КІБЕРНЕТИКА

УДК 51.681.3

С.Л. КРИВИЙ
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *sl.krivoi@gmail.com.*

В.М. ОПАНАСЕНКО
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *opanasenkoincyb@gmail.com*.

О.О. ГРІНЕНКО
Київський національний авіаційний університет, Київ, Україна,
e-mail: *olena.hrinenko@npp.nau.edu.*

Ю.О. НОРТМАН
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *ynortman@gmail.com.*

СИМЕТРИЧНА СИСТЕМА ОБМІНУ ІНФОРМАЦІЄЮ НА ОСНОВІ ІЗОМОРФІЗМУ КІЛЕЦЬ

Анотація. Пропонуються алгоритми обміну повідомленнями між абонентами на основі властивостей скінченних асоціативно-комутативних кілець з одиницею та діофантових рівнянь над такими кільцями. Наведено алгоритми побудови скінченних кілець, адитивні групи яких повноциклічні, та алгоритми побудови ізоморфізму між кільцем k-го порядку, адитивна група якого повноциклічна, і кільцем лишків Z_k за модулем k.

Ключові слова: криптографічний протокол, ізоморфізм, кільце, алгоритм.

ВСТУП

У цій статті запропоновано алгоритми обміну повідомленнями між абонентами на основі властивостей асоціативно-комутативних кілець з одиницею та систем лінійних діофантових рівнянь над такими кільцями. Ця робота є продовженням робіт [1, 2].

НЕОБХІДНІ ОЗНАЧЕННЯ ТА ПОНЯТТЯ

Наведемо означення і поняття, які потрібні далі для викладу.

Означення 1. Універсальна алгебра $G(A,\Omega)$ називається кільцем, якщо вона є Абелевою групою стосовно додавання, групоїдом стосовно множення та для довільних її елементів $a, b, c \in A$ виконуються закони дистрибутивності:

$$a(b+c) = (ab) + (ac), \quad (a+b)c = (ac) + (bc).$$

Це означає, що Ω містить чотири операції: бінарні операції додавання і множення, унарну операцію взяття протилежного стосовно операції додавання і нульарну операцію, яка фіксує нульовий елемент Абелевої групи кільця. Нульовий елемент називається нулем кільця.

Означення 2. Кільце називається асоціативно-комутативним, якщо його операція множення асоціативна і комутативна, та називається кільцем з одиницею, коли воно має одиничний елемент стосовно операції множення.

Позначимо G_k скінченне асоціативно-комутативне кільце з одиницею k-го порядку. Елементи $a, b \in G_k \setminus \{0\}$ називають дільниками нуля, якщо $a \cdot b = 0$. Оскільки кільце G_k з одиницею, то можна розглядати елементи $c, d \in G_k$ як такі, що $c \cdot d = 1$. Ці елементи в кільці називаються дільниками одиниці. Відомо, що дільники нуля в асоціативно-комутативному кільці лишків утворюють ідеал, а дільники одиниці — Абелеву групу [3]. Ця група називається мультиплікативною групою асоціативно-комутативного кільця.

Розглянемо спосіб побудови таких кілець та їхні властивості.

Побудова скінченного кільця G_k виконується за заданим рядком додавання з одиницею, який називатимемо визначальним. За цим рядком за законами, яким задовольняють операції додавання і множення кільця, будуються таблиці операцій кільця. Покажемо такий процес побудови на прикладі кільця шостого порядку.

Приклад 1. Нехай задано визначальний рядок додавання з одиницею адитивної групи кільця G_6:

$$0+1=1,\ 1+1=3,\ 1+3=2,\ 1+2=4,\ 1+4=5,\ 1+5=0.$$

Розглянемо процес побудови кільця G_6. Роль одиничного елемента кільця відіграє одиниця. На підставі аксіом кільця маємо: $\forall a \in G_6\ \ a+0=0+a=a$, $a \cdot 1 = 1 \cdot a = a,\ \ a \cdot 0 = 0 \cdot a = 0$. Отже, два рядки і два стовпчики таблиці додавання (табл. 1) і таблиці множення (табл. 2) визначені.

Таблиця 1

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	3	4	2	5	0
2	2	4	0	5	1	3
3	3	2	5	4	0	1
4	4	5	1	0	3	2
5	5	0	3	1	2	4

Таблиця 2

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	2	0	0	2
3	0	3	0	4	3	4
4	0	4	0	3	4	3
5	0	5	2	4	3	1

Побудова таблиці додавання відбувається так: послідовно знаходимо результати додавання з елементом 3, оскільки 3=1+1, а з елементом 1 операція додавання вже визначена:

$$3+2 = (1+1)+2=1+(1+2)=1+4=5,\ \ 3+3=(1+1)+3=1+(1+3)=1+2=4,$$

$$3+4 = (1+1)+4=1+(1+4)=1+5=0,\ \ 3+5=(1+1)+5=1+(1+5)=1+0=1.$$

Далі знаходимо значення 3+1=2 і обчислюємо операцію додавання з елементом 2, оскільки результати додавання з елементами 3 і 1 визначені:

$$2+2 = (1+3)+2=1+(3+2)=1+5=0,\ \ 2+3=(1+3)+3=1+(3+3)=1+4=5,$$

$$2+4 = (1+3)+4=1+(3+4)=1+0=1,\ \ 2+5=(1+3)+5=1+(3+5)=1+1=3.$$

Далі знаходимо значення 2+1=4 і обчислюємо операцію додавання з елементом 4, потім аналогічно обчислюємо операцію додавання з елементом 4+1=5.

Оскільки 5+1=0, то процес побудови закінчується, тому що для нуля, як і для всіх інших елементів, результати операції додавання визначено. Заносимо ці значення в табл. 1 і закінчуємо побудову таблиці додавання адитивної групи кільця G_6.

