Гомоморфность некоторых криптографических систем на основе неассоциативных структур

А. В. ГРИБОВ
Московский государственный университет им. М. В. Ломоносова
e-mail: alexey.gribov@yandex.ru

УДК 512.548.7+004.056.55

Ключевые слова: неассоциативные алгебраические структуры, криптосистема с открытым ключом, гомоморфное шифрование.

Аннотация

Гомоморфное шифрование позволяет производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполняемых с открытым текстом. Многие классические криптосхемы, например Эль-Гамаля и RSA, обладают свойством гомоморфности относительно одной операции. В 2009 году впервые была предложена модель полногомоморфной алгебраической системы, т. е. системы, гомоморфной для операций умножения и сложения одновременно. Эта модель была представлена К. Джантри. Схема была основана на алгебраических решётках. М. ван Дийк, К. Джантри, С. Халеви и В. Вайкунтанатан предложили схему, основанную на целых числах. А. В. Грибовым, П. А. Золотых, А. В. Михалёвым была построена криптосистема над квазигрупповым кольцом, развивающая подход С. К. Росошека. В данной работе исследован вопрос гомоморфности схемы над квазигрупповым кольцом. Приведён пример квазигруппы, при которой криптосхема является гомоморфной. Также показана гомоморфность схемы Эль-Гамаля для медиальной квазигруппы.

Abstract

A. V. Gribov, Some homomorphic cryptosystems based on nonassociative structures, Fundamentalnaya i prikladnaya matematika, vol. 20 (2015), no. 1, pp. 135—143.

A homomorphic encryption allows specific types of computations on ciphertext and generates an encrypted result that matches the result of operations performed on the plaintext. Some classic cryptosystems, e.g., RSA and ElGamal, allow homomorphic computation of only one operation. In 2009, C. Gentry suggested a model of a fully homomorphic algebraic system, i.e., a cryptosystem that supports both addition and multiplication operations. This cryptosystem is based on lattices. Later M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan suggested a fully homomorphic system based on integers. In a 2010 paper of A. V. Gribov, P. A. Zolotykh, and A. V. Mikhalev, a cryptosystem based on a quasigroup ring was constructed, developing an approach of S. K. Rososhek, and a homomorphic property of this system was investigated. An example of a quasigroup for which this system is homomorphic is given. Also a homomorphic property of the ElGamal cryptosystem based on a medial quasigroup is shown.

Фундаментальная и прикладная математика, 2015, том 20, № 1, с. 135—143.

1. Криптосхема для квазигруппового кольца

Пусть K — кольцо с единицей (необязательно ассоциативное), Q — квазигруппа. Рассмотрим квазигрупповое кольцо KQ, состоящее из всех формальных сумм вида

$$\sum_{q\in Q} \alpha_q \cdot q \quad (\alpha_q \in K),$$

в которых конечное число элементов α_q отлично от нуля. Предполагаем, что группы автоморфизмов $\operatorname{Aut} K$ кольца K и $\operatorname{Aut} Q$ квазигруппы Q некоммутативны, причём $|\operatorname{Aut} K| \geqslant t_1$, $|\operatorname{Aut} Q| \geqslant t_2$, где t_1 и t_2 — параметры безопасности. Также предполагаем, что в KQ достаточно элементов с нулевым левым аннулятором.

Для лучшего понимания предложен упрощённый вариант криптосхемы из [2].

