Н. Инассаридзе, М. Хазарадзе, Э. В. Хмаладзе, Б. Месаблишвили, Об односторонних гомоморфизмах колец, *Итоги науки и техн. Сер. Соврем. мат. и ее прил. Темат. обз.*, 2020, том 177, 80–86

DOI: https://doi.org/10.36535/0233-6723-2020-177-80-86

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 177 (2020). С. 80–86
DOI: 10.36535/0233-6723-2020-177-80-86

УДК 512.552; 509.07; 289.23.15.25

ОБ ОДНОСТОРОННИХ ГОМОМОРФИЗМАХ КОЛЕЦ

© 2020 г. **Н. ИНАССАРИДЗЕ, М. ХАЗАРАДЗЕ, Э. ХМАЛАДЗЕ, Б. МЕСАБЛИШВИЛИ**

Аннотация. В статье предложен новый кандидат на роль одностороннего гомоморфизма кольца, вводимый с помощью одностороннего гомоморфизма (неабелевых) групп. В качестве приложения предложенного одностороннего гомоморфизма кольца приведена многосторонняя схема цифровой подписи.

***Ключевые слова*:** односторонний гомоморфизм, групповое кольцо, многостадийная схема цифровой подписи.

ON ONE-WAY RING HOMOMORPHISMS

© 2020 **N. INASSARIDZE, M. KHAZARADZE, E. KHMALADZE, B. MESABLISHVILI**

Abstract. In this article, we propose a new candidate for a one-way ring homomorphism induced by a one-way (non-abelian) group homomorphism. A multi-party digital signature scheme is also given as an application of the proposed one-way ring homomorphism.

***Keywords and phrases*:** one-way homomorphism, group ring, multi-party digital signature scheme.
***AMS Subject Classification*:** 94A60, 94A62, 16S34

1. Введение. В криптографии односторонними функциями называются функции, которые легко вычислить для любых исходных данных, но для которых трудно найти обратную функцию от образа при случайных начальных данных. Односторонние функции представляют собой фундаментальную основу современной криптографии и играют важную роль в построении криптосистем, поскольку понятие односторонности было впервые введено для функций кодирования (см. [4,5,15]). Они используются в основанных на хэше схемах цифровой подписи (см. [8,11,14,16]), которые составляют многообещающую альтернативу схемам цифровой подписи RSA и схемам, основанным на эллиптических кривых, в современную эпоху постквантовых криптосистем. Хотя есть всеобщая убежденность, что односторонние функции существуют, дать доказательство их существования по крайней мере не легче, чем показать, что $P \neq NP$. Таким образом, ниже мы всегда будем ссылаться на односторонние функции при предположении, что они существуют.

Делалось много попыток использовать современные алгебраические структуры в различных криптографических конструкциях (см., например, [1, 2, 6, 13, 17, 18]). Данная статья может рассматриваться в этом контексте, поскольку в ней предложена конструкция, которая могла бы служить новым кандидатом на роль односторонней функции, имеющей алгебраическую природу (некоммутативного) гомоморфизма кольца. Поскольку определение односторонних функций зависит только от длины двоичных последовательностей входа-выхода и от их вычислимости за полиномиальное время, это определение мало что говорит о лежащих в их основе алгебраических

Работа Н. Инассаридзе выполнена при поддержке гранта STCU-2016-08/MTCU 6321 и гранта № MTM2016-79661-P (Agencia Estatal de Investigacíon).
Работа Э. Хмаладзе выполнена при поддержке гранта № MTM2016-79661-P (Agencia Estatal de Investigacíon).

структурах. Однако некоторые типичные и полезные функции кодирования (т.е. те функции, для которых неизвестен алгоритм, обращающий их за полиномиальное время), которые могут оказаться односторонними, являются гомоморфизмами групп (см. ниже примеры 6 и 7). Очевидно, возникает следующий естественный вопрос.

Вопрос 1 (см. [2])**.** Существуют ли односторонние гомоморфизмы, ассоциированные с какими-либо алгебраическими структурами, отличными от групп?

