DOI 10.31891/2307-5732-2023-323-4-278-285
УДК 621.397

ПОПОВИЧ БОГДАН
Національний університет "Львівська політехніка"
ORCID ID: 0000-0001-6259-2361
e-mail: bogdan.popovych@gmail.com
ПОПОВИЧ РОМАН
Національний університет "Львівська політехніка"
ORCID ID: 0009-0006-0992-0825
e-mail: rombp07@gmail.com

ЕЛЕМЕНТИ ВЕЛИКОГО ПОРЯДКУ ДЛЯ КРИПТОСИСТЕМ З НЕАБЕЛЕВИМИ БАЗОВИМИ ГРУПАМИ

Показано, як явно збудувати два елементи великого порядку, які не комутують, для випадку неабелевої групи квадратних матриць з ненульовим визначником над довільним скінченним полем. Для отримання таких двох елементів використано відомі результати про побудову елементів великого порядку в скінчених полях загального вигляду. Ключова думка полягає в тому, щоб утворити матрицю, визначник якої дорівнює елементу великого порядку в скінченному полі. Тоді порядок елемента скінченного поля є нижньою межею для порядку матриці. Пропонується утворювати таку матрицю як добуток нижньої трикутної та верхньої трикутної матриць. Розглянуто постквантові асиметричні криптосистеми, які використовують елементи великого порядку з вказаної групи.

Ключові слова: криптографічний захист інформації, скінченне поле, загальна лінійна група, порядок елемента, постквантова криптосистема.

POPOVYCH BOGDAN
Lviv Polytechnic National University
POPOVYCH ROMAN
Lviv Polytechnic National University

ELEMENTS OF HIGH ORDER FOR CRYPTOSYSTEMS WITH NON-ABELIAN PLATFORM GROUPS

The security of a number of well-known cryptographic primitives (Diffie-Hellman protocol, El-Gamal public key cryptosystem, El-Gamal digital signature) is based on the computational complexity of the discrete logarithm problem in a finite cyclic group. In the case of both abelian and non-abelian groups, this complexity is ensured by construction of elements of high (ideally, maximum possible) order from the group. Actually, such elements are used in the implementation of corresponding asymmetric cryptosystems. However, for the case of a non-abelian group, it is not known how to explicitly obtain such elements. Therefore, it is customary to take random elements, that does not guarantee the system's resistance to hacking.

The paper shows how to explicitly construct two high order elements that do not commute for the case of non-abelian group of square matrices with nonzero determinant over an arbitrary finite field. To obtain such two elements, known results on the construction of high order elements in finite fields of general form were used. The key idea is to form a matrix whose determinant is equal to high order element in the finite field. Then the order of this element is a lower bound for the order of the matrix. As one of the options, it is proposed to form such a matrix as a product of lower triangular and upper triangular matrices. Post-quantum asymmetric cryptosystems that use high order elements from the specified group are considered. It is shown how, using the constructed elements, to implement the cryptosystem that is analogous to the El-Gamal cryptosystem in the non-commutative case. A simple computational example is given that illustrates the implementation of this cryptosystem in the case of 2×2 matrices with elements from a finite field with 256 elements. Cryptosystems in the field of multivariate cryptography are also considered, for the construction of which high order elements from the specified group of matrices are required. Obtained results can be used in the construction of various post-quantum primitives.

Keywords: cryptographic information protection, finite field, general linear group, order of element, post-quantum cryptosystem.

Постановка проблеми

Важливою на даний час задачею є забезпечення конфіденційності, цілісності та автентичності інформації, криптографічний захист інформаційних зв'язків між компонентами сучасних комп'ютерних систем та мереж. Безпека низки відомих криптографічних примітивів (протокол Діффі-Хелмана, криптосистема Ель-Гамаля з відкритим ключем, цифровий підпис Ель-Гамаля) ґрунтується на складності проблеми дискретного логарифма в скінченній циклічній групі. Нагадаємо, що проблема дискретного логарифмування є наступною: для заданих елементів g і h групи знайти натуральне число x таке, що $g^x = h$. Як своєрідне узагальнення цієї проблеми можна вважати проблему спряженості: для заданих елементів g і h групи знайти елемент x групи такий, що $g^x = xgx^{-1} = h$. Хоча проблема дискретного логарифма формулюється для будь якої скінченої групи, але в застосуваннях до криптографії добре вивчені лише кілька груп: мультиплікативні групи простого та розширеного скінченних полів (алгоритм Діффі-Хелмана), група взаємно простих з числом pq (p та q – прості) і меншим за нього натуральних чисел (криптосистема RSA), група точок еліптичної кривої над скінченним полем. Усі наведені групи є абелевими.