Участник A:

1) конструирует автоморфизм $\sigma \in \operatorname{Aut} K$, порядок которого больше, чем t_3, $|\sigma| \geqslant t_3$, причём σ имеет нетривиальный централизатор $C(\sigma)$ в группе $\operatorname{Aut} K$ и $|C(\sigma) \setminus \langle\sigma\rangle| \geqslant t_4$, где t_3, t_4 — параметры безопасности;
2) конструирует автоморфизм $\eta \in \operatorname{Aut} Q$, порядок которого больше, чем t_5, $|\eta| \geqslant t_5$, причём η имеет нетривиальный централизатор $C(\eta)$ в группе $\operatorname{Aut} Q$ и $|C(\eta) \setminus \langle\eta\rangle| \geqslant t_6$, где t_5, t_6 — параметры безопасности;
3) случайно выбирает автоморфизмы $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$;
4) по τ и ω строит автоморфизм $\varphi \in \operatorname{Aut} KQ$ (назовём его *секретным автоморфизмом*) следующим образом: для любого $h \in KQ$ вида
$$h = a_{q_1} q_1 + \ldots + a_{q_n} q_n,$$
где $Q = \{q_1, \ldots, q_n\}$ — исходная квазигруппа, $a_{q_1}, \ldots, a_{q_n} \in K$, пусть
$$\varphi(h) = \tau(a_{q_1})\omega(q_1) + \ldots + \tau(a_{q_n})\omega(q_n);$$
5) выбирает элемент $x \in KQ$ и вычисляет $\varphi(x)$.

Открытым ключом участника A является $\big(\sigma, \eta, x, \varphi(x)\big)$.

Отметим, что при должных параметрах безопасности t_3, t_4, t_5, t_6 автоморфизмов, подходящих для открытого ключа, достаточно много. Сформированный открытый ключ участник A передаёт участнику B по открытому каналу.

Участник B:

1) выбирает натуральные числа (k, l);
2) используя открытый ключ участника A, получает пары автоморфизмов (σ^k, η^l) и по ним строит автоморфизм $\psi \in \operatorname{Aut} KQ$ таким же способом, как и участник A, т. е. для любого $h \in KL$ вида $h = a_{q_1} q_1 + \ldots + a_{q_n} q_n$ полагает
$$\psi(h) = \sigma^k(a_{q_1})\eta^l(q_1) + \ldots + \sigma^k(a_{q_n})\eta^l(q_n)$$
(автоморфизм ψ будем называть *сеансовым*);

3) вычисляет $\psi(x)$, $\psi\big(\varphi(x)\big)$ и левый аннулятор $\mathrm{Ann}\Big(\psi\big(\varphi(x)\big)\Big)$;
4) если полученный аннулятор $\mathrm{Ann}\Big(\psi\big(\varphi(x)\big)\Big)$ ненулевой, то производится новый сеанс связи с выбором нового элемента x или же выбираются другие сеансовые автоморфизмы;
5) записывает исходный текст, который надо передать, в виде $m \in KL$ и вычисляет $m \cdot \big[\psi\big(\varphi(x)\big)\big]$;
6) отправляет для A криптограмму

$$\big(\psi(x), m \cdot \big[\psi\big(\varphi(x)\big)\big]\big).$$

Получив криптограмму, участник A расшифровывает её:

1) используя секретный автоморфизм φ, вычисляет $\varphi\big(\psi(x)\big)$;
2) расшифровывает посланный текст, пользуясь тем, что ψ и φ коммутируют, поскольку сеансовый автоморфизм ψ построен на степенях выбранных автоморфизмов σ, η, а секретный автоморфизм φ построен с помощью элементов из централизаторов элементов σ, η. Участник A знает $m \cdot \big[\varphi\big(\psi(x)\big)\big] = h$ и $\varphi\big(\psi(x)\big) = r$, следовательно, для получения сообщения m достаточно решить линейную систему $m \cdot r = h$ с коэффициентами из кольца K.

Введём формальное определение гомоморфной системы шифрования из [8].

Гомоморфная система шифрования с открытым ключом E определяется четырьмя алгоритмами: KeyGen, Encrypt, Decrypt и Evaluate. Алгоритм KeyGen вырабатывает секретный ключ sk и открытый ключ pk, при этом задаётся множество открытых текстов M и зашифрованных текстов C. Алгоритм Encrypt принимает на вход открытый ключ pk и открытый текст m из M, на выходе выдаёт зашифрованный текст c из C. Алгоритм Decrypt принимает на вход sk и c, на выходе выдаёт открытый текст m. Алгоритм Evaluate принимает на вход открытый ключ pk, функцию F из множества возможных функций $\mathcal{F}$ и набор зашифрованных текстов $(c_1, c_2, \ldots, c_t)$, а на выходе выдаёт другой зашифрованный текст c.

