СИСТЕМА ОБМІНУ ІНФОРМАЦІЄЮ НА ОСНОВІ ВІДОБРАЖЕНЬ КІЛЕЦЬ

Кривий С.Л., Нортман Ю.О.

Abstract. Пропонуються алгоритми обміну повідомленнями між абонентами на основі сюр'єктивних відображень скінченних асоціативно-комутативних кілець з одиницею та систем лінійних рівнянь над такими кільцями. Наводяться алгоритми побудови скінченних кілець, побудова сюр'єктивних відображень кілець, а також протокол обміну інформацією та обчислювальні особливості засобів реалізації протоколу. Основною мотивацією розробки такої криптосистеми є те, що практично всі існуючі криптосистеми потребують обчислення або великих простих чисел, або побудови скінченних полів великих порядків. А такі обчислення та побудови потребують застосування досить складних алгоритмів. Пропонована система не потребує громіздких обчислень, не потребує побудови таблиць операцій кілець і її стійкість ґрунтується на комбінаторній складності множини сюр'єктивних відображень та ізоморфізмів між скінченними кільцями відносно невеликих порядків. Алгоритми розв'язання систем лінійних рівнянь, які фігурують в протоколі обміну інфоомацією, над такими кільцями мають поліноміальну складність. Робота криптосистеми демонструється на прикладах.

1 Вступ

В криптографічних застосуваннях найчастіше використовуються скінченні поля і Діофантові рівняння та системи таких рівнянь [1, 2]. Це пояснюється тим, що скінченне поле має циклічни мултиплікативну групу і в такій групі ефективне використання функції дискретного логарифму, а алгоритми розв'язання Діофантових рівнянь та систем таких рівнянь мають велику часову складність [3]. Криптосистеми, побудовані на таких структурах потребують побудови великих простих чисел, або полів великих порядків, або великих об'ємів пам'яті та часових затрат на підготовчі дії [4].

Основна ідея даної роботи полягає в тому, щоб створити достатньо надійну криптосистему, в якій фігурують об'єкти відносно невеликих розмірів, але які мають необхідний запас надійності. Такого типу система була запропонована в роботі [5] і дана робота є подальшим її розвитком. Основою криптосистеми є сюр'єктивні відображення скінченних кілець та їх ізоморфізми з використанням систем лінійних рівнянь над кільцями лишків. Надійність такої системи грунтується на комбінаторній складності множини відображень між кільцями, порядки яких відносно невеликі.

Системи лінійних рівнянь над такими кільцями використовуються для формування і шифрування повідомлення, що дає можливість практично повністю унеможливити застосування методу частотного аналізу та гамування.

2 Необхідні означення та поняття

Алгебра $G(A, \Omega)$ називається **кільцем**, якщо вона абелева група відносно додавання, групоїд відносно операції множення і для довільних її елементів $a, b, c \in A$

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

Нульовий елемент адитивної групи кільця називається **нулем** кільця.

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

Кількість елементів кільця називається порядком кільця. Будемо позначати скінченне асоціативно-комутативне кільце з одиницею k-го порядку G_k. Елементи $a, b \in G_k \setminus \{0\}$ називаються *дільниками нуля*, якщо $a \cdot b = 0$. Оскільки кільце G_k з одиницею, то елементи $c, d \in G_k$ такі, що $c \cdot d = 1$, називають *дільниками одиниці*. Відомо, що дільники одиниці в асоціативно-комутативному кільці утворюють абелеву групу [6].

Множення у кільці G_k виконується за правилом множення слів у напівгрупі, а сама напівгрупа називається *мультиплікативною напівгрупою* асоціативного кільця.

Побудова скінченного кільця G_k виконується за заданим рядком додавання з одиницею, який будемо називати *визначальним*. За цим рядком на підставі законів, яким задовольняють операції додавання і множення кільця, при потребі можна побудувати таблиці операцій кільця (алгоритми побудови таблиць кільця G_k можна занйти в [5]). Визначальний рядок визначає також ізоморфізм між кільцем лишків Z_k за модулем k і кільцем G_k. Цей ізоморфізм дає можливість уникнути побудови таблиць операцій кільця G_k, тому що операції можна виконувати в кільці Z_k і за ізоморфізмом знаходити результати операцій в кільці G_k, а в кільці Z_k операції виконуються ефективніше.