В більшості випадків інших груп, зокрема неабелевих, складність проблеми дискретного алгоритму є недостатньо дослідженою. Досить часто проблема залежить від вибору твірного елемента та способу подання інформації про групу [1, 2]. Група може бути визначена за допомогою твірних елементів і

відношень, як група автоморфізмів алгебраїчного многовиду, як група матриць над скінченим кільцем, група перестановок. Вона може визначатися багатьма іншими способами. Наступний приклад демонструє важливість способу зображення абстрактної групи. Мультиплікативна група Z_p^* цілих чисел за модулем простого числа p ізоморфна адитивній групі кільця Z_{p-1} цілих чисел за модулем числа $p-1$. Якщо p - досить велике, то проблема є важкою в Z_p^*, проте для Z_{p-1} проблема еквівалентна розв'язанню лінійного рівняння.

Слід зауважити, що отриманий елемент великого порядку в довільній групі можна розглядати як генератор псевдовипадкової послідовності. Елементами цієї послідовності є попарно різні степені елемента великого порядку. Довжина послідовності дорівнює порядку елемента. Це ще одне можливе застосування елементів великого порядку в групах.

Отже, питання дослідження складності задачі дискретного логарифма, а також пов'язане з ним питання побудови елементів великого порядку в неабелевих групах, залишається актуальним.

Аналіз останніх джерел

Через F_q, де $q = p^n$ для деякого простого числа p та натурального числа n, позначаємо скінченне поле з q елементів. Твірні мультиплікативної групи $F_q^* = F_q \setminus \{0\}$ називають примітивними елементами.

Для реалізації криптографічних примітивів потрібна скінченна циклічна група. Усі групи, які на даний час широко використовують, зокрема група точок еліптичної кривої над скінченним полем, є абелевими. Вважається, що відповідні криптографічні побудови над ними можна зламати з використанням достатньо потужного квантового комп'ютера. Тому розглядають постквантові побудови з використанням неабелевих груп [1, 2, 3].

У всіх випадках (як абелевих, так і неабелевих груп) складність проблеми дискретного логарифма забезпечується наявністю в групі елементів великого мультиплікативного порядку (в ідеалі твірних елементів груп). Для отримання елемента великого порядку є два відомих підходи: 1) побудова елемента з отриманням нижньої межі для порядку цього елемента [4, 5, 6]; 2) використання теореми Лагранжа для скінченних груп [7]. Цей підхід можна застосувати, якщо порядок групи розкладений в добуток простих чисел. Другий спосіб часто використовують для еліптичних кривих.

Однією з широко відомих неабелевих груп є загальна лінійна група $GL(m, F_q)$ – матриці розміру $m \times m$ заповнені елементами поля F_q та з ненульовим визначником відносно операції множення матриць (або в іншій формі лінійні перетворення в першому варіанті з $(F_q)^n$ в $(F_q)^n$, а в другому – з F_{q^n} в F_{q^n} відносно операції композиції відображень) [2, 3]. Так званий цикл Зінгера має максимальний можливий для загальної лінійної групи порядок $q^m - 1$ [8]. Проте, як явно збудувати цей елемент невідомо. Є лише відомі результати про його існування.

Схему узгодження ключа з використанням неабелевих груп запропоновано Стікелем [3]. Цю схему можна розглядати як перенесення ідеї протоколу Діффі-Хелмана для комутативних груп на некомутативний випадок. В комутативному випадку для вказаного протоколу використовують степінь g^u одного елемента g групи. В протоколі Стікеля використовують некомутативну поведінку добутку степенів a^v, b^w двох елементів a, b групи.