Використовуючи таблицю додавання і закон дистрибутивності, будуємо таблицю операції множення (табл. 2). Дійсно, для елемента 3 знаходимо добутки:

$$3\cdot 2=(1+1)\cdot 2=2+2=0;\quad 3\cdot 3=(1+1)\cdot 3=3+3=4;$$

$$3\cdot 4=(1+1)\cdot 4=4+4=3;\quad 3\cdot 5=(1+1)\cdot 5=5+5=4.$$

Далі, оскільки 1+3=2, дістаємо

$$2\cdot 2=(1+3)\cdot 2=2+3\cdot 2=2+0=2;\ 2\cdot 3=(1+3)\cdot 3=3+3\cdot 3=3+4=0;$$

$$2\cdot 4=(1+3)\cdot 4=4+3\cdot 4=4+3=0;\ 2\cdot 5=(1+3)\cdot 5=5+3\cdot 5=5+4=2.$$

За таблицею додавання маємо 2+1=4, і це дає змогу знайти значення операції множення з елементом 4. Аналогічно знаходимо значення операції множення з елементом 5=1+4 і решту елементів табл. 2. Оскільки 5+1=0, то це означає, що вся таблиця множення побудована. Із симетричності таблиці випливає, що побудована множина елементів задовольняє закон комутативності. Крім того, легко перевірити, що елементи цієї множини задовольняють також закон асоціативності, тобто G_6 — асоціативно-комутативне кільце з одиницею шостого порядку.

Отже, в загальному випадку побудова таблиць операцій кільця G_k за рядком додавання з одиницею $a=(1,a_1,a_2,\dots,a_{n-2},0)$ виконується за підстановкою f (її нижній рядок):

$$f=\begin{pmatrix}0 & 1 & 2 & 3 & \dots & a_1 & \dots & k-1\\ 1 & a_1 & a_r & a_t & \dots & a_2 & \dots & a_m\end{pmatrix},$$

яка індукує бієкцію $f(0)=0+1=1,\ f(1)=1+1=a_1,\ f(a_s)=a_s+1=a_{s+1},$ $f(a_{k-1})=0.$

Означення 3. Скінченна група k-го порядку називається повноциклічною, якщо підстановка f є повним циклом довжини k.

З цього означення випливає очевидне твердження.

Твердження 1. Скінченні повноциклічні групи одного і того порядку ізоморфні.

Доведення випливає з того, що повноциклічна група є циклічною, а скінченні циклічні групи однакових порядків ізоморфні.

Початковий визначальний рядок додавання з одиницею генерується таким алгоритмом.

GEN-*G* (a,c,k)

Вхід. Порядок k і коефіцієнти виразу $f(i)=a\cdot i+c$ (вираз можна вибрати іншим способом [4]), де НСД$(a,k)=1$.

Вихід. Рядок таблиці додавання у вигляді одномірного масиву $b=(b_1,b_2,\dots,b_{k)}$ довжиною k.

Метод:

1) for $i=0$ to $k-1$ do $b_{i+1}:=a\cdot i+c\ (\mathrm{mod}\ k)$ od (*або довільним іншим алгоритмом, який задає визначальний рядок *);

2) for $i=1$ to k do

if $(b_i=0\wedge i\neq k)$ then change b_i and b_k;

if $(b_i=1\wedge i\neq 1)$ then change b_i and b_1;

od

(* визначили ізоморфізм $g(i)=b_i$, де $i=1,2,\dots,k^*$);

3) за масивом $b=(b_1,b_2,\dots,b_{k)}$ будуємо масив $P[1\times k]$ (де зберігається визначальний рядок)

$P[0]:=b_1$;

for $i=1$ to $k-1$ do $P[b_i]:=b_{i+1}$ od (* побудували визначальний рядок P *).

Коректність алгоритму випливає з того, що коли елемент i пробігає повну систему лишків, то $a \cdot i + c$ теж пробігає повну систему лишків за умови, що НСД$(a, k) = 1$ [4].

Часова складність алгоритму GEN-G має вигляд $O(k \log^2 k)$, оскільки множення цілих чисел має складність $O(\log^2 k)$, а кількість всіх таких множень не більше, ніж k.

Зазначимо, що алгоритм GEN-G згенерує не більше, ніж $(k-2)\,\varphi(k)$ різних визначальних рядків, де φ — функція Ойлера. Інші визначальні рядки можна будувати вже за домовленістю між абонентами шляхом застосування узодженої перестановки елементів у побудованому алгоритмом GEN-G визначальному рядку або генерувати їх застосуванням алгоритмів генерації підстановок [5, 6].

Приклад 2. Згенерувати визначальний рядок для $k = 6$ і $f(i) = 5 \cdot i + 4$.

Перший цикл алгоритму GEN-G генерує таку послідовність значень:

$$b_1 = 4;\ b_2 = 3;\ b_3 = 2;\ b_4 = 1;\ b_5 = 0;\ b_6 = 5.$$

Другий цикл розставляє все на свої місця:

$$b_1 = 1;\ b_2 = 3;\ b_3 = 2;\ b_4 = 4;\ b_5 = 5;\ b_6 = 0.$$

Третій цикл за масивом $b = (b_1 = 1;\ b_2 = 3;\ b_3 = 2;\ b_4 = 4;\ b_5 = 5;\ b_6 = 0)$ генерує визначальний рядок $P = (1, 3, 4, 2, 5, 0)$. За цим рядком побудовано наведені таблиці операцій кільця G_6 в прикладі 1.

