежности группы G по подгруппе $\ker(f^*)$. Действительно, R^* состоит из всех слов множества W_R, которые являются каноническими словами из W_G. Следовательно, любые два элемента из R^* принадлежат различным правым классам смежности G по $\ker(f^*)$. Таким образом, сформулированное утверждение вытекает из того, что сужение отображения f^* на R^* является биекцией из R^* на K, совпадающей с f_i на R_i, $i = 1, \ldots, m$.

3.3. Опишем ещё один специальный гомоморфизм свободного произведения групп. С этой целью напомним некоторые факты о полупрямых произведениях групп (см., напр., [10]). Пусть K_1, K_2 – группы и $\varphi : K_2 \to \mathrm{Aut}(K_1)$ – гомоморфизм. Тогда множество $K_1 \times K_2$ образует группу, умножение в которой задаётся формулой

$$(k_1, k_2)(l_1, l_2) = (k_1(l_1)^{\varphi(k_2^{-1})}, k_2 l_2), \quad k_1, l_1 \in K_1, \quad k_2, l_2 \in K_2.$$

Эта группа называется *полупрямым произведением* групп K_1 и K_2 (относительно гомоморфизма φ); обозначим ее через $H = \Pi(K_1, K_2)$. Она содержит подгруппу K_i' (изоморфную K_i), состоящую из всех пар с $(3-i)$-ой координатой равной $1_{K_{3-i}}$, $i = 1, 2$. Кроме того, K_1' – нормальная подгруппа группы H, причём $K_1' \cap K_2' = \{1_H\}$ и $H = K_1'K_2'$. В общем случае, группа H с двумя подгруппами K_1', K_2', обладающими указанными свойствами, изоморфна полупрямому произведению этих групп относительно гомоморфизма φ, индуцированного действием K_2' на K_1' посредством сопряжения. Ниже мы будем отождествлять K_i с K_i', $i = 1, 2$. Помимо этого, мы расширяем определение полупрямого произведения на произвольное число групп, полагая по индукции для $m \geqslant 3$

$$\Pi(K_1, K_2, \dots, K_m) = \Pi(K_1, \Pi(K_2, \dots, K_m))$$

относительно подходящих гомоморфизмов вида φ. Таким образом, $\Pi(K_i, \dots, K_m) = \Pi(K_i, K^{(i)})$, где $K^{(i)} = \Pi(K_{i+1}, \dots, K_m)$ при $i = 1, \dots, m-1$ (здесь для $i = m-1$ мы полагаем $\Pi(K_m) = K_m$). Ниже группы $\Pi(K_1, K_2, \dots, K_m)$ будут предполагаться "маленькими" и задаваться своими таблицами умножений. Тем самым, их подгруппы $K_1, \dots, K_m$ также малы, и для каждого i гомоморфизм $\varphi_i : K^{(i)} \to \mathrm{Aut}\,(K_i)$ может быть задан указанием для каждого $k \in K^{(i)}$ перестановки $\varphi_i(k)$ множества K_i.

Лемма 3.3. *Пусть $H = \Pi(K_1, \dots, K_m)$ и $K = K_1 * \dots * K_m$, где $K_1, \dots, K_m$ попарно непересекающиеся конечные группы. Тогда существует эпиморфизм $Q : K \to H$, причём для каждого $k \in K$ элемент $Q(k)$ может быть найден за полиномиальное время от $|k|$ и $|H|$.*

Доказательство. В силу сделанных предположений группа H и множество

$$\mathcal{R}_H = \{x^{-1}yxy' \in W_K : \; x \in K^{(i)}, \\ y \in K_i, \; y' = (x^{-1}yx)^{-1}, \; i = 1, \dots, m-1\}$$

будут рассматриваться как подмножества группы K. По определению свободного произведения элементы группы H можно рассматривать как различные элементы фактор-группы $\overline{K}$ группы K, получающейся присоединением соотношений множества $\mathcal{R}_H$. С другой стороны, по определению $\mathcal{R}_H$ всякий элемент $\overline{k} \in \overline{K}$ может быть представлен элементом из K вида $k_1 \cdots k_m$ для подходящих $k_i \in K_i$, $i = 1, \dots, m$. Это представление однозначно, поскольку в противном случае равенство двух таких представлений было бы выводимо из соотношений $\mathcal{R}_H$, которые выполнены и в группе H, вопреки тому, что в ней любые два таких представления должны различаться. Отождествляя $\overline{K}$ с множеством всех таких представлений, получаем изоморфизм групп

$$\overline{K} \to H, \quad \overline{k} \mapsto k_1 \cdots k_m.$$

Обозначим через Q композицию естественного эпиморфизма $K \to \overline{K}$ с этим изоморфизмом. Тогда отображение $Q : K \to H$