Виходячи з протоколу Діффі-Хелмана в комутативному випадку було розроблено криптосистему Ель-Гамаля з відкритим ключем. Аналогічно в [3], виходячи з протоколу Стікеля, збудовано криптосистему з відкритим ключем. Суттєвою рисою цієї криптосистеми є те, що її реалізовано в некомутативній групі. Для її реалізації потрібно мати в повній лінійній групі два елементи великого порядку, які не комутують. Це відзначають автори роботи [3]. Проте, як отримати такі елементи в роботі не описано. В наведеному прикладі елементи вибирають випадком чином, а потім програмним шляхом обчислюють їх порядки. У випадку, коли повна лінійна група має досить багато елементів, це неможливо зробити за прийнятний час.

У роботах [1, 2] запропоновано криптосистеми з використанням низки бієктивних перетворень векторного простору $(F_q)^n$ (як лінійних, так і нелінійних). Такі перетворення з операцією їх композиції утворюють неабелеву групу. Маючи в цій групі елемент великого порядку, можна реалізувати як протокол Діффі-Хелмана, схему Ель-Гамаля чи цифровий підпис. Для отримання такого елемента потрібен елемент великого порядку в повній лінійній групі. Як його можна отримати в [1, 2] не сказано. Є лише згадка про

використання циклу Зінгера.

Таким чином, проблема стійкості до зламування запропонованих постквантових криптосистем [1, 2, 3], яка залежить від наявності елементів великого порядку в повній лінійній групі, залишається невирішеною. Тому актуальною задачею є розроблення методу отримання елементів великого порядку в повній лінійній групі.

Метою роботи є: запропонувати підхід до отримання елементів великого порядку із заданими властивостями в повній лінійній групі та дослідження подальшої можливості покращення криптосистем з робіт [1, 2, 3].

Виклад основного матеріалу

Далі описано, як отримати елементи A, B великого порядку в повній лінійній групі над скінченним полем. При цьому спираємось на результати робіт [4, 5, 6] стосовно отримання елементів великого порядку в довільних скінченних полях.

Ключова думка полягає в тому, щоб утворити матрицю A, визначник якої дорівнює $\det A = \alpha$, де α – елемент великого порядку рівного $ord(\alpha)$ в скінченному полі F_q. Оскільки визначник добутку матриць над полем дорівнює добутку визначників цих матриць, тобто $\det \prod_{i=1}^{r} M_i = \prod_{i=1}^{r} \det M_i$, то порядок матриці A є принаймні $ord(\alpha)$. Дійсно, $\det A^i = \alpha^i$, $\alpha^i \neq 1$ при $1 \le i < ord(\alpha)$ та $\alpha^{ord(\alpha)} = 1$. Порядок матриці може бути й більшим від $ord(\alpha)$, бо те, що визначник матриці $A^{ord(\alpha)}$ дорівнює одиниці, не означає співпадіння цієї матриці з одиничною матрицею.

Як утворити матрицю, визначник якої дорівнює α? Пропонується (для спрощення обчислень та можливості підсилення нижньої межі для порядків матриць) утворювати таку матрицю як добуток нижньої трикутної та верхньої трикутної матриць. Перша перевага – визначник верхньої (нижньої) трикутної матриці дорівнює добутку її діагональних елементів. Тому просто утворити нижню (верхню) трикутну матрицю, а тоді й довільну матрицю з потрібним визначником. Друга перевага – при викресленні з нижньої (верхньої) трикутної матриці якихось рядка і стовпця, на перетині яких знаходиться ненульовий елемент, отримуємо нижню (верхню) трикутну матрицю. Це дозволяє просто отримати обернену до нижньої (верхньої) трикутної матриці.

Більш точно, беремо нижню трикутну матрицю

$$\begin{pmatrix} \alpha & 0 & \dots & 0 \\ a_{21} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & & 1 \end{pmatrix},$$

де α – елемент великого порядку в F_q.