В [2] обсуждаются соотношения между односторонними гомоморфизмами групп и односторонними гомоморфизмами колец. Показано, что если существует односторонний гомоморфизм групп $f : U \to V$, то существует односторонний гомоморфизм колец

$$F : \mathbb{Z}_n \ltimes U \to \mathbb{Z}_m \ltimes V, \quad ([k], u) \mapsto ([k], f(u))$$

где U, V — такие конечные абелевы группы, что $|U| = n$, $|V| = m$, $m \mid n$; здесь $\ltimes$ означает полупрямое произведение (см. определение 9). Приведены некоторые примеры таких гомоморфизмов колец, которые являются односторонними при стандартных криптографических предположениях.

Этот результат также отвечает утвердительно на следующий вопрос, поставленный в [2].

Вопрос 2. Существует ли такая функция кодирования $f : A \to B$, что для данных $f(x)$ и $f(y)$ как $f(x+y)$, так и $f(xy)$ можно эффективно вычислить для некоторых алгебраических структур?

Построенный гомоморфизм колец, основанный на одностороннем гомоморфизме групп, зависит от порядка лежащей в основе группы и, следовательно, не является односторонним, если порядок группы не вычисляется за полиномиальное время. Таким образом, возникают еще два вопроса.

Вопрос 3. Существует ли односторонний гомоморфизм колец, основанный на одностороннем гомоморфизме групп, не зависящий от порядка лежащей в основе группы?

Вопрос 4. Существует ли односторонний гомоморфизм колец, основанный на одностороннем гомоморфизме неабелевых групп?

В данной статье предложен кандидат на роль одностороннего гомоморфизма колец, основанный на одностороннем гомоморфизме групп, положительно отвечающий как на вопрос 3, так и на вопрос 4, что заполняет пробел, упомянутый в [2]. Затем эта конструкция применяется для получения многосторонней схемы цифровой подписи. Структура статьи такова. После напоминания в разделе 2 определений, известных результатов и различных аспектов теории односторонних функций, которые нам потребуются, в разделе 3 мы покажем, как построить односторонний гомоморфизм колец для данного одностороннего гомоморфизма групп и как использовать такие гомоморфизмы колец для того, чтобы получить многостороннюю схему цифровой подписи аналогично тому, как это сделано в [2]. В конце раздела 3 мы обсудим рассмотрим эффективность этой схемы.

2. Предварительные сведения и известные результаты.

2.1. Обозначения. В этом разделе мы напомним некоторые основные факты об односторонних функциях, а также зафиксируем систему обозначений и терминологию. Будем следовать обычным соглашениям, как, например, в [3]. Всюду в статье будем использовать обозначение l в качестве параметра безопасности, включенного в наши определения.

Говорят, что функция $f : \mathbb{N} \to \mathbb{R}^+$ является пренебрежимой, если для любого положительного целого числа c существует такое целое число N_c, что

$$f(n) < 1/n^c \quad \text{для всех} \quad n > N_c.$$

Будем обозначать через $\{0,1\}^*$ и $\{0,1\}^n$ ($n \in \mathbb{N}$) множества всех последовательностей битов конечной длины и длины n соответственно.

Говорят, что алгоритм $\mathcal{A}$ является *вероятностным за полиномиальное время* (*ВПВ-алгоритмом*), если его поведение определяется подбрасыванием монеты и существует такой полином p, что среднее время прохождения алгоритма $\mathcal{A}$ на входах размера l меньше, чем $p(l)$.

Обозначим через $\mathcal{A}(x)$ значение, выдаваемое алгоритмом $\mathcal{A}$ на выходе для значения x на входе. Пишем $y \in \mathcal{A}(x)$, если алгоритм $\mathcal{A}$ выдает y при входном значении x для некоторых значений

внутреннего случайного подбрасывания монеты, в то время как $y = \mathcal{A}(x)$ означает результат работы алгоритма $\mathcal{A}$ при входном значении x и присвоения ему значения y на выходе.

Говорят, что вычислительная задача вычислительно неосуществима, если никакой ВПВ-алгоритм не выполняет поставленную задачу с ненулевой вероятностью.

Говорят, что конечное множество $\mathfrak{R}$ выборочно, если существует ВПВ-алгоритм, который случайным образом выбирает элемент из равномерного распределения на $\mathfrak{R}$. Если $\mathfrak{R}$ выборочно, то пишем $r \stackrel{\$}{\leftarrow} \mathfrak{R}$ для эксперимента равномерного выбора случайной величины из $\mathfrak{R}$ и присвоения r его значения.