является эпиморфизмом, а вычисление $Q(k)$ для $k \in K$ состоит в приведении k к виду $k_1 \cdots k_m$ последовательным применением соотношений из $\mathcal{R}_H$. Следующая процедура описывает процесс такого приведения.

Шаг 1. Если слово k пусто, то полагаем $Q(k) = k$.

Шаг 2. Используя соотношения вида $x^{-1}yxy' \in \mathcal{R}_H$ для $x \in K^{(1)}$ и $y \in K_1$, приведём k к виду $k_1\widetilde{k}$, где $k_1 \in K_1$ и $\widetilde{k} \in \widetilde{K} = K_2 * \cdots * K_m$.

Шаг 3. Применяя процедуру рекурсивно к $\widetilde{k} \in \widetilde{K}$ и $\widetilde{H} = K^{(2)}$, найдём $Q(\widetilde{k})$ и положим $Q(k) = k_1Q(\widetilde{k})$.

Для оценки сложности заметим, что длина любого промежуточного слова, возникающего при выполнении описанной процедуры, не превосходит $|k|$. Кроме того, количество рекурсивных вызовов (на шаге 3) не превосходит m. Таким образом, время работы процедуры не превосходит полинома от $|k|$ и $|H|$. Лемма доказана. □

3.4. Опишем основную конструкцию настоящего параграфа. Пусть $K_1, \ldots, K_m$ – попарно непересекающиеся циклические группы простых порядков и $H = \Pi(K_1, \ldots, K_m)$. Пусть, кроме того (R_i, A_i, P_i) – гомоморфная криптосистема над группой K_i относительно гомоморфизма $f_i : G_i \to K_i$ из параграфа 2, $i = 1, \ldots, m$. Не умаляя общности предположим, что группы $G_1, \ldots, G_m$ попарно не пересекаются. Положим $G = G_1 * \cdots * G_m$. Тогда по определению f^* (см. формулу (2)) и лемме 3.3 отображение $f = Qf^*$ из G в H является эпиморфизмом.

Теорема 3.4. *Тройка (R, A, P), где R – произвольное множество различных представителей правых классов смежности группы G по подгруппе* $\ker(f)$, *удовлетворяющее условию* (H2) *определения* 1.1,

$$A = \{(a, r) \in A^* \times R^* : \ f(r) = 1_H\}, \quad P : A \to G, \ (a, r) \mapsto \overline{P^*(a)r},$$

где A^*, P^* определены в параграфе 3.2 *и R^* определено в* (5), *является гомоморфной криптосистемой над группой H относительно гомоморфизма $f : G \to H$.*

Доказательство. Из определения R^* следует, что для всякого $g \in G$ существуют единственные элементы $g_0 \in \ker(f^*)$ и $r \in R^*$, для которых $g = g_0 r$. Имеем $f(g) = Q(f^*(g_0) f^*(r)) = Q(f^*(r)) = f(r)$. Поэтому $g \in \ker(f)$ тогда и только тогда, когда $f(r) = 1_H$. По лемме 3.2 отсюда вытекает, что $\mathrm{im}(P) = \ker(f)$. Далее, используя замечания перед леммой 3.2 о случайном порождении элементов множества A^*, и принимая во внимание, что множества R_i, $i = 1, \ldots, m$, заданы явно, мы получаем эффективный способ порождения элементов множества A. Поэтому выполнено условие (H1) определения 1.1. Остаётся убедиться, что выполнено условие (H3) этого определения, т.е. что P является секретно-обратимой функцией.