В загальному випадку визначальний рядок кільця G_k $a = (1, a_1, a_2, \ldots, a_{n-2}, 0)$ задається такою підстановкою (а точніше, її нижнім рядком):

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

Означення 1. *Скінченна група k-го порядку називається повноциклічною, якщо підстановка f є повним циклом довжини k.*

З цього означення випливає що скінченні повноциклічні групи одного і того порядку ізоморфні між собою, оскільки повноциклічна група циклічна, 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 $f(i) = a \cdot i + c$, де НСД(a, k)=1.

Вихід: Рядок таблиці додавання з одиницею у вигляді одномірного масиву $b = (b_1, b_2, \ldots, b_k)$ довжини k.

Метод:

1) for $i = 0$ to $k - 1$ do $b[i + 1] := a \cdot i + c \ (mod\ k)$ od

2) За спільними правилами перетворили масив b і зафіксували його значення (створили спільний визначальний рядок).

3) 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 $i = 1, 2, \ldots, k$ *)

4) за масивом $b = (b_1, b_2, \ldots, b_k)$ будуємо масив $P[1 \times k]$ (за яким будуються таблиці операцій кільця)

$P[0] := b_1$;

for $i = 1$ to $k - 2$ do $P[b_i] := b_{i+1}$ od

$P[b_{k-1}] := 0$.

Правильність алгоритма випливає з того, що коли i пробігає повну систему лишків, то $a \cdot i + c$ теж пробігає повну систему лишків, якщо НСД(a, k)=1 [6].

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

Зазначимо, що алгоритмом GEN-G можна згенерувати не більше ніж $(k-2)\varphi(k)$ визначальних рядків, де φ – функція Ойлера. Для криптографічних застосувань такої кількості не достатньо. Тому за домовленістю між абонентами згенерований алгоритмом визначальний рядок повинен перетворюватися однаковим чином, що визначає криптосистему як симетричну.

Приклад 1. Згенерувати визначальний рядок для $k = 6$ і $f(i) = i + 4$.

Перший цикл алгоритма генерує таку послідовність значень:

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

А другий цикл розставляє все на свої місця і видає ізоморфізм:

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

3) Третій цикл генерує за масивом $b_1 = 1, b_2 = 3, b_3 = 2, b_4 = 4, b_5 = 5, b_6 = 0$ рядок $P = (1, 4, 2, 5, 3, 0)$, за яким будуються таблиці операцій кільця G_6.

Неважко переконатися в тому, що кільце G_k, адитивна група якого повноциклічна, ізоморфне кільцю лишків Z_k. Такий ізоморфізм знаходиться за визначальним рядком, який згенерований алгоритмом GEN-G, тобто, генерація визначального рядка задає ізоморфізм між кільцями Z_k і G_k. Дійсно, маємо таку відповідність:

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

,

де ізоморфне відображення g буде таким: $g(k) = 0, g(1) = b_1 = 1, g(i) = b_i, i = 2, \ldots, k-1$.

Визначальний рядок, згенерований алгоритмом в прикладі 1, дає таке ізоморфне відображення $g(6) = g(0) = 0, g(1) = 1, g(2) = 5, g(3) = 3, g(4) = 4, g(5) = 2$.

3 Протокол обміну повідомленнями

Основна ідея побудови пропонованої криптосистеми ґрунтується на такій схемі:

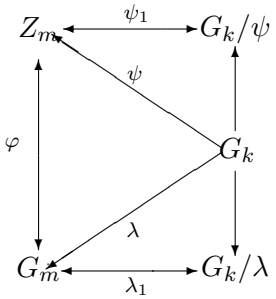

Рис.1. Схема системи

В цій схемі відображення

– φ – ізоморфізм між кільцями Z_m і R_m,

– ψ – сюр'єкція кільця G_k на кільце Z_m,

– λ – сюр'єкція кільця G_k на кільце G_m,

– ψ_1 – бієкція між фактор множиною G_k/ψ і кільця Z_m,

– λ_1 – бієкція між фактор множиною G_k/λ і кільця G_m, де $k = l \cdot m$ (сенс такого вибору чисел буде пояснено далі).