Определение 1.1 (корректность шифрования). Система шифрования

$$E = (\mathrm{KeyGen}, \mathrm{Encrypt}, \mathrm{Decrypt}, \mathrm{Evaluate})$$

корректна для функций из множества $\mathcal{F}$, если для любой пары $(\mathrm{sk}, \mathrm{pk})$, любой функции F из $\mathcal{F}$, любых t открытых текстов $m_1, m_2, \ldots, m_t$ и соответствующих им зашифрованных текстов $c_i = \mathrm{Encrypt}_E(\mathrm{pk}, m_i)$ выполняется равенство

$$\mathrm{Decrypt}_E\Big(\mathrm{sk}, \mathrm{Evaluate}_E\big(\mathrm{pk}, F, (c_1, c_2, \ldots, c_t)\big)\Big) = F(m_1, m_2, \ldots, m_t).$$

Определение 1.2 (компактность шифрования). Гомоморфная система шифрования

$$E = (\mathrm{KeyGen}, \mathrm{Encrypt}, \mathrm{Decrypt}, \mathrm{Evaluate})$$

компактна, если существует полиномиальная функция g, такая что размер выхода алгоритма Decrypt не превосходит g[размер входа].

Определение 1.3 (полногомоморфное шифрование). Система шифрования E называется полногомоморфной, если она корректна и компактна для всех для функций из множества $\mathcal{F}$.

Проще говоря, гомоморфность системы означает выполнения условий

$$\mathrm{Decrypt}(c_1 \cdot c_2) = m_1 \cdot m_2, \quad \mathrm{Decrypt}(c_1 + c_2) = m_1 + m_2,$$

где c_1, c_2 — зашифрованные тексты соответствующих открытых текстов m_1, m_2, а операции $\cdot$ и $+$ — это операции в используемых алгебраических структурах.

В описанной выше схеме In the above system,

$$\mathrm{Decrypt}(c_1 \cdot c_2) = \mathrm{Decrypt}\big(\psi_1(x_1) \cdot \psi_2(x_2), \big[m_1 \cdot \psi_1\big(\varphi(x_1)\big)\big] \cdot \big[m_2 \cdot \psi_2\big(\varphi(x_2)\big)\big]\big).$$

При расшифровке при помощи секретного автоморфизма φ можно получить

$$\varphi\big(\psi_1(x_1) \cdot \psi_2(x_2)\big) = \psi_1\big(\varphi(x_1)\big) \cdot \psi_2\big(\varphi(x_2)\big) = h_1$$

для операции умножения и

$$\varphi\big(\psi_1(x_1) + \psi_2(x_2)\big) = \psi_1\big(\varphi(x_1)\big) + \psi_2\big(\varphi(x_2)\big) = h_2$$

для операции сложения. Таким образом, для того чтобы схема обладала свойством гомоморфной корректности шифрования по умножению, необходимо получить значение $m_1 \cdot m_2$ из системы

$$\begin{cases} (m_1 \cdot x) \cdot (m_2 \cdot y) = r_1, \\ x \cdot y = h_1 \end{cases}$$

при известных r_1 и h_1. Данная задача может быть разрешена, если в качестве квазигруппы Q в квазигрупповом кольце KQ использовать медиальные лупы.