Неважко переконатися в тому, що кільце G_k, адитивна група якого повноциклічна, ізоморфне кільцю лишків Z_k. Це випливає з того, що їхні адитивні групи повноциклічні, однакових порядків і ізоморфізм цих кілець є продовженням ізоморфізму їхніх адитивних груп. Такий ізоморфізм будується безпосередньо за рядком, який згенерований алгоритмом GEN-G, тобто генерація визначального рядка задає також і ізоморфізм між кільцями Z_k і G_k. Дійсно, маємо таку відповідність:

1	2	3	4	…	$k-1$	k
b_1	b_2	b_3	b_4	…	b_{k-1}	0

Тут ізоморфне відображення g має вигляд $g(k) = 0,\ g(1) = b_1 = 1,\ g(i) = b_i$, $i = 2, \ldots, k-1$. Наприклад, визначальний рядок, згенерований алгоритмом у прикладі 2, задає таке ізоморфне відображення: $g(6) = 0, g(1) = 1, g(2) = 3, g(3) = 4, g(4) = 2,\ g(5) = 5$.

ПРОТОКОЛ ОБМІНУ ПОВІДОМЛЕННЯМИ

Розглянемо протокол обміну повідомленнями між абонентами.

Попередньо Аліса і Боб закритим каналом обмінюються трійкою (a, c, k), елементи якої є параметрами алгоритму GEN-G. За допомогою виразу $f(i) = a \cdot i + c$ згенерували початкову підстановку і далі за домовленістю зафіксували деякий визначальний рядок $b = (b_1 = 1, b_2, \ldots, b_{k-1}, 0)$.

Далі Аліса і Боб виконують такі кроки.

Крок 1.

1. Аліса будує систему виразів

$$l(x) = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mq}x_q. \end{cases}$$

2. Вибирає вектори $a_1, a_2, \ldots, a_r, a_{r+1}$ і перетворює $l(x)$ в кільці G_k таким чином:

$$L(x) = B_r(B_{r-1}(\ldots B_2(B_1(l(x)+a_1)+a_2)+\ldots+a_{r-1})+a_r)+a_{r+1},$$

де B_i — невироджені матриці розміру $m \times m$, a_i — вектори розмірності $1 \times m$, $i = 1,2, \ldots, r+1$.

3. Аліса висилає Бобу відкритим каналом вирази $l(x)$ і $L(x)$.

Крок 2.

1. Боб вибирає два вектори $\bar{x}$ і $\bar{a}$ розмірності $1 \times q$.

2. Обчислює вектори значень $l(\bar{x}) = \upsilon$, $l(\bar{a}) = d$ та $L(\bar{x}+\bar{a}) = d_1$ за модулем k.

3. Значення υ, яке він хоче передати Алісі, зберігає в таємниці, а значення d і d_1 висилає Алісі відкритим каналом.

Крок 3.

1. Аліса обчислює обернені матриці до матриць B_i в кільці G_k.

2. Знаходить значення υ за значеннями векторів a_{r+1} і d, оскільки ці значення вона має.

Теорема 1. Обмін повідомленнями за протоколом виконується коректно.

Доведення випливає з властивостей лінійних операторів і лінійних функцій в кільці G_k. Дійсно, позначимо добуток матриць $B_r B_{r-1} \ldots B_1 = D$, тоді

$$d_1 = L((\bar{x}+\bar{a})+a_1) = D(l(\bar{x}+\bar{a})+a_1)+b+a_{r+1} = D(l(\bar{x}+\bar{a})+a_1)+c,$$

де $c = b + a_{r+1}$, а b — вектор значень, отриманий внаслідок множення матриць $B_1, B_2, \ldots, B_r$ на вектори $a_1, a_2, \ldots, a_r$. Отримуємо

$$D^{-1}(D(d_1 - a_{r+1})) - D^{-1}b = D^{-1}(D(l(\bar{x}+\bar{a})+a_1)+b) - D^{-1}b = l(\bar{x}+\bar{a})+a_1.$$

Отже, $l(\bar{x}+\bar{a})+a_1-[a_1+d] = l(\bar{x})$.

Розглянемо криптоаналіз протоколу. Очевидними кроками криптоаналітика є спроба розв'язати в кільці G_k систему лінійних рівнянь

$$l(\bar{a}) = d \tag{1}$$

з метою знаходження $\bar{a}$. Зауважимо, що для цього достатньо знайти довільний розв'язок цього рівняння в кільці G_k.

Далі за матрицями виразів $L(x)$ і $l(x)$ знайти матрицю D^{-1} і значення $L(\bar{a})$ та розв'язати в кільці G_k систему рівнянь

$$L(\bar{x}) = d_1 - L(\bar{a}), \tag{2}$$

звідки дістаємо значення $l(\bar{x})$ за допомогою матриці D^{-1}.

Описані дії криптоаналітика будуть успішними за умови, що йому відомі порядок кільця і ізоморфізм g: $G_k \to Z_k$ або таблиці операцій кільця G_k. Але жоден з цих об'єктів йому невідомий і тому він не може знайти розв'язки систем (1) і (2). Отже, стійкість запропонованого протоколу ґрунтується на ізоморфізмі g і порядку кільця k. Оскільки кількість способів вибору порядку кільця необмежена і ізоморфізмів між G_k і Z_k існує $(k-2)!$, то це гарантує необхідну стійкість запропонованого протоколу. Дійсно, якщо для кожного сеансу обміну повідомленнями змінювати визначальний рядок b кільця G_k та вектори $\bar{a}$ і a_{r+1}, змінюючи тим самим ізоморфізм, то протокол буде мати потрібну стійкість. До того ж для шифрування, завдяки необмеженій кількості способів вибору вектора $\bar{a}$, можна повністю приховати частоту входження символів у зашифрованому тексті.