Обмін повідомленнями між Алісою і Бобом виконується за таким протоколом.

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

Після цього Аліса і Боб виконують такі кроки.

Крок 1.

а) Аліса будує систему виразів в кільці G_m:

$$l(x) = Ax = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_q + \ldots + a_{nq}x_q. \end{cases}$$

б) Перетворює $l(x)$ в кільці G_m таким чином:

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

де B_i – невироджені матриці розмірності $n \times n$, a, a_j – вектори розмірності $1 \times n$, $i = 1, 2, \ldots, r, = 1, 2, \ldots, r + 1$. Результатом такого перетворення є система

$$L(x) = Bx + a = \begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1q}x_q + a_1, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2q}x_q + a_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{n1}x_1 + b_{n2}x_q + \ldots + b_{nq}x_q + a_q. \end{cases}$$

в) Записує $l(x)$ і $L(x)$ шляхом заміни коефіцієнтів їхніми відповідниками з фактор-множини G_k/λ_1:

$$\bar{l}(x) = \bar{A}x = \begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1q}x_q, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2q}x_q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{n1}x_1 + b_{n2}x_q + \ldots + b_{nq}x_q. \end{cases}$$

і

$$\bar{L}(x) = \bar{B}x + b = \begin{cases} c_{11}x_1 + c_{12}x_2 + \ldots + c_{1q}x_q + b_1, \\ c_{21}x_1 + c_{22}x_2 + \ldots + c_{2q}x_q + b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_{n1}x_1 + c_{n2}x_q + \ldots + c_{nq}x_q + b_q. \end{cases}$$

Аліса висилає відкритим каналом або виставляє на своєму сайті вирази $\bar{l}(x)$ і $\bar{L}(x)$.

Крок 2.

а) Боб за виразами $\bar{l}(x)$ і $\bar{L}(x)$ та відповідними відображеннями знаходить вирази $l(x)$ і $L(x)$ в кільці Z_m, вибирає два вектори $\bar{x}$ і $\bar{a}$ розмірності $1 \times q$.

б) Обчислює вектори значень $\bar{l}(\bar{x}) = v$ і $\bar{l}(\bar{a}) = d$ та $\bar{L}(\bar{x} + \bar{a}) = d_1$ за модулем m.

в) Значення v, яке він хоче передати Алісі, зберігає в таємниці, а значення d і d_1 записує в кільці G_m (за ізоморфізмом φ) і висилає Алісі відкритим каналом пару векторів (d, d_1).

Крок 3.

а) Аліса обчислює обернені матриці до матриць B_i в кільці G_m (а це обчислення виконується в кільці Z_m) за ізоморфізмом φ.

б) Знаходить значення v, оскільки всі дані для цього в неї є.

Твердження 1. *Обмін повідомленнями за протоколом виконується коректно.*

Доведення очевидним чином випливає з властивостей лінійних операторів, бієкції λ_1 та ізоморфізму φ. 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 в результаті множення матриць $B_1, B_2, \ldots, B_r$ на вектори $a_1, a_2, \ldots, a_r$. Тоді

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

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

З рисунка 1 випливає, що в схемі системи існує принаймні три шляхи створення шифрограми:

1) $G_k/\psi_1 \to Z_m \to G_m$, що означає побудову виразів $l(x)$ і $L(x)$ у фактор-множині G_k/ψ_1, за бієкцією ψ_1 ці вирази записуються в кільці Z_m де виконуються обчислення і будується шифрограма. Ця шифрограма за ізоморфізмом φ перетворюється в шифрограму в кільці G_m.

Цьому шляху відповідає вищенаведений протокол.

2) $G_k/\lambda_1 \to G_m \to Z_m \to G_k/\psi_1$, що означає побудову виразів $l(x)$ і $L(x)$ у фактор-множині G_k/λ_1, за бієкцією λ_1 ці вирази записуються в кільці G_m, за ізоморфізмом φ записуються в кільці Z_m де виконуються обчислення і будується шифрограма. Ця шифрограма за бієкцією ψ_1 перетворюється в шифрограму у фактор-множині $G_k/\psi-1$.