Определение 1.4 (медиальные квазигруппы). Квазигруппа $(Q, \cdot)$ называется медиальной, если выполняется тождество

$$xy \cdot uv = xu \cdot yv.$$

В [1, 5, 10] показано, что каждую медиальную квазигруппу $(Q, \cdot)$ можно представить как изотоп абелевой группы $(Q, +)$:

$$x \cdot y = \chi(x) + \nu(y) + a,$$

где χ, ν — автоморфизмы абелевой группы $(Q, +)$, такие что $\chi\nu = \nu\chi$ и a — некоторый фиксированный элемент множества Q. Более того, верно и обратное утверждение: для каждой абелевой группы $(Q, +)$, двух автоморфизмов χ, ν группы $(Q, +)$, $\chi\nu = \nu\chi$, и a из Q существует медиальная квазигруппа $(Q, \cdot)$, причём $x \cdot y = \chi(x) + \nu(y) + a$.

Таким образом, можно строить различные примеры медиальных квазигрупп с заданными свойствами, используя изотопию абелевых групп.

В качестве рабочего примера алгебраической структуры для описанной выше схемы можно использовать кольцо Z_2Q, где в качестве Q выбрать следующую конструкцию: пусть $p > 2$ — простое число, $A, B \in F_p$, $q = p^k$,

в качестве абелевой группы используется группа $(E, \oplus)$ точек эллиптической кривой $y^2 = x^3 + Ax + B$, в качестве автоморфизмов группы используются χ, $\chi\big((x,y)\big) = (x^p, y^p)$ и $\nu = 1_E$.

Ещё более простым примером является следующая конструкция. Рассмотрим абелеву группу $(Z_p, \oplus)$ и построим медиальную квазигруппу $(Q, \cdot)$ с операцией $x \cdot y = x\alpha \oplus y\beta$, где α, β — это коммутативные автоморфизмы группы $(Z_p, \oplus)$. В качестве автоморфизмов можно выбрать $\alpha\colon z \to kz$, $\beta\colon z \to lz$, где k, l — целые числа.

Теорема 1.1. *Пусть $(KQ, +, \cdot)$ — квазигрупповое кольцо, где Q — медиальная квазигруппа и K — произвольное кольцо (необязательно ассоциативное). Тогда криптосхема является гомоморфной по операции умножения для кольца KQ.*

Доказательство. Корректность гомоморфного шифрования данной схемы отмечена выше. Пусть теперь функция F из алгоритма Evaluate осуществляет не одно умножение зашифрованных текстов, а несколько. На примере трёх умножений покажем, что криптосхема удовлетворяет определению компактности шифрования.

Пусть даны зашифрованные тексты

$$c_1 = [\psi_1(x_1), m_1 \cdot \psi_1\big(\varphi(x_1)\big)], \quad c_2 = [\psi_2(x_2), m_2 \cdot \psi_2\big(\varphi(x_2)\big)],$$
$$c_3 = [\psi_3(x_3), m_1 \cdot \psi_3\big(\varphi(x_3)\big)]$$

и функция $F(x,y,z) = x(yz)$. Тогда при расшифровке выполняется

$$\mathrm{Decrypt}\big(F(c_1, c_2, c_3)\big) = F(m_1, m_2, m_3).$$

Действительно, значение этой функции равно

$$F(c_1, c_2, c_3) = \\ = \Big[\psi_1(x_1)\big(\psi_2(x_2)\psi_3(x_3)\big), m_1\psi_1\big(\varphi(x_1)\big)\Big(m_2\psi_2\big(\varphi(x_2)\big) \cdot m_3\psi_3\big(\varphi(x_3)\big)\Big)\Big].$$

Используя медиальность квазигруппы, можно получить следующую цепочку равенств:

$$m_1\psi_1\big(\varphi(x_1)\big)\Big(m_2\psi_2\big(\varphi(x_2)\big) \cdot m_3\psi_3\big(\varphi(x_3)\big)\Big) = \\ = m_1\psi_1\big(\varphi(x_1)\big)\Big(m_2m_3 \cdot \psi_2\big(\varphi(x_2)\big)\psi_3\big(\varphi(x_3)\big)\Big) = \\ = m_1(m_2m_3) \cdot \psi_1\big(\varphi(x_1)\big)\Big(\psi_2\big(\varphi(x_2)\big)\psi_3\big(\varphi(x_3)\big)\Big).$$