Приклад 3. Нехай Аліса і Боб обмінялися трійкою (a, c, k) і зупинилися на визначальному рядку кільця G_{25}:

$$b = (1,6,8,10,2,4,3,5,7,9,11,13,15,17,19,21,12,14,16,18,20,24,22,23,0).$$

Другий цикл алгоритму GEN-G знаходить ізоморфне відображення $g\colon Z_{25} \to G_{25}$, яке в цьому випадку набуває вигляду:

$$\begin{array}{lllll} g(0)=0, & g(5)=2, & g(10)=9, & g(15)=19, & g(20)=18, \\ g(1)=1, & g(6)=4, & g(11)=11, & g(16)=21, & g(21)=20, \\ g(2)=6, & g(7)=3, & g(12)=13, & g(17)=12, & g(22)=24, \\ g(3)=8, & g(8)=5, & g(13)=15, & g(18)=14, & g(23)=22, \\ g(4)=10, & g(9)=7, & g(14)=17, & g(19)=16, & g(24)=23, \end{array}$$

де $g(25)=g(0)=0,\ g(1)=1,\ g(2)=g(1+1)=6,\ g(3)=6+1=8,\ g(4)=8+1=10,$ … , $g(24)=23.$

За цим ізоморфізмом третій цикл алгоритму GEN-G будує масив $P[1\times k]$ (для зручності читання він поданий нижнім рядком підстановки):

$$P=\left(\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|} \hline 0&1&2&3&4&5&6&7&8&9&10&11&12&13&14&15&16&17&18&19&20&21&22&23&24 \\ \hline 1&6&4&5&3&7&8&9&10&11&2&13&14&15&16&17&18&19&20&21&24&12&23&0&22 \\ \hline \end{array}\right).$$

За масивом P будуються таблиці операцій додавання і множення кільця G_{25} (алгоритми побудови таблиць операцій кільця G_k наведено в додатку, а для кільця G_{25} зображено і самі таблиці, згенеровані цими алгоритмами).

Крок 1. Нехай Аліса побудувала в кільці G_{25} вираз $l(x)$, який має вигляд

$$l(x)=\begin{cases} 2x_1 - 16x_2 + 7x_3 + 20x_4, \\ 0x_1 + 1x_2 - 17x_3 - 11x_4, \end{cases}$$

а еквівалентний йому вираз має вигляд

$$l'(x)=\begin{cases} 2x_1 + 4x_2 + 7x_3 + 20x_4, \\ 0x_1 + 1x_2 + 11x_3 + 17x_4, \end{cases}$$

де від'ємні коефіцієнти замінені своїми протилежними.

Аліса вибрала вектори $a_1=(1,2)^t$ і $a_2=(1,1)^t$ і перетворила $l(x)$ до вигляду

$$L(x)=B_1(l(x)+(1,2)^t)+(1,1)^t=\begin{cases} 9x_1 - 13x_2 + 10x_3 - 16x_4 + 5, \\ 18x_1 + 14x_2 - 18x_3 + 19x_4 + 18, \end{cases}$$

а еквівалентний йому вираз має вигляд

$$L'(x)=\begin{cases} 9x_1 + 15x_2 + 10x_3 + 4x_4 + 5, \\ 18x_1 + 14x_2 + 2x_3 + 19x_4 + 18, \end{cases}$$

де від'ємні коефіцієнти замінені своїми протилежними;

$$B_1=\left(\begin{array}{cc} 6 & 1 \\ 23 & 23 \end{array}\right).$$

(Можна спробувати знайти обернену матрицю в кільці G_{25}, коли ізоморфізм між Z_{25} і G_{25} невідомий.)

Аліса вислала Бобу вирази $l(x)$ і $L(x)$.

Крок 2. Боб вибирає вектори

$$\bar{x} = (0,0,13,0),\ \bar{a} = (0,1,0,1),$$

обчислює вектор $\bar{x} + \bar{a} = (0,1,13,1)$ і значення

$$l(\bar{x}) = (5,3) = v,\ \ l(\bar{a}) = (6,19) = d,\ \text{ і } L(\bar{x} + \bar{a}) = (0,15) = d_1.$$

Боб зберігає значення v в таємниці, а значення d і d_1 висилає Алісі.

Крок 3. Аліса виконує такі обчислення:

а) знаходить обернену матрицю B_1^{-1} до B_1 в кільці G_{25}:

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix};$$

б) обчислює $B_1^{-1}[(0,15) - (1,1)^t] = B_1^{-1}(23,13)$ і знаходить

$$B_1^{-1}(23,13)^t = (11,6) = l(\bar{x} + \bar{a}) + (1,2)^t = l(\bar{x}) + d + (1,2)^t;$$

в) обчислює значення

$$(11,6) - [(1,2) + (6,19)] = (11,6) + (24,2) = (5,3) = v.$$

З наведеного прикладу випливає, що в обчислювальному сенсі найскладнішим етапом є побудова обернених матриць в кільці G_k. Для того щоб спростити ці обчислення, можна скористатися ізоморфізмом між кільцями $g\colon G_k \to Z_k$ і виконати обчислення в кільці лишків Z_k. Коли обернені матриці будуть знайдені, то виконати зворотні підстановки і отримати відповідні матриці в кільці G_k.

Як зазначалося вище, мультиплікативна група дільників одиниці кільця G_k є Абелевою групою. Якщо така група циклічна, то в ній можна користуватися найбільш уживаною криптографічною функцією дискретного логарифма. Отже, виникає питання: за яких умов група дільників одиниці кільця G_k буде циклічною? Відповідь на це питання дає така теорема.

Теорема 2. Мультиплікативна група кільця Z_k буде циклічною тоді і тільки тоді, коли k дорівнюватиме 2, 4, p^m або $2p^m$, де $m \geq 1$, p — непарне просте число [3].

З цієї теореми випливає, що мультиплікативна група побудованого в прикладі 3 кільця G_{25}, яке ізоморфне кільцю Z_{25}, буде циклічною, оскільки $k = 25 = 5^2$ задовольняє умови теореми 2. Зокрема, мультиплікативна група кільця G_{25} матиме $\varphi(5^2) = 20$ елементів і вісім породжувальних елементів, оскільки $\varphi(20) = 8$. Отже, в таких кільцях можна використовувати функцію дискретного логарифма.