3) $G_m/\psi_1 \to Z_m \to G_m \to G_k/\lambda_1$. що означає побудову виразів $l(x)$ і $L(x)$ у фактор-множині G_k/ψ_1, за бієкцією ψ_1 ці вирази записуються в кільці Z_m де виконуються обчислення і будується шифрограма. Ця шифрограма за ізоморфізмом φ перетворюється в шифрограму в кільці G_m, а потім за бієкцією λ_1 перетворюється в шифрограму у фактор-множині G_k/λ_1.

Приклад 2. Нехай Аліса і Боб обмінялися трійкою $(a,c,2,25)$ і зупинилися на такому 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-$G(a,c,25)$ знаходить ізоморфне відображення $\varphi: Z_{25}\to G_{25}$, яке в даному випадку набуває вигляду:

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

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

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

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

Нехай літери алфавіту англійської мови перенумеровані природним чином:

Таблиця 1 (цифрових відповідників символів алфавіту)

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

Задаючи бієкцію ψ_1 кільця G_{49}[1] на кільце G_{25} вигляду

$$\psi_1=\left\{\begin{array}{cc} \psi(0)=7, & i=0\\ \psi(i\ (mod\ 25)) & = \quad m_{i-1}+1,\ i\geq 1,\end{array}\right.$$

[1]В якості G_{49} можна взяти довільну множину, потужності $25\cdot l$, Алісі і Бобу однаковим чином упорядкувати її елементи і побудувати бієкцію ψ_1.

де $i = 1, 2, \ldots, 49$, дістаємо порядковий номер класу елемента m_i:

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
7	10	17	2	34	11	20	39	33	48	3	45	4	37	6	41	13	43	15	36	8	38	9	35	12
40	14	44	19	46	16	47	21	31	24	27	42	29	22	32	23	30	25	28	18	26	0	1	5	
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

Крок 1. Нехай Аліса побудувала в кільці G_{25} такі вирази:

$$l(x) = \left\{ \begin{array}{l} 2x_1 - 16x_2 + 7x_3 + 20x_4, \\ 0x_1 + 1x_2 - 17x_3 - 11x_4 \end{array} \right. \quad \left(= \left\{ \begin{array}{l} 2x_1 + 4x_2 + 7x_3 + 20x_4, \\ 0x_1 + 1x_2 + 11x_3 + 17x_4 \end{array} \right. \right)$$

і

$$L(x) = B_1(l(x) + (1,2)^t) = \left\{ \begin{array}{l} 9x_1 - 13x_2 + 10x_3 - 16x_4 + 3, \\ 18x_1 + 14x_2 - 18x_3 + 19x_4 + 16, \end{array} \right. \quad \left(= \left\{ \begin{array}{l} 9x_1 + 15x_2 + 10x_3 + 4x_4 + 3, \\ 18x_1 + 14x_2 + 2x_3 + 19x_4 + 16, \end{array} \right. \right)$$

де матриця B_1 має вигляд:

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

Крок 2. Аліса виконує заміну коефіцієнтів у побудованих виразах і матриці відповідниками з фактор множини G_{49}/λ_1 і дістає такі вирази:

$$\bar{l}(x) = \left\{ \begin{array}{l} 17x_1 + 34x_2 + 21x_3 + 26x_4, \\ 7x_1 + 14x_2 + 42x_3 + 43x_4 \end{array} \right.$$

і

$$\bar{L}(x) = B_1(l(x) + (1,2)^t) = \left\{ \begin{array}{l} 48x_1 + 41x_2 + 3x_3 + 46x_4 + 19, \\ 15x_1 + 32x_2 + 44x_3 + 36x_4 + 30 \end{array} \right.$$

і висилає Бобу відкритим каналом ці вирази.

Боб хоче вислати Алісі повідомлення (16,0). Для цього він виконує такі кроки.