Во-первых, отметим, что по утверждению (i1) леммы 3.2 и лемме 3.3 отображение P вычислимо за полиномиальное время. Во-вторых, по условию (H3) для гомоморфной криптосистемы (R_i, A_i, P_i) имеется алгоритм, который по заданным $i \in \{1, \ldots, m\}$ и $g_i \in G_i$ эффективно находит некоторый элемент множества $P_i^{-1}(g_i)$. Исходя из этого покажем, что отображение P может быть эффективно обращено. Действительно, в этом случае для каждого $g \in G$ элемент $f^*(g) \in K$ эффективно вычислим. Поскольку $g = g_0 r$ для однозначно определённых элементов $g_0 \in \ker(f^*)$ и $r \in R^*$, а $f^*(r) = f^*(g)$, мы можем найти элемент r, а потому (за то же время) и элемент $g_0 = g r^{-1}$. По утверждению (i2) леммы 3.3 мы также можем найти элемент $a \in A^*$, для которого $P^*(a) = g_0$. Таким образом, для обращения P достаточно уметь проверять равенство $f(r) = 1_H$ (если оно выполнено, то $(a, r) \in A$ и $P(a, r) = g$). Имеем $f(r) = Q(f^*(r))$. Далее, по условию (H2) для гомоморфной криптосистемы (R_i, A_i, P_i) мы можем найти элемент $f^*(r)$ и, следовательно, по лемме 3.3 элемент $Q(f^*(r))$ и, в конечном счёте, проверить равенство $f(r) = 1_H$.

Наконец, предположим что мы умеем эффективно обращать P. Пусть $g \in G$. Если $g \notin \ker(f)$, то, очевидно, и $g \notin \ker(f^*)$. Пусть теперь $g \in \ker(f)$ и $(a, r) \in A$ – доказательство для g, то есть $\overline{P^*(a)} r = g$. Поскольку r принадлежит множеству различных представителей R^* правых классов смежности по подгруппе $\ker(f^*)$ группы G, то $g \in \ker(f^*)$ тогда и только тогда, когда $r = 1_G$. Более того, если $r = 1_G$, то, очевидно, и $P^*(a) = g$. Поэтому задача нахождения $(P^*)^{-1}$ сводится в полиномиальное время к задаче нахождения P^{-1}. Следовательно, по утверждению (i3) леммы 3.2 задача нахождения P_i^{-1}, $i = 1, \ldots, m$, сводится в полиномиальное время к задаче нахождения P^{-1}. Таким образом, мы доказали, что функция P эффективно обратима тогда и только тогда, когда для каждого $i = 1, \ldots, m$ функция P_i эффективно обратима. Это показывает, что P – секретно-обратимая функция, что и требовалось доказать. $\square$

Отметим, что нетрудно явно построить некоторое множество R, удовлетворяющее условию теоремы 3.4, т.е. условию (H2). Именно, для каждого элемента $h \in H$ найдём представление $h = k_1 \cdots k_m$, где $k_i \in K_i$ (см. параграф 3.3), и выберем $r_i \in R_i$ так, чтобы $f_i(r_i) = k_i$, $i = 1, \ldots, m$. Тогда в качестве R можно взять множество всех элементов вида $r_1 \cdots r_m$ для всех $h \in H$.

Из теорем 2.2 и 3.4 немедленно получается следующее утверждение.

Следствие 3.5. *Пусть $K_1, \ldots, K_m$ попарно непересекающиеся циклические группы простых порядков, $m \geqslant 1$. Тогда $\Pi(K_1, \ldots, K_m) \in \mathcal{G}_{crypt}$.* $\square$

3.5. Частными случаями полупрямых произведений являются прямое произведение и сплетение. Действительно, сплетение групп G_1 и G_2 определяется как полупрямое произведение группы $G_1^{|G_2|} = G_1 \times \cdots \times G_1$ и группы G_2, действующей на этом произведении перестановками сомножителей, см. напр. [10]. Таким образом в качестве следствия теоремы 3.4 мы получаем, что класс $\mathcal{G}_{crypt}$ содержит группы, получающиеся с помощью прямых произведений и сплетений из циклических групп простых порядков (ср. следствие 3.5). Используя это обстоятельство мы докажем основной результат настоящей статьи.