Вказаний елемент великого порядку будуємо, використовуючи підходи, які описані в [4, 5, 6]. Наприклад [4], для випадку $q = p = 3$, $n = 298$ маємо $l = 3^6 = 729$, $t^l - g(t) = t^{729} - (2t^7 + t^4 + t^3 + t^2 + 1)$. Многочлен $t^l - g(t)$ розкладається над полем F_3 на нерозкладні многочлени степеня 10, 310, 298, 22, 25, 4, 60. Нерозкладний многочлен $f(t)$ степеня 298 задає потрібне скінченне поле $F_3(\alpha) = F_3[t]/(f(t))$ з 3^{298} елементів. Елемент α є елементом великого порядку в цьому скінченому полі.

Оскільки визначник цієї матриці дорівнює α, то вона має порядок принаймні $ord(\alpha)$ і є елементом великого порядку в групі $GL(m, F_q)$. Аналогічно виглядає верхня трикутна матриця

$$\begin{pmatrix} 1 & b_{12} & \dots & b_{1m} \\ 0 & \alpha & \dots & b_{2m} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & & 1 \end{pmatrix}.$$

Добуток такої верхньої трикутної і аналогічної нижньої трикутної матриць є матрицею з ненульовим визначником α^2, яка загалом вже не є ні верхньою, ні нижньою трикутною матрицею. Вона

має порядок принаймні $ord(\alpha^2)$. Елементи в матрицях над головною діагоналлю можемо довільно вибирати. Беремо їх так, щоб добуток цих матриць мав якнайбільший порядок. Зауважимо, що кожна матриця з повної лінійної групи має *LU*-розклад, тобто може бути записана у вигляді добутку нижньої трикутної та верхньої трикутної матриць.

Інший варіант утворення матриці з потрібним визначником – це утворення верхньої трикутної матриці з таким визначником і домноження її зліва на якусь оборотну матрицю та справа на обернену до цієї оборотної матриці (тобто формування спряженої до верхньої трикутної матриці). Зауважимо, що спряжені елементи в будь-якій групі мають однакові порядки. Дійсно, це випливає з рівності

$$(HAH^{-1})^k = HA^kH^{-1}.$$

У частковому випадку повної лінійної групи можемо пробувати підбирати параметри q і m так, щоб число $q^m - 1$ мало великий простий дільник. Згідно з наслідком з теореми Лагранжа для скінченних груп, якщо кількість елементів групи є простим числом, то всі елементи цієї групи, крім нейтрального, є твірними елементами цієї групи. У вказаному випадку можна скористатися цим наслідком. Досить перевірити, чи взята матриця у степені простого дільника числа $q^m - 1$ дорівнює одиничній матриці. Зокрема, можна вибрати $q = 2$ та m таке просте число, що $2^m - 1$ є простим числом (так зване просте число Мерсена). Наприклад, число $2^{521} - 1$ є простим [9]. Інший можливий вибір: $q = 109987$ – просте, $m = 137$ – просте, число $q^m - 1 = 2467 \cdot D$ (D – великий простий дільник) має приблизно 17x137≈2000 біт.

Коротко опишемо, які обчислення виконують при реалізації криптосистеми з роботи [3].

Початковий крок. Припускають, що в групі існують два елементи A, B великих порядків $ord(A) = n_1$ та $ord(B) = n_2$, $AB \neq BA$ та проблема дискретного логарифму й проблема спряженого елемента є обчислювально важкими.

Утворення ключів. Аліса вибирає випадковим чином $0 < r < n_1$, $0 < s < n_2$, (r, s) – приватний ключ Аліси, і обчислює $K = A^r B^s$, (A, B, K) – публічний ключ.

Шифрування. Щоб переслати Алісі повідомлення M (довільна матриця розміру $m \times m$, заповнена елементами поля F_q), Боб вибирає $0 < v < n_1$, $0 < w < n_2$ і виконує обчислення

$$X = A^v B^w,\ C_1 = X^{-1} K X,\ C_2 = X K X^{-1},\ C = C_1 M C_2,\ C' = A^v K B^w.$$

Пара (C, C') є шифрограмою.