Крок 3. Боб знаходить відповідники виразів $\bar{l}(x)$ і $\bar{L}(x)$ в кільці G_{25}

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

і

$$L(x) = \left\{ \begin{array}{l} 9x_1 + 15x_2 + 10x_3 + 4x_4 + 3, \\ 18x_1 + 14x_2 + 2x_3 + 19x_4 + 16, \end{array} \right.$$

Знаходить відповідник виразу $l(x)$ в кільці Z_{25}

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

Боб хоче передати Алісі повідомлення (16,0), відповідником якого є (19,0) в кільці Z_{25}. Боб розв'язує систему лінійних рівнянь в кільці Z_{25}

$$S = \left\{ \begin{array}{l} 5x_1 + 6x_2 + 9x_3 + 21x_4 = 19, \\ 0x_1 + 1x_2 + 11x_3 + 14x_4 = 0 \end{array} \right.$$

і знаходить розв'язок (0,12,8,0), якому відповідає розв'язок $x = (0, 13, 5, 0)$ в кільці G_{25}. Далі вибирає вектор

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

Обчислює вектор $\bar{x} + \bar{a} = (1, 15, 5, 0)$ в кільці G_{25} і значення

$$l(\bar{x}) = (16,0) = v,\ l(\bar{a}) = (11,1) = d \text{ і і } L(\bar{x}+\bar{a}) = (14,15) = d_1.$$

Боб зберігає значення v в таємниці, а значення d і d_1 висилає Алісі відкритим каналом або виставляє на сайті.

Крок 4. Аліса виконує такі обчислення.

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

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

б) Обчислює вектор $B_1^{-1}d_1^t = B_1^{-1}(14,15)^t$ і знаходить

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix}(14,15)^t = (4,4) = l(x+a) + (1,2)^t.$$

в) Обчислює значення

$$(4,4) - [(1,2) + (11,1)] = (4,4) + (15,16) = (16,0) = v\ \spadesuit.$$

3.1 Криптоаналіз протоколу

Очевидними кроками криптоаналітика є спроба розв'язати систему лінійних рівнянь в кільці Z_m

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

з метою знаходження $l(\bar{a})$. Зауважимо, що для цього потрібно знайти довільний розв'язок рівняння $l(\bar{a}) = d$ в кільці Z_k.

Потім за матрицями виразів $L(x)$ і $l(x)$ знайти матрицю D^{-1} і значення $L(\bar{a})$. А для цього потрібно знайти розв'язок системи рівнянь:

$$D^{-1}(B_r(B_{r-1}(\dots B_1(l(x)+a)\dots) = a^t. \tag{2}$$

Обчислити різницю $L(\bar{x}+\bar{a}) - L(\bar{a})$ і розв'язати систему рівнянь

$$L(\bar{x}+\bar{a}) - L(\bar{a}) = d_1\ (mod\ m), \tag{3}$$

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

Описані дії криптоаналітика будуть успішними за умови, що йому відомий ізоморфізм $\varphi : G_k \to Z_k$ та бієкції ψ_1 і λ_1. Але ці відображення йому невідомі і тому він не може знайти розв'язки систем (1), (2) і (3). Отже, стійкість пропонованого протоколу цілком ґрунтується на ізоморфізмі φ та бієкціях ψ_1, λ_1.

З розглянутої побудови скінченного кільця G_k випливає, що ізоморфізмів між G_m і Z_m існує $(m-2)!$, а число бієкцій між кільцями Z_m і G_k, як відомо, дорівнює кількості можливих різних розбиттів множини, яка має $k = l \cdot m$ елементів, на m класів по l елементів в кожному дорівнює $\frac{(lm)!}{(l!)^m m!}$ [7]. Отже, загальна кількість способів побудови шифрограми пропорційна

$$\frac{(lm)!}{(l!)^m m!} \cdot (m-2)! = \frac{(lm)!}{(l!)^m m(m-1)} = \frac{k!}{(l!)^m m(m-1)}.$$

Звідси дістаємо що коли при кожному сеансі обміну змінювати визначальний рядок, змінюючи тим самим ізоморфізм, то протокол буде мати необхідну стійкість.