Через $\Pr[A : B; C]$ обозначим вероятность того, что логическое выражение A выполняется для данного эксперимента, состоящего из последовательного выполнения B и C.

2.2. Односторонние функции. Интуитивно, односторонняя функция (ОФ) — это функция, которую легко вычислить, но вычислительно сложно обратить.

Определение 5. Функция $f : \{0,1\}^* \to \{0,1\}^*$ называется *односторонней функцией*, если ее:
легко вычислить: существует ВПВ-алгоритм, который на входе x выдает значение $f(x)$;
трудно обратить: не существует такого ВПВ-алгоритма $\mathcal{A}$, что

$$\Pr\left[f(x') = y : x \stackrel{\$}{\leftarrow} \{0,1\}^l;\ y = f(x);\ x' = \mathcal{A}(y)\right]$$

— непренебрежимая функция длины x.

В дальнейшем пишем «односторонняя функция» (соответственно, «гомоморфизм»), имея в виду кандидата на роль односторонней функции (соответственно, гомоморфизма).

Приведем несколько хорошо известных примеров односторонних функций, широко используемых в криптографических схемах в настоящее время.

Пример 6. Пусть f — классическая функция кодирования

$$f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*, \quad f(x) = g^x \pmod{p},$$

где p — простое число >2 и $g \in \mathbb{Z}_p^*$. Тогда f — гомоморфизм групп, действующий из $\mathbb{Z}_{p-1}$ на циклическую группу $\langle g\rangle \subseteq \mathbb{Z}_p^*$, порожденную g. В частности, если g — примитивный корень в $\mathbb{Z}_{p-1}$, то f — изоморфизм абелевых групп $\mathbb{Z}_{p-1}$ и $\mathbb{Z}_p^*$.

Пример 7. Пусть h — хорошо известная RSA-функция кодирования

$$h : \mathbb{Z}_n^* \to \mathbb{Z}_n^*, \quad h(x) = x^e \pmod{n},$$

где n (модуль) и e (показатель кодирования) — подходящим образом выбранные целые числа. Тогда h — изоморфизм групп.

Следовательно, если f в примере 6 и h в примере 7 действительно односторонние, то они являются односторонними гомоморфизмами групп.

Пример 8. Так называемая увеличенная матричная степенная функция (МСФ), представленная в [17], может рассматриваться как кандидат на роль одностороннего гомоморфизма неабелевых групп.

2.3. Основные результаты (см. [2]). Хорошо известно, что криптографические отображения, приведенные в примерах 6 и 7, являются гомоморфизмами групп, на которых конкретные гомоморфизмы колец, рассмотренные в [2], отождествляются как односторонние функции. В этом разделе сформулируем основной результат работы [2] в терминах полупрямых произведений колец. Сначала напомним следующее определение.

Определение 9. Пусть R — коммутативное кольцо и M — R-модуль. Полупрямое произведение R и M — это кольцо, обозначаемое $R \ltimes M$ и определенное следующим образом:

(i) множество, на котором оно определено, — это декартово произведение $R \times M$;
(ii) для всех $r, r' \in R$ и $m, m' \in M$ операции заданы следующим образом:

$$(r, m) + (r', m') = (r + r', m + m'), \quad (r, m) \cdot (r', m') = (rr', rm' + r'm).$$

Легко проверить, что $R \ltimes M$ действительно является коммутативным кольцом. Кроме того, полупрямое произведение функториально в следующем смысле: рассмотрим категорию, объекты которой — все пары (R, M), где R — коммутативное кольцо, M — R-модуль и морфизм из (R, M) в (R', M') является парой (ϕ, f), где $\phi : R \to R'$ — гомоморфизм колец и $f : M \to M'$ — гомоморфизм абелевых групп, для которых равенство $f(rm) = \phi(r)f(m)$ выполняется при всех $r \in R$, $m \in M$. Тогда полупрямое произведение является функтором, действующим из этой категории в категорию коммутативных колец (о категориях и функторах см. [10]). Следовательно, для любой такой пары (ϕ, f) существует естественный гомоморфизм колец

$$\phi \ltimes f : R \ltimes M \to R' \ltimes M', \quad (\phi \ltimes f)(r, m) = (\phi(r), f(m)).$$

Сформулируем основной результат [2] следующим образом.