ФОРМУВАННЯ ПОВІДОМЛЕННЯ

Розглянемо питання: яким чином формуються параметри протоколу та повідомлення, яке потрібно передати. Зі сказаного вище випливає, що Аліса і Боб повинні мати алгоритми побудови визначального рядка кільця, який задає ізоморфізм. Для цього вони повинні обмінятися закритим каналом трійкою чисел (a, c, k), де a, c, k — параметри алгоритму GEN-G.

З наведеного протоколу і прикладів випливає, що для передачі потрібного повідомлення $b = (b_1, b_2, \ldots, b_m)$ необхідно, щоб система рівнянь

$$l(x)=\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1q}x_q=b_1,\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2q}x_q=b_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{m1}x_1+a_{m2}x_2+\ldots+a_{mq}x_q=b_m \end{cases} \tag{3}$$

мала розв'язок. Розв'язання такої системи зводиться до розв'язання системи однорідних рівнянь вигляду

$$l(x)=\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1q}x_q-b_1x_0=0,\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2q}x_q-b_2x_0=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ a_{m1}x_1+a_{m2}x_2+\ldots+a_{mq}x_q-b_mx_0=0, \end{cases} \tag{4}$$

де x_0 — додаткова невідома.

Серед розв'язків системи (4) потрібно знайти розв'язок, у якого остання координата, що відповідає додатковій невідомій, дорівнює одиниці. Відкидаючи в цьому розв'язку останню координату, дістаємо окремий розв'язок системи (3).

Отже, потрібно сформулювати умови, за яких така система буде сумісною. Із властивостей дільників нуля і дільників одиниці примарного кільця та *TSS*-алгоритму [7, 8] отримуємо таке твердження.

Твердження 2. 1. Якщо всі коефіцієнти системи (3) і її вільні члени є дільниками нуля, то система не має розв'язку в кільці G_k.

2. Якщо серед розв'язків системи (4) існує хоча б один розв'язок, у якого остання координата є дільником одиниці, то система має розв'язок в кільці G_k.

Доведення. Пункт 1 випливає з того, що в процесі роботи *TSS*-алгоритму виконуються додавання і множення елементів. На підставі того, що дільники нуля в кільці утворюють ідеал, то в отриманих розв'язках системи (4) остання координата, яка відповідає вільним членам, буде дільником нуля і не матиме оберненого елемента. Тому отримати значення останньої координати, яке дорівнює одиниці, неможливо.

Доведення п. 2 випливає з того, що маючи розв'язок b системи (4), у якого остання координата c є дільником одиниці, будуємо розв'язок $c^{-1}(b)$, який буде окремим розв'язком системи (3).■

З цього твердження випливає, що в процесі застосування *TSS*-алгоритму слід вибирати для комбінування дільники одиниці. Якщо таких дільників на деякому кроці роботи алгоритму немає, то система буде несумісною. Якщо потрібно мати гарантію існування розв'язку системи (3), то слід будувати поле k-го порядку (тобто вибирати порядок кільця k простим числом), оскільки в цьому випадку система (3) буде завжди сумісною за умови лінійної незалежності її рівнянь [7, 9]. У застосуваннях простіше побудувати систему з лінійно незалежними рівняннями, ніж шукати підбір коефіцієнтів системи для забезпечення її сумісності.

Приклад 4. Нехай в табл. 3 літери алфавіту англійської мови перенумеровані природним чином.

Таблиця 3

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
a	b	c	d	e	f	g	h	i/j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

До того ж Аліса і Боб домовилися працювати в кільці G_{25}, яке було побудоване вище, і Аліса вибрала вектори $a_1=(1,2)^t$, $a_2=(1,1)^t$ та побудувала вирази, які наведено в прикладі 3.

Припустимо, що Боб хоче передати Алісі повідомлення *meet me in twelve* і він виконує такі обчислення.

1. Розбиває повідомлення на блоки, кожен з яких має два символи, цифровими відповідниками блоків є пари чисел із табл. 3:

$$\begin{array}{cccccccc} \text{me} & \text{et} & \text{me} & \text{in} & \text{tw} & \text{el} & \text{ve} \\ 11,4 & 4,18 & 11,4 & 8,12 & 18,21 & 4,10 & 20,4. \end{array}$$

2. Розв'язує систему рівнянь

$$l(x) = \begin{cases} 2x_1 + 4x_2 + 7x_3 + 20x_4 = 11, \\ 0x_1 + 1x_2 + 11x_3 + 17x_4 = 4 \end{cases}$$

і знаходить розв'язок $\bar{x} = (0,4,0,0)$. Значення $v_1 = (11,4)$ він тримає в секреті.

3. Вибирає вектор $\bar{a}_1 = (0,1,0,1)$, обчислює значення $d = l(\bar{a}_1) = (6,19)$ і до розв'язку цієї системи $\bar{x} = (0,4,0,0)$ додає вектор $\bar{a}_1 = (0,1,0,1)$. Цю суму векторів $\bar{x} + \bar{a}_1 = (0,3,0,1)$ він підставляє в $L(x)$, знаходячи тим самим значення $d_1 = (2,11)$. Значення d і d_1 Боб передає Алісі.