Дешифрування. Аліса виконує обчислення

$$D = (A^r)^{-1} C' (B^s)^{-1},\ D_1 = D^{-1} K^{-1} D,\ D_2 = D K^{-1} D^{-1},\ M = D_1 C D_2.$$

В роботі [3] описано, що матриця повідомлення повинна бути елементом повної лінійної групи. Тоді виникає проблема, як довільне повідомлення (блок), яке можна розглядати як послідовність символів в системі числення за основою p, перетворити в оборотну матрицю над полем F_q, де $q = p^n$. Насправді матриця повідомлення M не мусить бути оборотною матрицею, бо не фігурує в виразах, де треба знаходити обернену матрицю. M може бути довільною матрицею розміру $m \times m$, заповненою елементами поля F_q. Кожен елемент поля F_q можна розглядати як послідовність з n символів в системі числення за основою p.

За оцінкою авторів роботи [3] описана криптосистема дає безпеку d біт, якщо скінченне поле F_q має розмір $2d$ біт. Наприклад, для досягнення рівня безпеки 112 біт слід використовувати поле, яке має принаймні 2^{224} елементів. У цьому разі не враховано вплив розміру матриць m. Для врахування цього параметра слід зменшити розмір поля до q/m^2, тобто до $2d - \log_2 m^2$ біт.

Далі даємо простий приклад реалізації описаної раніше криптосистеми з роботи [3] з врахуванням запропонованих нами вдосконалень. Обчислювальні дані отримані з використанням реалізації криптосистеми в середовищі об'єктно-орієнтованого програмування C# 5.0. Ця реалізація, зокрема, містить функції додавання та множення елементів скінченного поля, множення матриць із загальної лінійної групи, піднесення матриці до степеня, знаходження оберненої матриці.

Розглядаємо матриці розміру 2x2 з ненульовим визначником над скінченним полем $F_{2^8} = F_2[t]/(t^8+t^4+t^3+t+1)$. Зауважимо, що многочлен $f(x) = t^8+t^4+t^3+t+1$ є нерозкладним над полем F_2. При виконанні обчислень слід додавати й множити елементи поля F_{2^8}. Множення елементів заміняємо на послідовні зсуви коефіцієнтів многочлена від змінної t і корекції (відповідні додавання).

Початковий крок. Матрицю A отримуємо як добуток нижньої трикутної матриці

$$A_1 = \begin{pmatrix} 1 & 0 \\ t^7+t+1 & t+1 \end{pmatrix}$$

та верхньої трикутної матриці

$$A_2 = \begin{pmatrix} t+1 & t \\ 0 & 1 \end{pmatrix}.$$

Матриця A_1 має визначник рівний $t+1$. Оскільки елемент $t+1$ є примітивним елементом скінченного поля F_{256}, тобто має максимально можливий порядок 255, то порядок матриці A_1 принаймні 255. Аналогічно матриця A_2 має визначник $t+1$ і порядок принаймні 255.

Матриця

$$A = A_1A_2 = \begin{pmatrix} t+1 & t \\ t^7+t^4+t^3+t^2+t & t^4+t^3+t^2+t \end{pmatrix}$$

має визначник $(t+1)^2 = t^2+1$, який є примітивним елементом в F_{256}. Таким чином, порядок матриці A принаймні 255. Обчислення показують, що $A^{255} \neq E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, а $A^{255\cdot 257} = E$. Так як 257 – просте число, то порядок матриці A дорівнює $n_1 = ord(A) = 255\cdot 257 = 65535$. Це максимально можливий порядок елемента в повній лінійній групі, яку розглядаємо. Такий елемент прийнято називати циклом Зінгера.

Аналогічно матрицю B отримуємо як добуток нижньої трикутної матриці

$$B_1 = \begin{pmatrix} t^3+t+1 & 0 \\ t^5+t^2+1 & 1 \end{pmatrix}$$

та верхньої трикутної матриці

$$B_2 = \begin{pmatrix} 1 & t \\ 0 & t^3+t+1 \end{pmatrix}.$$

Елемент t^3+t+1 є примітивним елементом скінченного поля F_{256}. Матриця

$$B = B_1B_2 = \begin{pmatrix} t^3+t+1 & t^4+t^2+t \\ t^5+t^2+1 & t^6+1 \end{pmatrix}$$

має порядок $n_2 = ord(B) = 65535$.

У результаті маємо дві матриці A, B, мультиплікативні порядки яких дорівнюють 65535. Крім того, перевірка показує, що ці матриці не комутують, тобто $AB \neq BA$.