З вищенаведеного прикладу видно, що в обчислювальному сенсі найскладнішим етапом є побудова обернених матриць в кільці G_m. Для того, щоб спростити ці обчислення, краще скористатися ізоморфізмом між кільцями $\varphi : G_m \to Z_m$ і вести обчислення в кільці лишків Z_m. Коли обернені матриці будуть знайдені, то виконати зворотні підстановки і отримати відповідні матриці в кільці G_m.

Як відомо, мультиплікативна група дільників одиниці кільця G_k є абелевою групою [6]. Для того, щоб в цій групі можна було застосовувати функцію дискретного логарифма, вона повинна бути циклічною. Тобто мати твірний елемент, який її породжує. Отже, виникає питання: за яких умов група дільників одиниці кільця G_k буде циклічною? Відповідь на це питання дає

Теорема 1. *Мультиплікативна група кільця Z_k буде циклічною тоді і тільки тоді, коли k дорівнює 2, 4, p^m або $2p^m$, де $m \geq 1$, p – непарне просте число [6].*

4 Формування повідомлення

Розглянемо питання: яким чином формуються та передаються параметри протоколу, а також повідомлення. 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 числами (a, c, l, k), де a, c, k – параметри алгоритма GEN-G(a, c, k). Якщо вибрати порядок кільця k кратним порядку кільця Z_m, тобто $k = l \cdot m$, то на підставі взаємної простоти чисел k, m і a, способи побудова кілець будуть відомі, а перетворення з метою побудови визначальних рядків кілець взяти однаковими ьдля G_k і G_m.

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

$$l(x) = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2q}x_q = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_q + \ldots + a_{mq}x_q = b_m \end{cases} \tag{4}$$

мала розв'язок. Отже, потрібно сформулювати умови, за яких така система буде сумісною. Умови сумісності дає таке

Твердження 2. *Система лінійних рівнянь $Ax = b \ (mod\ m)$ сумісна, якщо всі розв'язки системи лінійних однорідних рівнянь $A^T y = 0 \ (mod\ m)$ ортогональні вектору вільних членів b [7].*

З цього твердження випливає, що Аліса при побудові лінійних виразів $l(x)$ повинна перевірити лінійну незалежність за модулем k (тобто, розв'язати систему $A^T y = 0\ (mod\ k)$). Якщо вирази лінійно незалежні, то система $A^T y = 0\ (mod\ K)$ матиме тільки нульовий розв'язок, який, очевидно, ортогональний довільному вектору вільних членів системи $Ax = b$.

Приклад 3. Нехай літери алфавіту англійської мови перенумеровані природним чином (див. табл. 1):

Крім того, Аліса і Боб домовилися працювати в кільцях G_{25}, G_{49}, які ізоморфні кільцям Z_{25} і Z_{49} відповідно. Відображення φ, λ_1 були побудовані в прикладі 2.

Нехай Аліса побудувала вирази, які були наведені в прикладі 2.

Боб хоче передати Алісі повідомлення

tara tara tarara.

а) Боб розбиває повідомлення на блоки по два символи в блоці, цифровими відповідниками яких є пари чисел, взяті з таблиці 1:

ta	ra	ta	ra	ta	ra	ra
18,0	16,0	18,0	16,0	18,0	16,0	16,0

.

б) Розв'язує систему рівнянь в кільці G_{25}

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

Значення $v_1 = (18, 0)$ він тримає в секреті.

в) Обирає вектор $\bar{a} = (0, 1, 0, 1)$ і обчислює значення $d = l(\bar{a}) = (6, 19)$ і до розв'язку даної системи $\bar{x} = (0, 9, 19, 0)$ додає вектор $\bar{a} = (0, 1, 0, 1)$ і цю суму векторів $\bar{x} + \bar{a} = (0, 11, 19, 1)$ підставляє в $L(x)$, знаходячи тим самим значення $d_1 = (21, 3)$. Значення d і d_1 Боб передає Алісі.