Используя тот факт, что φ — автоморфизм кольца, получаем

$$m_1(m_2m_3) \cdot \psi_1\big(\varphi(x_1)\big)\Big(\psi_2\big(\varphi(x_2)\big)\psi_3\big(\varphi(x_3)\big)\Big) = \\ = m_1(m_2m_3) \cdot \varphi\big[\psi_1(x_1)\big(\psi_2(x_2)\psi_3(x_3)\big)\big].$$

Теперь при помощи секретного ключа φ можно определить значение

$$F(m_1, m_2, m_3) = m_1(m_2 m_3).$$

Данные рассуждения легко распространяются на любое количество умножений. Таким образом, можно сделать вывод, что криптосистема гомоморфна по умножению относительно введённых определений, т. е.

$$\begin{aligned}\mathrm{Decrypt}\big(\mathrm{sk}, F(c_1, c_2, \ldots, c_n)\big) &= \\ &= F\big(\mathrm{Decrypt}(\mathrm{sk}, c_1), \ldots, \mathrm{Decrypt}(\mathrm{sk}, c_n)\big) = F(m_1, \ldots, m_n). \quad \square\end{aligned}$$

2. Схема Эль-Гамаля для квазигрупп с перестановочными степенями

Классическая схема Эль-Гамаля — это криптосистема с открытым ключом, предложенная Т. Эль-Гамалем [7] в 1985 г. Стойкость схемы основана на решении задачи дискретного логарифмирования в циклической группе: найти x из уравнения $g^x = h$, где g, h — элементы циклической группы G, а x — натуральное число.

В [3] предлагается рассмотреть класс группоидов с перестановочными степенями для использования в системе выработки открытого ключа Диффи—Хеллмана.

Определение 2.1. Для элемента g группоида $(G, \star)$ и заданных натуральных чисел r, l правой r-й и левой l-й степенями называются элементы

$$g^{[r]} = \big(\ldots\big((g \star g) \star g\big)\ldots\big)$$

и

$${}^{[l]}g = \big(\ldots\big(g \star (g \star g)\big)\ldots\big).$$

Элемент g называется элементом с перестановочными правыми степенями, если для любых натуральных чисел m, n выполнено $g^{[m][n]} = g^{[n][m]}$. Если это тождество выполняется для всех элементов g из G, то группоид $(G, \star)$ называется группоидом с перестановочными правыми степенями.

Аналогично с использованием тождества ${}^{[m][n]}g = {}^{[n][m]}g$ для всех m, n определяются элементы и группоиды с перестановочными левыми степенями.

Определение 2.2. Группоид $(G, \star)$ называется группоидом с перестановочными степенями, если он является группоидом с перестановочными правыми степенями и группоидом с перестановочными левыми степенями.

Стоит отметить, что рассматриваются группоиды с условием $g^{[m][n]} \neq g^{[mn]}$.

Примером такого группоида может служить медиальная квазигруппа. Докажем некоторые нужные нам свойства для медиальных квазигрупп.

Лемма 2.1. *Пусть $(Q,\cdot)$ — медиальная квазигруппа, построенная на основе абелевой группы $(Q,+)$ и коммутирующих автоморфизмов σ, τ: $x\cdot y=\sigma(x)+$ $+\tau(y)$. Тогда для элемента q с перестановочными правыми степенями из заданной квазигруппы выполняется следующее свойство*:

$$\left(q^{[k]}\cdot q^{[l]}\right)^{[n]}=q^{[k][n]}\cdot q^{[l][n]}.$$

Доказательство. Можно заметить, что для элемента q квазигруппы $(Q,\cdot)$ выполнено равенство

$$q^{[k]}=\sigma^{k-1}(q)+\sigma^{k-2}\tau(q)+\ldots+\sigma\tau(q)+\tau(q).$$

Используя его, получаем

$$\left(q^{[k]}\right)^{[n]}=q^{[k][n]}=\sigma^{n-1}\left(q^{[k]}\right)+\sigma^{n-2}\tau\left(q^{[k]}\right)+\ldots+\sigma\tau\left(q^{[k]}\right)+\tau\left(q^{[k]}\right).$$