Для пришвидшення обчислень при утворенні ключів, шифруванні та дешифруванні можна на початковому кроці крім вибору матриць A, B підготувати (обчислити) A^{2^i}, B^{2^i} для $i=1,2,...,15$, та A^{-2^j}, B^{-2^j}. для $j=1,2,...,15$.

Утворення ключів. Для утворення публічного та секретного ключів, Аліса вибирає два випадкових натуральних числа $r=20312<n_1=65535$ та $s=37411<n_2=65535$. Тоді вона обчислює

$$K=A^{20312}B^{37411}=\begin{pmatrix} t^7+t^6+t^5+t^4+t^3+1 & t^4+t+1 \\ t^7+t^5+t^4+t^3+t^2+t & t^7+t^4+t^3+t^2+t+1 \end{pmatrix}.$$

Секретний ключ Аліси дорівнює (20312; 37411), а публічний – (A,B,K).

Шифрування. Щоб зашифрувати для Аліси повідомлення

$$M=\begin{pmatrix} t^7+t & t^6+t^2 \\ t^5 & t^6+t^4+t^2+1 \end{pmatrix},$$

Боб вибирає випадковим чином $u=11547<n_1$ та $v=23178<n_2$. Вхідними даними для шифрування є повідомлення M (зауважимо, що обсяг кожного такого повідомлення в даному прикладі – 4×8=32 біти) та публічний ключ Аліси (A,B,K). Для отримання шифрограми Боб виконує такі обчислення.

Знаходить

$$Y=A^{11547}B^{23178}=\begin{pmatrix} t^4+t^3+t^2+t+1 & t^7+t^6+t^4+t^3+t+1 \\ t^7+t^2+t+1 & t^6+t^2 \end{pmatrix},$$

$$Y^{-1}=\begin{pmatrix} t^7+t^6+t^4+t^3+t^2+t+1 & t^6+t^3+t \\ t^7+t^3+t & t^7+t^6+t^3+t^2 \end{pmatrix}.$$

Тоді утворює

$$C_1=Y^{-1}KY=\begin{pmatrix} t^6+t^5+t^3+t^2 & t^7+t^5+t^3+1 \\ t^7+t^6+t^3+1 & t^3+t \end{pmatrix},$$

$$C_2=YKY^{-1}=\begin{pmatrix} t^7+t^6+t^5+t^3 & t^7+t^5+t^2+t \\ t^7+t^4+t^3+t^2+t+1 & t^7+t^3+t^2+t \end{pmatrix}.$$

Отримує

$$C=C_1MC_2=\begin{pmatrix} t^6+t^4+t^2+t & t^7+t^2 \\ t^7+t^5+t^4+t^2+t & t^5+t^4+t^2+t+1 \end{pmatrix},$$

$$C'=A^{11547}KB^{23178}=\begin{pmatrix} t^4+t^3+t^2+t+1 & t^6 \\ t^5+t^3+1 & t^7+t^4+t^2 \end{pmatrix}.$$

Криптограма, яку Боб пересилає Алісі, це пара (C,C').

Дешифрування. Аліса обчислює

$$A^{-20312}=\begin{pmatrix} t^4+t^3+t^2 & t^7+t^6+t^2 \\ t^7+t^6+t^5+t^3+t^2+1 & t^7+t^5+t^3+1 \end{pmatrix},$$

$$B^{-37411}=\begin{pmatrix} t^3+t^2+t+1 & t^7+t^3+t^2+t+1 \\ t^5+t^4+t^2 & t^6+t^5+t^2+t+1 \end{pmatrix}$$

і тоді отримує

$$D = A^{-20312}C'B^{-37411} = \begin{pmatrix} t^4+t^3+t^2+t+1 & t^7+t^6+t^4+t^3+t+1 \\ t^7+t^2+t+1 & t^6+t^2 \end{pmatrix}.$$