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

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

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

б) Обчислює $B_1^{-1} d_1^t = B_1^{-1}(21, 3)^t$ і знаходить

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix} (21, 3)^t = (22, 18) = l(\bar{x} + \bar{a}) + (1, 2)^t.$$

в) Обчислює значення

$$(22, 18) - [(1, 2) + l(\bar{a})] = (22, 18) - [(1, 2) + (6, 19)] = (22, 18) + (24, 2) = (18, 0) = v_1.$$

а) Боб розв'язує систему рівнянь

$$l(x) = \begin{cases} 1 & 2x_1 + 4x_2 + 7x_3 + 20x_4 = 16, \\ & 0x_1 + 1x_2 + 11x_3 + 17x_4 = 0. \end{cases}$$

Значення $v_2 = (16, 0)$ він тримає в секреті.

б) Обирає вектор $\bar{a} = (1, 0, 1, 0)$ і обчислює значення $d = l(\bar{a}) = (17, 11)$ і до розв'язку даної системи $\bar{x} = (0, 13, 5, 0)$ додає вектор $\bar{a} = (1, 0, 1, 0)$ і цю суму векторів $\bar{x} + \bar{a} = (1, 13, 7, 0)$ підставля в $L(x)$, знаходячи тим самим значення $d_1 = (7, 0)$.

в) Значення d і d_1 Боб передає Алісі.

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

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

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

б) Обчислює $B_1^{-1}d_1^t = B_1^{-1}(7,0)^t$ і знаходить

$$B_1^{-1} = \begin{pmatrix} 1 & 1 \\ 23 & 22 \end{pmatrix}(7,0)^t = (7,21) = l(\bar{x}+\bar{a}) + (1,2)^t.$$

в) Обчислює значення

$$(7,21) - [(1,2) + l(\bar{a})] = (7,21) - [(1,2) + (17,11)] = (7,21) - (19,21) = (7,21) + (9,7) = (16,0) = v_2.$$

Оскільки наступний блок такий самий як і перший, тобто $v_3 = (18,0)$. Це змушує Боба вибрати новий вектор $\bar{a} = (0,0,1,1)$, за яким він обчислює значення

$$d = l(\bar{a}) = (2,0),\ \bar{x}+\bar{a} = (0,9,21,1),\ d_1 = L(\bar{x}+\bar{a}) = (3,16).$$

і висилає Алісі $d = (2,0),\ d_1 = (3,16)$.

Аліса обчислює

$$B_1^{-1}d_1^t = B_1^{-1}(3,16)^t = (1,2) = l(\bar{x}+\bar{a}) + (1,2)^t.$$

Звідки знаходить

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

Оскільки наступний блок такий самий як і перший, тобто $v_4 = (16,0)$. Це змушує Боба вибрати новий вектор $\bar{a} = (0,0,0,1)$, за яким він обчислює значення

$$d = l(\bar{a}) = (20,17),\ \bar{x}+\bar{a} = (0,13,5,1),\ d_1 = L(\bar{x}+\bar{a}) = (1,19).$$

і висилає Алісі $d = (20,17),\ d_1 = (1,19)$.

Аліса обчислює

$$B_1^{-1}d_1^t = B_1^{-1}(1,19)^t = (21,16) = l(\bar{x}+\bar{a}) + (1,2)^t.$$

Звідки знаходить

$$l(\bar{x}+\bar{a}) - [(1,2) + (20,17)] = (21,16) - (24,16) = (21,16) + (8,4) = (16,0) = v_4.$$

Оскільки наступний блок такий самий як і перший, тобто $v_3 = (18,0)$. Це змушує Боба вибрати новий вектор $\bar{a} = (0,1,0,0)$, за яким він обчислює значення

$$d = l(\bar{a}) = (4,1),\ \bar{x}+\bar{a} = (0,11,19,0),\ d_1 = L(\bar{x}+\bar{a}) = (9,12).$$

і висилає Алісі $d = (4,1),\ d_1 = (9,12)$.