Тогда

$$q^{[k][n]}\cdot q^{[l][n]}=\sigma\left(q^{[k][n]}\right)+\tau\left(q^{[l][n]}\right).$$

Раскрыв скобки, получим, что

$$q^{[k][n]}\cdot q^{[l][n]}=\sigma^{n}\left(q^{[k]}\right)+\sigma^{n-1}\tau\left(q^{[k]}\right)+\ldots+\sigma\tau\left(q^{[k]}\right)+$$
$$+\sigma^{n-1}\tau\left(q^{[l]}\right)+\sigma^{n-2}\tau^{2}\left(q^{[l]}\right)+\ldots+\tau^{2}\left(q^{[l]}\right).$$

С другой стороны,

$$\left(q^{[k]}\cdot q^{[l]}\right)^{[n]}=\left(\sigma\left(q^{[k]}\right)+\tau\left(q^{[l]}\right)\right)^{[n]}=\sigma^{n-1}\left(\sigma\left(q^{[k]}\right)+\tau\left(q^{[l]}\right)\right)+$$
$$+\sigma^{n-2}\tau\left(\sigma\left(q^{[k]}\right)+\tau\left(q^{[l]}\right)\right)+\ldots+\sigma\tau\left(\sigma\left(q^{[k]}\right)+\tau\left(q^{[l]}\right)\right)+\tau\left(\sigma\left(q^{[k]}\right)+\tau\left(q^{[l]}\right)\right).$$

Заметим, что, переставляя слагаемые в абелевой группе $(Q,+)$, легко получить требуемое равенство. □

Построим аналог криптосхемы Эль-Гамаля для медиальной квазигруппы.

1. Алгоритм генерации ключей (KeyGen). Пусть $(Q,\cdot)$ — квазигруппа с перестановочными степенями, q — элемент квазигруппы, порождающий достаточно большую подквазигруппу. Участник A случайно выбирает натуральное число x и вычисляет $h=q^{[x]}$. Открытым ключом является (Q,q,h), а секретным x.
2. Алгоритм шифрования (Encrypt). Для шифрования сообщения m (элемента квазигруппы Q) участник B выполняет следующие действия:
   — случайно выбирает натуральное число y и вычисляет $v_1=q^{[y]}$;
   — вычисляет $s=h^{[y]}=q^{[x][y]}$ и $v_2=m\cdot s=m\cdot q^{[x][y]}$.

   Зашифрованным текстом является $(v_1,v_2)=\left(q^{[y]},m\cdot s\right)$.
3. Алгоритм расшифровки (Decrypt). Для расшифровки зашифрованного текста (v_1,v_2) при помощи секретного ключа участник A выполняет следующие действия:

— вычисляет $s = v_1^{[x]} = q^{[y][x]} = q^{[x][y]}$;
— решает уравнение в квазигруппе $v_2 = m \cdot s$ относительно m при известных v_2 и s.

Классическая схема Эль-Гамаля является гомоморфной по операции умножения. Криптосхема для медиальных квазигрупп также будет гомоморфной по квазигрупповой операции.