Теорема 3.6. *Всякая неединичная разрешимая группа содержится в классе $\mathcal{G}_{crypt}$.*

Доказательство. Хорошо известно, что всякая разрешимая группа может быть построена из циклических групп простого порядка последовательными циклическими расширениями. С другой стороны, согласно [10, Теорема 6.2.8] любое расширение одной группы с помощью другой изоморфно подгруппе их сплетения. Поэтому достаточно проверить (см. следствие 3.5), что любая неединичная подгруппа полупрямого произведения циклических групп простых порядков принадлежит классу $\mathcal{G}_{crypt}$.

Для доказательства последнего утверждения рассмотрим произвольную группу $H \in \mathcal{G}_{crypt}$. Тогда существует гомоморфная криптосистема $\mathcal{S} = (R, A, P)$ над H относительно некоторого эпиморфизма $f : G \to H$. Не умаляя общности можно считать, что $\mathcal{S}$ есть гомоморфная криптосистема из теоремы 3.4. Для заданной явно неединичной подгруппы H' группы H положим $G' = f^{-1}(H')$, $f' = f|_{G'}$ и $\mathcal{S}' = (R', A', P')$, где $R' = R \cap f^{-1}(H')$,

$$A' = \{(a, r) \in A^* \times (R^*)' : \ f(r) = 1_H\}, \quad P' : A' \to G', \ (a, r) \mapsto \overline{P^*(a)r}$$

Тогда $\mathcal{S}'$ является гомоморфной криптосистемой над H' относительно гомоморфизма $f' : G' \to H'$. Действительно, представим группу G' как подгруппу группы G, порождённую объединением множеств $\mathrm{im}\,(P')$ и R'. (В этом представлении мы не сможем эффективно распознавать принадлежность элемента группы G к подгруппе G', но этого и не требуется.) Тогда условия (H1) и (H2) определения 1.1 выполнены для $\mathcal{S}'$, поскольку они выполняются для $\mathcal{S}$ (чтобы породить случайный элемент из A', достаточно породить случайный элемент r' из $(R^*)'$, для чего, в свою очередь, достаточно породить случайный элемент $r \in R^*$ и положить $r' = \overline{r\widetilde{r}}$, где $\widetilde{r}$ – элемент из R', для которого $f(r)f(\widetilde{r})^{-1} \in H'$). Поскольку $\ker\,(f') = \ker\,(f)$, то и $\mathrm{im}\,(P') = \ker\,(f')$. Наконец условие (H3) также выполнено для $\mathcal{S}'$, поскольку оно выполнено для $\mathcal{S}$.$\square$

Следует отметить, что изложенная в настоящем параграфе конструкция гомоморфной криптосистемы над разрешимой группой H имеет, скорее, теоретическое значение. Вычислительная сложность алгоритмов, использованных в конструкции, оценивается сверху полиномом, степень которого зависит от $|H|$. Помимо этого, размер представления группы G может быть экспоненциальным от $|H|$ из-за использования полупрямых произведений. Было бы интересно построить более экономные представления для маленьких групп H.

Из теоремы 3.6 вытекает, что существует гомоморфная криптосистема над симметрической группой $\mathrm{Sym}\,(n)$ при $n \leqslant 4$. Кажется важным построить гомоморфную криптосистему над произвольной симметрической группой, поскольку такая криптосистема позволила бы осуществлять секретные вычисления с любыми группами перестановок и, более того, позволила бы реализовать любую булевскую схему в смысле [1]. В этой связи упомянем, что любая булевская схема логарифмической глубины может быть реализована в произвольной неразрешимой группе (см. [1]). С другой стороны, в [1] было доказано, что для всякой нильпотентной группы найдётся булевская схема логарифмической глубины, которая не может быть реализована в этой группе. Если же группа разрешима, но не нильпотентна, то известны лишь реализации экспоненциального размера и гипотеза состоит в том, что реализации меньшего размера невозможны [1]. Таким образом, если бы эта гипотеза оказалась неверной, то по теореме 3.6 можно было бы сделать секретной любую булевскую схему.

Благодарности. Авторы признательны Математическому Институту общества Макса Планка (Бонн), во время пребывания в котором эта работа была сделана, а также Э. Беккеру, который обратил внимание авторов на гомоморфные криптосистемы, и И. Шпарлинскому за полезные замечания.