Далі обчислює

$$D^{-1} = \begin{pmatrix} t^7+t^6+t^4+t^3+t^2+t+1 & t^6+t^3+t \\ t^7+t^3+t & t^7+t^6+t^3+t^2 \end{pmatrix},$$

$$K^{-1} = \begin{pmatrix} t^7+t^3+t^2+t & t^3+t \\ t^6+t^2 & t^7+t^6+t^5+t^4+t^3+t^2+t \end{pmatrix},$$

$$D_1 = D^{-1}K^{-1}D = \begin{pmatrix} t^6+t^5+t^3+t & t^7+t+1 \\ t^7+t^6+t^2+t & t^4+t^3+t \end{pmatrix},$$

$$D_2 = DK^{-1}D^{-1} = \begin{pmatrix} t^6+t^5+t^3+t^2+t+1 & t^7+t^6+t^4+t^3+t^2 \\ t^7+t^3+t^2+t & t^4+t^3+t^2+t+1 \end{pmatrix}.$$

У результаті Аліса отримує повідомлення, яке зашифрував Боб:

$$M = D_1CD_2 = \begin{pmatrix} t^7+t & t^6+t^2 \\ t^5 & t^6+t^4+t^2+1 \end{pmatrix}.$$

У роботах [1, 2] для побудови криптосистем в криптографії багатьох змінних використовують групу, елементами якої є всеможливі бієктивні перетворення (як лінійні, так і нелінійні) векторного простору $(F_q)^n$ над скінченним полем F_q. Маючи в цій неабелевій групі елемент великого порядку g, можна реалізувати як протокол Діффі-Хелмана, так і схему Ель-Гамаля. У роботі [1] потрібний елемент $g = N^{-1}AN$ має порядок $q^n - 1$, де N – нелінійне перетворення, а A – елемент загальної лінійної групи. В [2, Theorem 2] описано, як отримати бажаний елемент g, застосовуючи низку певних елементів групи перетворень. Нижня межа для порядку елемента g визначається одним із застосовуваних елементів, який є елементом групи $GL(k, F_q)$, де $n = k(k+1)$. Таким чином, для обидвох випадків необхідно знайти елемент A великого порядку у відповідній повній лінійній групі.

В [1, 2] сказано, що як елемент A слід взяти так цикл Зінгера, який має максимальний можливий порядок для загальної лінійної групи. Проте, як вже було зауважено раніше, як явно збудувати цикл Зінгера невідомо. Є лише відомі результати про його існування. Пропонуємо як елемент A брати будь-яку з матриць, запропонованих у цій роботі для криптосистеми з [3].

Висновки

З метою покращення відомих асиметричних криптосистем, розглянуто можливість отримання елементів великого порядку із заданими властивостями в повній лінійній групі над довільним скінченним полем.

Для випадку неабелевої групи квадратних матриць з ненульовим визначником над довільним скінченним полем показано, як явно збудувати два елементи великого порядку з цієї групи, які не комутують. Для отримання таких двох елементів використано відомі результати про побудову елементів великого порядку в скінчених полях загального вигляду. Ключова думка полягає в тому, щоб утворити матрицю, визначник якої дорівнює елементу великого порядку в скінченному полі. Тоді порядок елемента скінченного поля є нижньою межею для порядку матриці. Пропонується утворювати таку матрицю як добуток нижньої трикутної та верхньої трикутної матриць.

Також розглянуто постквантові асиметричні криптосистеми багатьох змінних, які використовують елементи великого порядку з вказаної групи. Отримані результати можуть бути використані при побудові різних постквантових примітивів.

Майбутнє дослідження може бути спрямоване на покращення нижніх меж для порядків отриманих елементів з повної лінійної групи.

Література

1. Ustimenko V. On the families of stable transformations of large order and their cryptographical

applications / V. Ustimenko // Tatra Mountains Mathematical Publications. – 2017, Volume 70 (1), P. 107–117. DOI: https://doi.org/10.1515/tmmp-2017-0021.

2. Ustimenko V. On computations with double Schubert automaton and stable maps of multivariate cryptography / V. Ustimenko // Interdisciplinary Studies of Complex Systems. – 2021, No. 19, P. 18–32. DOI: https://doi.org/10.31392/iscs.2021.19.018.

3. Kanwal S. A cryptosystem with noncommutative platform groups / S. Kanwal, R. Ali // Neural Computing and Applications. – 2018. – Volume 29. – P. 1273–1278. – DOI: https://doi.org/10.1007/s00521-016-2723-8.