Теорема 10. *Пусть U и V — такие конечные абелевы группы, что $|U| = n$ и $|V| = m$, $m \mid n$. Если существует односторонний гомоморфизм групп $f : U \to V$, то существует односторонний гомоморфизм колец*

$$\pi \ltimes f : \mathbb{Z}_n \ltimes U \to \mathbb{Z}_m \ltimes V,$$

где $\pi : \mathbb{Z}_n \to \mathbb{Z}_m$ — естественная проекция колец и U (соответственно, V) рассматривается как $\mathbb{Z}_n$-модуль (соответственно, $\mathbb{Z}_m$-модуль).

С помощью этого результата в [2] получены конкретные примеры гомоморфизмов колец, являющиеся односторонними при стандартном криптографическом предположении. Это дает утвердительный ответ на вопросы 1 и 2.

Односторонние гомоморфизмы колец можно широко использовать в криптосистемах как важное основание. Например, фундаментальное приложение теоремы 10 дано в [2] в виде построения новой схемы многосторонней цифровой подписи.

3. Новые односторонние гомоморфизмы колец и схема многосторонней цифровой подписи. Сначала напомним хорошо известную алгебраическую конструкцию, которая потребуется в дальнейшем.

Определение 11. Пусть G — группа и R — коммутативное кольцо. Групповое кольцо группы G над R обозначается $R[G]$ и определяется как множество всех формальных сумм $\sum r_i g_i$, где $g_i \in G$, $r_i \in R$, и все r_i, кроме их конечного числа, являются нулевыми. Сумма двух элементов из $R[G]$ определяется формулой

$$\sum r_i g_i + \sum r'_i g_i = \sum (r_i + r'_i) g_i,$$

где умножение определено дистрибутивно с помощью $g \cdot r = rg$.

В дальнейшем для элемента общего вида из кольца $R[G]$ пишем $\sum\limits_{i=1}^{k} r_i g_i$, где $r_i \neq 0$, $1 \leqslant i \leqslant k$, и называем k *длиной* этого элемента.

Следующее предложение, утверждающее, что конструкция группового кольца функториальна, является хорошо известным фактом в алгебре (см., например, [9, 10]).

Предложение 12. *Пусть R — коммутативное кольцо и $\alpha : G \to G'$ — гомоморфизм групп. Тогда существует естественным образом индуцированный гомоморфизм колец*

$$R[\alpha] : R[G] \to R[G'],$$

заданный формулой

$$R[\alpha] \left(\sum_{i=1}^{k} r_i g_i \right) = \sum : k_{i=1} r_i \alpha(g_i).$$

В частности, для кольца целых чисел $R = \mathbb{Z}$ справедлива следующая теорема.

Теорема 13. *Пусть G и G' — группы. Если существует односторонний гомоморфизм групп $\alpha : G \to G'$, то существует односторонний гомоморфизм колец*

$$\mathbb{Z}[\alpha] : \mathbb{Z}[G] \to \mathbb{Z}[G'],$$

заданный как в предложении 12.

Замечание 14. Теорема 13 и пример 8 дают положительный ответ на вопросы 3 и 4.

Теперь дадим приложение нашего одностороннего гомоморфизма колец, построив новую схему многосторонней цифровой подписи аналогично [2]. Дальнейшую информацию о многосторонних цифровых подписях см. в [7, 12].

Чтобы предложить конкретную схему цифровой подписи, нужно разложить любой элемент группового кольца $\mathbb{Z}[\mathbb{Z}_q]$:

$$w = \sum_{i=1}^{k} n_i g_i, \quad \text{где} \quad n_i \in \mathbb{Z} \quad \text{и} q \quad g_i \in \mathbb{Z}_q,$$

следующим образом:

$$w = w_{\text{pos}} + w_{\text{neg}}, \quad \text{где} \quad w_{\text{pos}} = \sum_{j=1}^{k_1} n_{i_j} g_{i_j} \quad \text{и} \quad w_{\text{neg}} = \sum_{j'=1}^{k_2} m_{i_{j'}} g_{i_{j'}}; \tag{3.1}$$

здесь $n_{i_j} > 0$ для всех $1 \leqslant j \leqslant k_1$, $m_{i_{j'}} < 0$ для всех $1 \leqslant j' \leqslant k_2$ и $k_1 + k_2 = k$.