Литература

1. D. M. Barrington, H. Straubing, D. Therien, *Nonuniform automata over groups.* — Information and Computation **132** (1990), 89–109.
2. J. Benaloh, *Dense probabilistic encryption.* — First Ann. Workshop on Selected Areas in Cryptology (1994), pp. 120–128.
3. S. Cook, R. A. Reckhow, *The relative efficiency of propositional proof systems.* — J. Symbolic Logic **44** (1979), 36–50.
4. D. Coppersmith, I. Shparlinski, *On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping.* — J. Cryptology **13** (2000), 339–360.
5. Г. Дэвенпорт, *Мультипликативная теория чисел.* Наука, М. (1971).
6. Do Long Van, A. Jeyanthi, R. Siromony, K. Subramanian, *Public key cryptosystems based on word problems.* in: ICOMIDC Symp. Math. of Computations, Ho Chi Minh City, April (1988).
7. 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.
8. S. Goldwasser, M. Bellare, *Lecture Notes on Cryptography.* — http://www-cse.ucsd.edu/users/mihir/papers/gb.html, 2001.
9. S. Goldwasser, S. Micali, *Probabilistic encryption.* — J. Comput. Syst. Sci. **28** (1984), 270–299.
10. М. И. Каргаполов, Ю. И. Мерзляков, *Основы теории групп.* Наука, М. (1977).
11. 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 Computer Science **1880** (2000), 166–183.
12. 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 Computer Science **576** (1991), 252–266.

13. W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations.* — Interscience Publishers, New York-London-Sydney (1966).
14. U. Maurer, S. Wolf, *Lower bounds on generic algorithms in groups.* — Lecture Notes in Computer Science **1403** (1998), 72–84.
15. R. Motwani, P. Raghavan, *Randomized Algorithms.* Cambridge University Press (1995).
16. D. Naccache, J. Stern, *A new public key cryptosystem based on higher residues.* in: Proc. 5th ACM Conference on Computer and Communication Security (1998), pp. 59–66.
17. T. Okamoto, S. Uchiyama, *A New Public-Key Cryptosystem as Secure as Factoring.* — Lecture Notes in Computer Science **1403** (1998), 308–317.
18. S.-H. Paeng, D. Kwon, K.-C. Ha, J. H. Kim, *Improved public key cryptosystem using finite non-abelian groups.* Preprint NSRI, Korea.
19. P. Paillier, *Public-Key Cryptosystem Based on Composite Degree Residuosity Classes.* — Lecture Notes in Computer Science **1592** (1999), 223-238.
20. M. O. Rabin, *Probabilistic algorithms in finite fields.* — SIAM J. Comput. **9** (1980), 273–280.
21. D. K. Rappe, *Algebraisch homomorphe kryptosysteme.* — Diplomarbeit, Dem Fachbereich Mathematik der Universität Dortmund, Oktober 2000.
22. R. L. Rivest, L. Adleman, M. Dertouzos, *On Data Banks and Privacy Homomorphisms.* Foundation of Secure Computation, Academic Press (1978), pp. 169–177.
23. T. Sander, A. Young, M. Young, *Noninteractive cryptocomputing for NC^1.* in: Proc. 40th IEEE Symp. Found. Comput. Sci (1999), pp. 554–566.
24. A. Yao, *How to generate and exchange secrets.* in: Proc. 27th IEEE Symp. Found. Comput. Sci (1986), pp. 162–167.

Grigoriev D. Yu., Ponomarenko I. N. On non-abelian homomorphic public-key cryptosystems.

We construct homomorphic cryptosystems being (secret) epimorphisms $f : G \to H$, where G, H are (publically known) groups and H is finite. A letter of a message to be encrypted is an element $h \in H$, while its encryption $g \in G$ is such that $f(g) = h$. A homomorphic cryptosystem allows one to perform computations (operating in a group G) with encrypted information (without knowing the original message over H).

In this paper certain homomorphic cryptosystems are constructed for the first time for non-abelian groups H (earlier, homomorphic cryptosystems were known only in the Abelian case). In fact, we present such a system for any solvable (fixed) group H.

Поступило 7 декабря 2002 г.

IRMAR, Université de Rennes
Beaulieu, 35042, Rennes, France
http://maths.univ-rennes1.fr/~dima
С.-Петербургское отделение
Математического института
им.В. А. Стеклова РАН
inp@pdmi.ras.ru