Аліса, отримавши значення d, d_1, виконує такі обчислення:

а) знаходить обернену матрицю B_1^{-1} в кільці G_{25}:

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix};$$

б) обчислює $B_1^{-1}[d_1^t - (1,1)^t] = B_1^{-1}[(2,11)^t - (1,1)^t] = B_1^{-1}(10,9)^t$ і знаходить

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix}(10,9)^t = (17,1) = l(\bar{x} + \bar{a}_1) + (1,2)^t;$$

в) обчислює значення

$$(17,1) - [(1,2) + l(\bar{a}_1)] = (17,1) - [(1,2) + (6,19)] = (17,1) + (24,2) = (11,4) = v_1.$$

Далі Боб виконує такі обчислення:

а) розв'язує систему рівнянь (яка була наведена в прикладі 3, крок 1):

$$l'(x) = \begin{cases} 2x_1 + 4x_2 + 7x_3 + 20x_4 = 4, \\ 0x_1 + 1x_2 + 11x_3 + 17x_4 = 18, \end{cases}$$

значення $v_2 = (4,18)$ він тримає в секреті;

б) обчислює значення $d = l(\bar{a}_1) = (6,19)$, до розв'язку цієї системи $\bar{x} = (0,22,6,0)$ додає вектор $\bar{a}_1 = (0,1,0,1)$ і цю суму векторів $\bar{x} + \bar{a}_1 = (0,23,6,1)$ підставляє в $L(x)$, знаходячи тим самим значення $d_1 = (7,6)$;

в) значення d і d_1 Боб передає Алісі.

Аліса, отримавши значення d, d_1, виконує такі обчислення:

а) знаходить обернену матрицю B_1^{-1} (у цьому випадку немає потреби, оскільки матриця не змінювалася) в кільці G_{25}:

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix};$$

б) обчислює $B_1^{-1}[d_1^t - (1,1)^t] = B_1^{-1}[(7,6)^t - (1,1)^t = B_1^{-1}(5,1)^t$ і знаходить

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix}(5,1)^t = (7,19) = l(\bar{x} + \bar{a}_1) + (1,2)^t;$$

в) обчислює значення

$$(7,19) - [(1,2) + l(\bar{a}_1)] = (7,19) - [(1,2) + (6,19)] = (7,19) + (24,2) = (4,18) = v_2.$$

Оскільки наступний блок $v_3 = (11,4)$ такий самий, як і перший, то це змушує Боба вибрати новий вектор $\bar{a}_2 = (0,0,1,1)$, за яким він обчислює значення

$$d = l(\bar{a}_2) = (2,0), \quad \bar{x} + \bar{a}_2 = (0,4,1,1), \quad d_1 = L(\bar{x} + \bar{a}_2) = (18,24)$$

і висилає Алісі значення $d = (2,0)$, $d_1 = (20,22)$.

Аліса обчислює значення

$$B_1^{-1}[d_1^t - (1,1)^t] = B_1^{-1}[(20,22)^t - (1,1)^t] = (12,11) = l(\bar{x} + \bar{a}_2) + (1,2)^t$$

і знаходить

$$l(\bar{x} + \bar{a}_2) - [(1,2) + (2,0)] = (12,11) - (4,2) = (12,11) + (16,18) = (11,4) = v_3 .$$

Цю процедуру Боб і Аліса повторюють стільки разів, скільки блоків у повідомленні (у цьому випадку ще чотири рази). У такий спосіб Аліса отримує повідомлення

11,4	4,18	11,4	8,12	18,21	4,10	20,4
me	et	me	in	tw	el	ve

.

У цьому прикладі використовувалося одне і те самє кільце, але можна для кожного сеансу передачі або з певним періодом між передачами змінювати кільце. Можна також змінювати вектори a_1 і $\bar{a}$, які змінюють значення $l(\bar{a})$ і $L(\bar{x} + \bar{a})$.

Наведений протокол можна зробити складнішим, якщо використовувати для шифрування кожного блоку різні кільця або різні значення параметрів — матриць і векторів.

Очевидним недоліком цього протоколу є те, що довжина шифрованого повідомлення в два рази довша, ніж саме повідомлення.

ОБЧИСЛЮВАЛЬНІ ОСОБЛИВОСТІ

Виходячи з того, що процес обчислення в кільці G_k не є звичним, то покращити ефективність шифрування і розшифрування можна, якщо знову скористатися ізоморфізмом між кільцями G_k і Z_k. Дійсно, пошук протилежного елемента до елемента a в кільці Z_k зводиться до обчислення різниці $k - a$, а обчислення оберненого елемента до a виконується шляхом застосування розширеного алгоритма Евкліда для розв'язання рівняння $ax + ky = 1$ (розширений алгоритм Евкліда обчислює розклад $ax + by = d$, де $d = \text{НСД}(a, b)$). За результатом виконання цього алгоритму маємо $x = a^{-1}$.

Використовуючи ізоморфізм g з прикладу 3, система рівнянь з прикладу 4 в кільці Z_{25} набуває вигляду

$$\overline{l(x)} = \begin{cases} 5x_1 + 6x_2 + 9x_3 + 21x_4 = 11, \\ 0x_1 + 1x_2 + 11x_3 + 14x_4 = 6. \end{cases}$$

Розв'язком цієї системи є вектор $x = (0,6,0,0)$, якому відповідає розв'язок $\bar{x} = (0,4,0,0)$ системи

$$l'(x) = \begin{cases} 2x_1 + 4x_2 + 7x_3 + 20x_4 = 11, \\ 0x_1 + 1x_2 + 11x_3 + 17x_4 = 4. \end{cases}$$

В кільці Z_{25} матриці

$$B_1 = \begin{pmatrix} 6 & 1 \\ 23 & 23 \end{pmatrix}$$

відповідає матриця

$\bar{B}_1 = \begin{pmatrix} 2 & 1 \\ 24 & 24 \end{pmatrix}$ або $\bar{B}_1 = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$, обернена до якої є $\bar{B}_1^{-1} = \begin{pmatrix} 1 & 1 \\ -1 & -2 \end{pmatrix}$.