Пусть $U_1, U_2, \ldots, U_t$ — персоны, которые подписываются, и V — проверяющий. Пусть

$$H : \{0,1\}^* \to \{0,1\}^l \subseteq \mathbb{Z}_{p-1}$$

— хэш-функция для некоторого простого числа $p > 2$ и $M \in \{0,1\}^*$ — сообщение, которое должно быть подписано всеми сторонами. Схема многосторонней подписи позволяет проверяющему V установить, что M подписано всеми U_i, $1 \leqslant i \leqslant t$.

3.1. Генерация ключа. Для каждого подписывающегося U_i, $1 \leqslant i \leqslant t$, пара из секретного и открытого ключа генерируется следующим образом.

Зафиксируем некоторое положительное целое число N и рассмотрим подмножество K множества $\mathbb{Z}[\mathbb{Z}_{p-1}]$, состоящее из всех элементов $\sum\limits_{i=1}^{k} n_i g_i$ при $-N \leqslant n_i \leqslant N$ для всех $i = 1, 2, \ldots, q$. Секретный ключ — это случайно порождаемый и равномерно распределенный элемент $k_i^{\text{priv}} \in K \subset \mathbb{Z}[\mathbb{Z}_{p-1}]$, а открытый ключ является таким элементом $k_i^{\text{pub}} \in \mathbb{Z}[\mathbb{Z}_p^*]$ группового кольца, что

$$\mathbb{Z}[\alpha](k_i^{\text{priv}}) = k_i^{\text{pub}},$$

где α дано в примере 6. Из того факта, что $\mathbb{Z}[\alpha]$ — изоморфизм колец (согласно предложению 12), вытекает следующее утверждение.

Лемма 15. *Пусть*

$$k_i^{\text{priv}} = k_{\text{pos},i}^{\text{priv}} + k_{\text{neg},i}^{\text{priv}}, \quad k_i^{\text{pub}} = k_{\text{pos},i}^{\text{pub}} + k_{\text{neg},i}^{\text{pub}}$$

— разложения секретного и открытого ключа согласно (3.1). *Тогда выполняются равенства*

$$\mathbb{Z}[\alpha](k_{\text{pos},i}^{\text{priv}}) = k_{\text{pos},i}^{\text{pub}}, \quad \mathbb{Z}[\alpha](k_{\text{neg},i}^{\text{priv}}) = k_{\text{neg},i}^{\text{pub}}.$$

3.2. Генерация подписи. Для данного элемента $v = \sum\limits_{i=1}^{k} n_i h_i \in \mathbb{Z}[\mathbb{Z}_p^*]$ обозначим через $\tilde{v}$ элемент

$$\sum_{i=1}^{k} n_i \left(h_i \mod (p-1)\right).$$

Очевидно, $\tilde{v} \in \mathbb{Z}[\mathbb{Z}_{p-1}]$.

Сообщение $M \in \{0,1\}^*$ подписывается каждым участником U_i, $1 \leqslant i \leqslant t$, с помощью его секретного ключа k_i^{priv}. Сначала вычисляется дайджест сообщения $H(M) = D \in \mathbb{Z}_{p-1}$.

(i) Участник U_1 раскладывает свой секретный и открытый ключ согласно (3.1) следующим образом:

$$k_1^{\text{priv}} = k_{\text{pos},1}^{\text{priv}} + k_{\text{neg},1}^{\text{priv}} \in \mathbb{Z}[\mathbb{Z}_{p-1}], \quad k_1^{\text{pub}} = k_{\text{pos},1}^{\text{pub}} + k_{\text{neg},1}^{\text{pub}} \in \mathbb{Z}[\mathbb{Z}_p^*].$$

Наконец, U_1 вычисляет

$$s_1 = k_{\text{pos},1}^{\text{priv}} \cdot \widetilde{k_{\text{neg},1}^{\text{pub}}} + D \cdot k_{\text{neg},1}^{\text{priv}}$$

и посылает M и s_1 участнику U_2.