4. Попович Б.Р. Комп'ютерна перевірка припущення Гао, пов'язаного з отриманням елементів великого порядку в скінченних полях / Б.Р. Попович // Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. – 2018. – № 905. – С. 106–110. – DOI: https://doi.org/10.23939/csn2018.905.106.

5. Попович Б.Р. Елементи великого мультиплікативного порядку в розширених скінченних полях на основі модифікованого підходу Гао / Б.Р. Попович // Науковий журнал "Комп'ютерні системи та мережі", Національний університет "Львівська політехніка". – 2019. – Випуск 1 (1). – С. 63–68. – DOI: https://doi.org/10.23939/csn2019.01.063.

6. Dunets R. On construction of high order elements in arbitrary finite fields / R. Dunets, B. Popovych, R. Popovych // JP Journal of Algebra, Number Theory and Applications. – 2019. – Volume 42 (1). – P. 71–76. – DOI: http://dx.doi.org/10.17654/NT042010071.

7. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton: CRC Press, 2001. – 816 p.

8. Ghorpade S. R. Primitive polynomials, singer cycles and word-oriented linear feedback shift registers / S. R. Ghorpade, S. U. Hasan, M. Kumari // Designs, Codes and Cryptography. – 2011. – Volume 58 (2). P. 123–134. DOI: https://doi.org/10.1007/s10623-010-9387-7.

9. Great Internet Mersenne Prime Search. [Електронний ресурс]. – Режим доступу: https://www.mersenne.org/primes/ – (Дата звернення 16.08.2023). – Назва з екрану.

References

1. Ustimenko V. On the families of stable transformations of large order and their cryptographical applications / V. Ustimenko // Tatra Mountains Mathematical Publications. – 2017, Volume 70 (1), P. 107–117. DOI: https://doi.org/10.1515/tmmp-2017-0021.

2. Ustimenko V. On computations with double Schubert automaton and stable maps of multivariate cryptography / V. Ustimenko // Interdisciplinary Studies of Complex Systems. – 2021, No. 19, P. 18–32. DOI: https://doi.org/10.31392/iscs.2021.19.018.

3. Kanwal S. A cryptosystem with noncommutative platform groups / S. Kanwal, R. Ali // Neural Computing and Applications. – 2018. – Volume 29. – P. 1273–1278. – DOI: https://doi.org/10.1007/s00521-016-2723-8.

4. Popovych B.R. Kompiuterna perevirka prypushchennia Gao, poviazanoho z otrymanniam elementiv velykoho poriadku v skinchennykh poliakh / B.R. Popovych // Visnyk Natsionalnoho universytetu "Lvivska politekhnika". Kompiuterni systemy ta merezhi. – 2018. – № 905. – S. 106–110. – DOI: https://doi.org/10.23939/csn2018.905.106.

5. Popovych B.R. Elementy velykoho multyplikatyvnoho poriadku v rozshyrenykh skinchennykh poliakh na osnovi modyfikovanoho pidkhodu Gao / B.R. Popovych // Naukovyi zhurnal "Kompiuterni systemy ta merezhi", Natsionalnyi universytet "Lvivska politekhnika". – 2019. – Vypusk9999 1 (1). – S. 63–68. – DOI: https://doi.org/10.23939/csn2019.01.063.

6. Dunets R. On construction of high order elements in arbitrary finite fields / R. Dunets, B. Popovych, R. Popovych // JP Journal of Algebra, Number Theory and Applications. – 2019. – Volume 42 (1). – P. 71–76. – DOI: http://dx.doi.org/10.17654/NT042010071.

7. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton: CRC Press, 2001. – 816 p.

8. Ghorpade S. R. Primitive polynomials, singer cycles and word-oriented linear feedback shift registers / S. R. Ghorpade, S. U. Hasan, M. Kumari // Designs, Codes and Cryptography. – 2011. – Volume 58 (2). P. 123–134. DOI: https://doi.org/10.1007/s10623-010-9387-7.

9. Great Internet Mersenne Prime Search. [Online]. – Access mode: https://www.mersenne.org/primes/ – (Date of application 16.08.2023). – Name from the screen.