Аліса обчислює

$$B_1^{-1}d_1^t = B_1^{-1}(9,12)^t = (6,4) = l(\bar{x}+\bar{a}) + (1,2)^t.$$

Звідки знаходить

$$l(\bar{x}+\bar{a}) - [(1,2) + (4,1)] = (6,4) - [(1,2) + (4,1)] = (6,4) - (3,4) = (6,4) + (14,16) = (18,0) = v_5.$$

Цю процедуру Боб і Аліса повторюють стільки разів, скільки блоків у повідомленні (в даному випадку один раз). Таким чином Аліса отримує шифрограму

(6,19,21,3) (17,11,7,0) (2,0,3,16) (20,17,1,19) (4,1,9,12) (11,1,14,15) (19,13,13,22).

Після дешифраці Аліса відкриває повідомлення

$$\begin{matrix} 18{,}0 & 16{,}0 & 18{,}0 & 16{,}0 & 18{,}0 & 16{,}0 & 16{,}0 \\ \text{ta} & \text{ra} & \text{ta} & \text{ra} & \text{ta} & \text{ra} & \text{ra} \end{matrix} \ \spadesuit .$$

В наведеному прикладі використовувалося одне і те саме кільце, але можна при кожному сеансі передачі або з певним періодом між передачами змінювати кільце. Можна змінювати вектори a і $\bar{a}$, які змінюють значення $l(\bar{a})$ і $L(\bar{x}+\bar{a})$.

Наведений протокол можна зробити складнішим, якщо використовувати при шифруванні кожного блоку різні кільця або різні значення параметрів – матриць і векторів. Крім того, якщо шифрований текст представити відповідниками в кільці G_{49}

(47,36,38,2) (43,45,39,40) (44,7,19,30) (26,25,10,18) (46,14,48,4) (42,10,6,23) (18,22,37,9),

то криптоаналітику зовсім недоступні ситеми виразів, кільце G_{25} і відображення.

5 Обчислювальні особливості

Виходячи з того, що обчислення в кільці G_m не є звичним при обчисленнях, то покращити ефективність шифрування і розшифрування можна, якщо знову скористатися ізоморфізмом між кільцями G_m і Z_m. Дійсно, пошук протилежного елемента до елемента a в кільці Z_m зводиться до обчислення різниці $m-a$, а обчислення оберненного елемента до a виконується шляхом застосування розширенного алгоритма Евкліда для розв'язання рівняння $ax+my=1$ (рзширений алгоритм Евкліда обчислює розклад $ax+by=d$, де d =НСД(a,b)). Результатом виконання цього алгоритму є значення $x=a^{-1}$.

Використовуючи ізоморфізм φ з приклада 2, система рівнянь з приклада 3 в кільці Z_{25} набуває вигляду:

$$\bar{l}(x)=\begin{cases} 5x_1+6x_2+9x_3+21x_4=20, \\ 0x_1+1x_2+11x_3+14x_4=0. \end{cases}$$

Розв'язком цієї системи є вектор $x=(0,10,15,0)$, якому відповідає розв'язок $\bar{x}=(0,9,19,0)$ системи

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

В кільці Z_{25} матриці

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

відповідає матриця

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

Література

[1] *Wenbo Mao.* Modern Cryptography. – Pearson Education. – Prentice Hall Professional Technical Reference Upper Saddle River. – New Jersey. – 2004. – 768 p.

[2] *Kameswari P.A., Sriniasarao S.S., Belay A.* An application of Linear Diophantine equations to Cryptography. – Advanced in Mathematics: Scientific Journal. –2021. – v. 10. – P. 2799 – 2806.

[3] *Hermann M., Juban L., Kolaitis P. G.* On the Complexity of Counting the Hilbert Basis of a Linear Diophantine System. – Springer Verlag. – LNCS. – 1999. – 1705. – P. 13–32.

[4] *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.

[5] *Kryvyi S., Opanasenko V., Grinenko O., Nortman Yu.* Symmetric system for Exchange Information on the Base of Surjective Isomorphism of Rings. *12th Int. IEEE Conf. on Dependable Systems, Services and Technologies (DESSERT 2022). – 2022.– December 9-11. – pp. 1-7.*

[6] *Shoup V.* An Computational Introduction to Number Theory and Algebra. – Cambridge University Press. – 2008. – 580 p.

[7] *Кривий С.Л.* Лінійні діофантові обмеження та їх застосування. – Київ: Інтерсервіс. – 2021. – 257 с.