(ii) Участник U_i, $2 \leqslant i \leqslant t-1$, раскладывает свой секретный ключ согласно (3.1) следующим образом:

$$k_i^{\mathrm{priv}} = k_{\mathrm{pos},i}^{\mathrm{priv}} + k_{\mathrm{neg},i}^{\mathrm{priv}} \in \mathbb{Z}[\mathbb{Z}_{p-1}], \quad k_i^{\mathrm{pub}} = k_{\mathrm{pos},i}^{\mathrm{pub}} + k_{\mathrm{neg},i}^{\mathrm{pub}} \in \mathbb{Z}[\mathbb{Z}_p^*].$$

Наконец, U_i вычисляет

$$s_i = s_{i-1} \cdot \left(k_{\mathrm{pos},i}^{\mathrm{priv}} \cdot \widetilde{k_{\mathrm{neg},i}^{\mathrm{pub}}} + D \cdot k_{\mathrm{neg},i}^{\mathrm{priv}} \right)$$

и посылает M и s_i участнику U_{i+1}.

(iii) Участник U_t раскладывает свой секретный ключ согласно (3.1) следующим образом:

$$k_t^{\mathrm{priv}} = k_{\mathrm{pos},t}^{\mathrm{priv}} + k_{\mathrm{neg},t}^{\mathrm{priv}} \in \mathbb{Z}[\mathbb{Z}_{p-1}], \quad k_t^{\mathrm{pub}} = k_{\mathrm{pos},t}^{\mathrm{pub}} + k_{\mathrm{neg},t}^{\mathrm{pub}} \in \mathbb{Z}[\mathbb{Z}_p^*].$$

Наконец, U_t вычисляет

$$s_t = s_{t-1} \cdot \left(k_{\mathrm{pos},t}^{\mathrm{priv}} \cdot \widetilde{k_{\mathrm{neg},t}^{\mathrm{pub}}} + D \cdot k_{\mathrm{neg},t}^{\mathrm{priv}} \right)$$

и посылает M и s_t проверяющему V.

Замечание 16. Коммутативность кольца $\mathbb{Z}[\mathbb{Z}_{p-1}]$ обеспечивает тот важный факт, что порядок подписывающихся не важен в этой схеме многосторонней подписи.

3.3. Проверка подписи. Чтобы проверить подпись s сообщения M, проверяющий V вычисляет дайджест сообщения $H(M) = D \in \mathbb{Z}_{p-1}$. Затем он раскладывает открытый ключ согласно (3.1) следующим образом:

$$k_i^{\mathrm{pub}} = k_{\mathrm{pos},i}^{\mathrm{pub}} + k_{\mathrm{neg},i}^{\mathrm{pub}} \in \mathbb{Z}[\mathbb{Z}_p^*], \quad 0 \leqslant i \leqslant t,$$

и затем подсчитывает элемент

$$v = \left(k_{\mathrm{pos},1}^{\mathrm{pub}} \cdot \mathbb{Z}[\alpha](\widetilde{k_{\mathrm{neg},1}^{\mathrm{pub}}}) + \mathbb{Z}[\alpha](D) \cdot k_{\mathrm{neg},1}^{\mathrm{pub}} \right) \cdots \left(k_{\mathrm{pos},t}^{\mathrm{pub}} \cdot \mathbb{Z}[\alpha](\widetilde{k_{\mathrm{neg},t}^{\mathrm{pub}}}) + \mathbb{Z}[\alpha](D) \cdot k_{\mathrm{neg},t}^{\mathrm{pub}} \right).$$

Наконец, V проверяет, верно ли, что

$$\mathbb{Z}[\alpha](s_t) = v.$$

Очевидно, что проверка этой схемы основана на свойстве гомоморфизма колец $\mathbb{Z}[\alpha]$ (см. теорему 13) и лемме 15.

3.4. Эффективность схемы. Для оценки эффективности этой схемы предположим, что длина k_i^{priv} не более, чем k. Тогда генерирование ключа для U_i требует 1 вычислений одностороннего гомоморфизма кольца $\mathbb{Z}[\alpha]$, что эквивалентно не более чем k вычислениям одностороннего гомоморфизма групп α (см. пример 6).

Размер секретных ключей, k_i^{priv}, составляет $\mathcal{O}(k \log(N(p-1))$ бит, а размер открытых ключей, k_i^{pub}, составляет $\mathcal{O}(k \log(Np)$ бит.