Оскільки вектору $d_1 = (10,9)$ кільця G_{25} відповідає вектор $\overline{L}(x+a) = (4,10)$ кільця Z_{25}, то $\overline{B}_1^{-1}(4,10)^t = (14,1)$. Далі вектору (1, 2) кільця G_{25} відповідає вектор (1, 5) кільця Z_{25}, а вектору (6,19) кільця G_{25} відповідає вектор (2,15) кільця Z_{25}. Звідси дістаємо вектор $(14,1) - (1,5) - (2,15) = (11,6)$ в кільці Z_{25}, якому відповідає вектор $l(\overline{x}) = (11,4)$ в кільці G_{25}. Отже, всі обчислення можна виконувати в кільці лишків Z_{25}, а далі, використовуючи обернений ізоморфізм, знаходити відповідні значення в кільці G_{25}. Саме таким способом виконувалися обчислення в наведених прикладах.

ВИСНОВКИ

Підводячи підсумки, зазначимо, що використання діофантових рівнянь у криптографічних системах є відомими [10]. Криптографічний протокол, який грунтується на властивостях лінійних діофантових рівнянь над множиною цілих чисел, описаний у роботі [11]. Криптографічна стійкість цього протоколу є недостатньою. Стійкіший протокол, що грунтується на поліноміальних діофантових рівняннях над множиною цілих чисел, представлений у роботі [12].

Підхід, розглянутий в цій статті, планується розширити на область прямих добутків скінченних кілець і полів. Наприклад, якщо $G = G_{k_1} \times G_{k_2} \times G_{k_3}$, то в одному з цих кілець виконувати обмін ключами, в другому — шифрування, а в третьому буде виконуватися обмін додатковою інформацією.

СПИСОК ЛІТЕРАТУРИ

1. Кривий С.Л. Криптосистема на основі абелевих груп і кілець. *Проблеми програмування.* 2020. № 2–3. С. 270–277.
2. Кривий С.Л. Застосування комутативних кілець з одиницею для побудови системи симетричного шифрування. *Кібернетика та системний аналіз*. 2022. Т. 58, № 3. Р. 3–16.
3. Кострикин А.И. Введение в алгебру. Москва: Наука, 1977. 495 с.
4. Бухштаб А.А. Теория чисел. Москва: Просвещение, 1966. 384 с.
5. Липский В. Комбинаторика для программистов. Москва: Мир, 1988. 201 с.
6. Коблиц Н. Курс теории чисел и криптографии. Москва: Научное издательство ТВП, 2001. 260 с.
7. Kryvyi S.L. Algorithms for solution of systems of linear Diophantine equations in residues fieds. *Cybernetics and Systems Analysis.* 2007. N 2. P. 171–178.
8. Kryvyi S.L. Algorithms for solving systems of linear Diophantine equations in residues rings. *Cybernetics and Systems Analysis.* 2007. N 6. C. 787–798.
9. Opanasenko V.N., Kryvyi S.L. Synthesis of neural-like networks on the basis of conversion of cyclic Hamming codes. *Cybernetics and Systems Analysis.* 2017. Vol. 53, N. 4. P. 627–635.
10. Венбо Мао. Современная криптография. Санкт-Петербург: Изд. дом «Вильямс», 2005. 763 с.
11. Kameswari P.A., Sriniasarao S.S., Belay A. An application of linear Diophantine equations to cryptography. *Advanced in Mathematics: Scientific Journal.* 2021. Vol. 10. P. 2799–2806.
12. Berczes A., Lajos H., Hirete-Kohno N., Kovacs T. A key exchange propocol based on Diophantine equations and *S*-integers. *JSIAM Letters*, 2014. P. 85–88.

ДОДАТОК

Алгоритми побудови таблиць операцій

Наведені нижче алгоритми побудови таблиць операцій кільця G_k мають складність $O(k^2 \log k)$ і $O(k^2 \log^2 k)$ відповідно за такими алгоритмами [5].

ADD-TAB $G(1,k)$:

0) задекларувати масив $T_+[k \times k]$;
1) занести в T_+ в перший рядок результати додавання з нулем;
2) занести в T_+ в другий рядок результати додавання з 1;
3) покласти $c = 1$;
4) взяти в T_+ елемент $c' = c + 1$;
5) для всіх $x \in G_k$ занести в T_+ в рядок з номером c' суми $c' + x$;
6) покласти $c = c'$; $c' = c + 1$; якщо $c' = 0$, то СТОП, інакше на крок 5).

MUL-TAB $G(1,k)$:

0) задекларувати масив $T_\times[k \times k]$;
1) занести в $T_\times$ в рядки з номерами 0 і 1 результати множення на 0 і на 1;
2) покласти $c = 1$;
3) взяти в T_+ елемент $c' = c + 1$;
4) для всіх $x \in G_k$ занести в $T_\times$ в рядок з номером c' добутки $c' \cdot x$;
5) покласти $c = c'$; $c' = c + 1$; якщо $c' = 0$, то СТОП, інакше на крок 4).