Теорема 2.1. *Пусть $(Q, \cdot)$ — медиальная квазигруппа. Тогда криптосистема Эль-Гамаля для квазигруппы Q является гомоморфной относительно квазигрупповой операции.*

Доказательство. Рассмотрим два зашифрованных текста для сообщений m_1, m_2: $c_1 = \mathrm{Encrypt}(h, m_1) = \left(q^{[y_1]}, m_1 \cdot h^{[y_1]}\right)$ и $c_2 = \mathrm{Encrypt}(h, m_2) = \left(q^{[y_2]}, m_2 \cdot h^{[y_2]}\right)$. Покажем корректность шифрования для этих зашифрованных текстов. Итак,

$$\mathrm{Decrypt}(x, c_1) \cdot \mathrm{Decrypt}(x, c_2) = \\ = \left(q^{[y_1]}, m_1 \cdot h^{[y_1]}\right) \cdot \left(q^{[y_2]}, m_2 \cdot h^{[y_2]}\right) = \Big(q^{[y_1]} \cdot q^{[y_2]}, \left(m_1 \cdot h^{[y_1]}\right)\left(m_2 \cdot h^{[y_2]}\right)\Big).$$

По условию медиальности квазигруппы выражение $\left(m_1 \cdot h^{[y_1]}\right)\left(m_2 \cdot h^{[y_2]}\right)$ можно преобразовать к виду $(m_1 \cdot m_2)\left(h^{[y_1]} \cdot h^{[y_2]}\right)$. Теперь для того, чтобы расшифровать, достаточно возвести в степень x значение $v_2' = q^{[y_1]} \cdot q^{[y_2]}$. Воспользовавшись доказанной леммой 2.1, получим

$$\left(q^{[y_1]} \cdot q^{[y_2]}\right)^{[x]} = q^{[y_1][x]} \cdot q^{[y_2][x]} = q^{[x][y_1]} \cdot q^{[x][y_2]} = h^{[y_1]} \cdot h^{[y_2]} = s'.$$

Наконец, вычислим значение $m' = (m_1 \cdot m_2)$ из уравнения $v_2' = m' \cdot s'$. Таким образом, выполняется следующее соотношение:

$$\mathrm{Decrypt}(x, c_1) \cdot \mathrm{Decrypt}(x, c_2) = \mathrm{Decrypt}(x, c_1 \cdot c_2).$$

Используя рассуждения для криптосистемы из первого раздела, можно показать, что гомоморфность также не зависит от количества используемых умножений. Таким образом,

$$\mathrm{Decrypt}\big(\mathrm{sk}, F(c_1, c_2, \ldots, c_n)\big) = \\ = F\big(\mathrm{Decrypt}(\mathrm{sk}, c_1), \ldots, \mathrm{Decrypt}(\mathrm{sk}, c_n)\big) = F(m_1, \ldots, m_n),$$

где $F \in \mathcal{F}$. □

Литература

[1] Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967.

[2] Грибов А. В., Золотых П. А., Михалёв А. В. Построение алгебраической криптосистемы над квазигрупповым кольцом // Матем. вопросы криптографии. — 2010. — Т. 4, № 4. — С. 23—33.

[3] Катышев С. Ю., Марков В. Т., Нечаев А. А. Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискрет. матем. — 2014. — Т. 26, № 3. — С. 45—64.

[4] Росошек С. К. Криптосистемы групповых колец // Вестн. Томск. гос. ун-та. — 2003. — № 6. — С. 57—62.

[5] Bruck R. A Survey of Binary Systems. — Berlin: Springer, 1958.

[6] Dijk M., Gentry C., Halevi S., Vaikuntanathan V. Fully homomorphic encryption over the integers // Advances in Cryptology — EUROCRYPT 2010. — Berlin: Springer, 2010. — (Lect. Notes Comput. Sci.; Vol. 6110). — P. 24—43.

[7] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms // IEEE Trans. Inform. Theory. — 1985. — Vol. 31, no. 4. — P. 469—472.

[8] Gentry C. A Fully Homomorphic Encryption Scheme: Ph.D. Thesis. — Stanford Univ., 2009.

[9] Smith J. D. H. Representation Theory of Infinite Groups and Finite Quasigroups. — Montreal: Univ. Montreal, 1986.

[10] Toyoda K. On axioms of linear functions // Proc. Imp. Acad. Tokyo. — 1941. — Vol. 17. — P. 221—227.