Вычисляя размер подписи, можно вывести, что размер s_1 равен размеру s_i/s_{i-1} для всех $2 \leqslant i \leqslant t$ и составляет $\mathcal{O}(k^2 \log(N(p-1))$ бит.

Подпись для всех t участников и проверка требуют одного и того же времени работы алгоритма, $\mathcal{O}(tk^2 + k^{2t})$, в то время как проверка требует кроме этого одно вычисление одностороннего гомоморфизма колец $\mathbb{Z}[\alpha]$.

СПИСОК ЛИТЕРАТУРЫ

1. *Anshel I., Anshel M., Goldfeld D.* An algebraic method for public-key cryptography// Math. Res. Lett. — 1999. — *6*. — P. 287–291.
2. *Chida E., Nishizeki T., Ohmori M., Shizuva H.* On the one-way algebraic homomorphism// IEICE Trans. Fundam. — 1996. — *E79-A*, № 1. — P. 54–60.
3. *Delfs H., Knebl H.* Introduction to Cryptography. Principles and Applications. — Berlin–Heidelberg: Springer-Verlag, 2015.
4. *Diffie W., Hellman M. E.* New directions in cryptography// IEEE Trans. Information Theory. — 1976. — *22*. — P. 644–654.

5. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms// Lect. Notes Comp. Sci. — 1985. — *196*. — P. 10–18.
6. *Inassaridze N., Kandelaki T., Ladra M.* Categorical interpretations of some key agreement protocols// J. Math. Sci. — 2013. — *195*, № 4. — P. 439–444.
7. *Itakura K., Nakamura K.* A public-key cryptosystem suitable for digital multi-signatures// Trans. Inform. Process. Soc. Jpn. — 1983. — *24*, № 2. — P. 474–480.
8. *Lamport L.* Constructing digital signatures from a one way function. `http://www.cacr.math.uwaterloo.ca`
9. *Lang S.* Algebra. — New York–Berlin–Heidelberg: Springer-Verlag, 2002.
10. *MacLane S.* Categories for the Working Mathematician. — New York–Berlin–Heidelberg: Springer-Verlag, 1978.
11. *Merkle R. C.* A certified digital signature// Lect. Notes Comput. Sci. — 1989. — *435*. — P. 218–238.
12. *Micali S., Ohta K., Reyzin L.* Accountable subgroup multisignatures// in: Proc. 8th ACM Conf. on Computer and Communications Security. — New York: ACM, 2001. — P. 245–254.
13. *Pavlovic D.* Chasing diagrams in cryptography// Lect. Notes Comput. Sci. — 2014. — *8222*. — P. 353–367.
14. *Rabin M. O.* Digitalized signatures// in: Foundations of Secure Communication. — Academic Press, 1978. — P. 155–168.
15. *Rivest R. L., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems// Commun. ACM. — 1978. — *21*, № 2. — P. 120–126.
16. *Rompel J.* One-way functions are necessary and sufficient for secure signatures// in: Proc. ACM STOC'90, 1990. — P. 387–394.
17. *Sakalauskas E.* Enhanced matrix power function for cryptographic primitive construction// Symmetry. — 2018. — *10*, № 2. — P. 43.
18. *Yanai N., Chida E., Mambo M.* A secure structured multisignature scheme based on a non-commutative ring homomorphism// IEICE Trans. Fundam. — 2011. — *E94-A*, № 6. — P. 54–60.

Инассаридзе Н.
Математический институт им. А. Размадзе, Тбилиси, Грузия;
Тбилисский государственный университет, Тбилиси, Грузия;
Грузинский технический университет, Тбилиси, Грузия
E-mail: `niko.inas@gmail.com`

Хазарадзе М.
Грузинский технический университет, Тбилиси, Грузия

Хмаладзе Э.
Математический институт им. А. Размадзе, Тбилиси, Грузия;
Тбилисский государственный университет, Тбилиси, Грузия;
Грузинский технический университет, Тбилиси, Грузия

Месаблишвили Б.
Математический институт им. А. Размадзе, Тбилиси, Грузия;
Тбилисский государственный университет, Тбилиси, Грузия
E-mail: `bachuki.mesablishvili@tsu.ge`