ТАБЛИЦІ ОПЕРАЦІЙ КІЛЬЦЯ G_{25}, ПОБУДОВАНІ НАВЕДЕНИМИ АЛГОРИТМАМИ

Таблиця додавання кільця G_{25}

⊕	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1	6	4	5	3	7	8	9	10	11	2	13	14	15	16	17	18	19	20	21	24	12	23	0	22
2	2	4	9	13	11	15	3	17	5	19	7	21	24	12	22	14	23	16	0	18	1	20	8	10	6
3	3	5	13	17	15	19	7	21	9	12	11	14	23	16	0	18	1	20	6	24	8	22	2	4	10
4	4	3	11	15	13	17	5	19	7	21	9	12	22	14	23	16	0	18	1	20	6	24	10	2	8
5	5	7	15	19	17	21	9	12	11	14	13	16	0	18	1	20	6	24	8	22	10	23	4	3	2
6	6	8	3	7	5	9	10	11	2	13	4	15	16	17	18	19	20	21	24	12	22	14	0	1	23
7	7	9	17	21	19	12	11	14	13	16	15	18	1	20	6	24	8	22	10	23	2	0	3	5	4
8	8	10	5	9	7	11	2	13	4	15	3	17	18	19	20	21	24	12	22	14	23	16	1	6	0
9	9	11	19	12	21	14	13	16	15	18	17	20	6	24	8	22	10	23	2	0	4	1	5	7	3
10	10	2	7	11	9	13	4	15	3	17	5	19	20	21	24	12	22	14	23	16	0	18	6	8	1
11	11	13	21	14	12	16	15	18	17	20	19	24	8	22	10	23	2	0	4	1	3	6	7	9	5
12	12	14	24	23	22	0	16	1	18	6	20	8	7	10	9	2	11	4	13	3	15	5	19	21	17
13	13	15	12	16	14	18	17	20	19	24	21	22	10	23	2	0	4	1	3	6	5	8	9	11	7
14	14	16	22	0	23	1	18	6	20	8	24	10	9	2	11	4	13	3	15	5	17	7	21	12	19
15	15	17	14	18	16	20	19	24	21	22	12	23	2	0	4	1	3	6	5	8	7	10	11	13	9
16	16	18	23	1	0	6	20	8	24	10	22	2	11	4	13	3	15	5	17	7	19	9	12	14	21
17	17	19	16	20	18	24	21	22	12	23	14	0	4	1	3	6	5	8	7	10	9	2	13	15	11
18	18	20	0	6	1	8	24	10	22	2	23	4	13	3	15	5	17	7	19	9	21	11	14	16	12
19	19	21	18	24	20	22	12	23	14	0	16	1	3	6	5	8	7	10	9	2	11	4	15	17	13
20	20	24	1	8	6	10	22	2	23	4	0	3	15	5	17	7	19	9	21	11	12	13	16	18	14
21	21	12	20	22	24	23	14	0	16	1	18	6	5	8	7	10	9	2	11	4	13	3	17	19	15
22	22	23	8	2	10	4	0	3	1	5	6	7	19	9	21	11	12	13	14	15	16	17	20	24	18
23	23	0	10	4	2	3	1	5	6	7	8	9	21	11	12	13	14	16	15	17	18	19	24	22	20
24	24	22	6	10	8	2	23	4	0	3	1	5	17	7	19	9	21	11	12	13	14	15	18	20	16

Таблиця множення кільця G_{25}

.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	0	2	0	9	2	19	9	18	19	0	18	2	9	9	19	19	18	18	0	0	2	2	19	18	9
3	0	3	9	23	12	4	17	15	20	18	8	6	16	7	1	21	5	22	19	2	24	13	11	14	10
4	0	4	2	12	11	22	13	10	14	9	23	21	6	24	5	8	17	7	18	19	1	20	15	16	3
5	0	5	19	4	22	17	21	24	23	2	3	15	11	20	16	10	6	13	9	18	14	8	7	12	1
6	0	6	9	17	13	21	10	14	4	18	5	24	7	23	11	1	15	8	19	2	12	3	20	22	16
7	0	7	18	15	10	24	14	4	6	19	11	23	8	5	13	12	20	1	2	9	17	16	3	21	22
8	0	8	19	20	14	23	4	6	7	2	13	5	1	11	10	17	3	12	9	18	15	22	16	24	21
9	0	9	0	18	9	2	18	19	2	0	19	9	18	18	2	2	19	19	0	0	9	9	2	19	18
10	0	10	18	8	23	3	5	11	13	19	21	16	14	22	24	6	1	4	2	9	7	17	12	20	15
11	0	11	2	6	21	15	24	23	5	9	16	20	13	3	22	14	7	10	18	19	4	1	8	17	12
12	0	12	9	16	6	11	7	8	1	18	14	13	17	10	4	20	22	15	19	2	3	24	21	5	23
13	0	13	9	7	24	20	23	5	11	18	22	3	10	16	21	4	8	14	19	2	6	12	1	15	17
14	0	14	19	1	5	16	11	13	10	2	24	22	4	21	23	7	12	6	9	18	8	15	17	3	20
15	0	15	19	21	8	10	1	12	17	2	6	14	20	4	7	16	24	3	9	18	22	5	23	13	11
16	0	16	18	5	17	6	15	20	3	19	1	7	22	8	12	24	11	21	2	9	23	10	13	4	14
17	0	17	18	22	7	13	8	1	12	19	4	10	15	14	6	3	21	20	2	9	16	23	24	11	5
18	0	18	0	19	18	9	19	2	9	0	2	18	19	19	9	9	2	2	0	0	18	18	9	2	19
19	0	19	0	2	19	18	2	9	18	0	9	19	2	2	18	18	9	9	0	0	19	19	18	9	2
20	0	20	2	24	1	14	12	17	15	9	7	4	3	6	8	22	23	16	18	19	21	11	5	10	13
21	0	21	2	13	20	8	3	16	22	9	17	1	24	12	15	5	10	23	18	19	11	4	14	7	6
22	0	22	19	11	15	7	20	3	16	2	12	8	21	1	17	23	13	24	9	18	5	14	10	6	4
23	0	23	18	14	16	12	22	21	24	19	20	17	5	15	3	13	4	11	2	9	10	7	6	1	8
24	0	24	9	10	3	1	16	22	21	18	15	12	23	17	20	11	14	5	19	2	13	6	4	8	7

S.L. Kryvyi, V.N. Opanasenko, E.A. Grinenko, Yu.A. Nortman

SYMMETRIC INFORMATION EXCHANGE SYSTEM BASED ON RING ISOMORPHISM

Abstract. The algorithms for exchange of information between subscribers on the basis of finite associative-commutative rings with unity and linear Diophantine equations over such rings are proposed. Algorithms for construction of finite rings whose additive groups are full-cycle, and algorithms for construction of the izomorphism between a ring of k-th order whose additive group is full-cycle and the residue ring Z_k modulo k are presented.

Keywords: cryptographical protocol, izomorphism, ring, algorithm.

Надійшла до редакції 15.05.2022