DOI: https://doi.org/ csn2024.02.183
УДК 004.056, 519.6

ПРОГРАМНА РЕАЛІЗАЦІЯ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ

Б.Р. Попович[1,2]***, Р.Б. Попович***[1]

[1]Національний університет "Львівська політехніка"
кафедра спеціалізованих комп'ютерних систем
[2]Львівський національний медичний університет імені Данила Галицького
кафедра медичної інформатики
E-mail: bogdan.r.popovych@lpnu.ua,roman.b.popovych.lpnu.ua

Розроблено на платформі C# (.NET Framework 5.0) , що забезпечує високу гнучкість у роботі, програму для виконання операцій (додавання, множення, піднесення до степеня великого натурального числа, знаходження оберненого відносно множення) над елементами розширених скінченних полів та загальних лінійних груп над такими полями. Загальна лінійна група є однією з відомих неабелевих груп, застосування якої активно вивчають в області постквантової криптографії. Використовуючи вказані операції, реалізовано низку криптографічних примітивів: загальновідомі протоколи Діфі-Хелмана, Стікеля узгодження таємного ключа й недавно запропоновані узагальнення протоколу Лізами-Ромеро та асиметричної криптосистеми Канвал-Алі. Програма дозволяє досліджувати особливості відомих та перевірку нових криптографічних примітивів. Застосовуючи її, підтверджено достовірність двох згаданих нових примітивів для різних значень параметрів.

Ключові слова: скінченне поле, загальна лінійна група, криптографічний примітив

1. Вступ

Сучасний етап розвитку суспільства характеризується суттєвим збільшенням обсягів інформації у всіх сферах людського буття. Для опису цього явища навіть з'явився термін "великі дані" (англ. big data), який позначає феноменальне прискорення нагромадження даних та їх ускладнення. Це підсилює вагу методів та засобів захисту інформації при її передаванні та опрацюванні. Ще одним викликом є необхідність протидіяти кібертероризму й кіберагресії. Їх здійсненням займаються організації або навіть держави, що мають майже необмежені фінансові й обчислювальні ресурси. Відбиток на дослідження питань захисту інформації також накладає очікування появи потужних квантових комп'ютерів. Вони зможуть вирішувати складні обчислювальні проблеми, які не під силу наявним сьогодні детермінованим комп'ютерам.

Основою багатьох криптографічних систем захисту інформацію є низка обчислювально складних задач. Однією з таких задач є проблема дискретного логарифму у вдало вибраній скінченній групі. У новітніх публікаціях пропонують поєднання дискретного логарифму з іншими криптографічними прийомами, зокрема проблемою спряженості або нелінійними перетвореннями. У цьому разі, зокрема, потрібно забезпечити обчислення над елементами скінченного поля та загальної лінійної групи над скінченним полем. Дослідженням таких методів підвищення ефективності захисту інформації в комп'ютерних системах на основі дискретного логарифму в комутативних та некомутативних групах приділено недостатньо уваги. Тому розробка та дослідження згаданих методів, їх програмна та апаратна реалізація є актуальними.

2. Огляд літературних джерел

Трьома базовими задачами криптографії є такі: узгодження таємного ключа через відкритий канал зв'язку, побудова асиметричних криптосистем, цифрове підписування. Для вирішення кожної з цих задач запропоновано низку обчислювальних схем, які прийнято називати примітивами.

Для реалізації криптографічних примітивів потрібна скінченна циклічна група [3]. 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 [3, 4, 5]. Однією з широко відомих неабелевих груп є загальна лінійна група [3, 4].

Для узгодження таємного ключа через відкритий канал зв'язку запропоновано низку протоколів, першим з яких був протокол Діфі-Хелмана [3]. Протокол з використанням неабелевих груп запропоновано Стікелем [3]. Його можна розглядати як перенесення ідеї протоколу Діфі-Хелмана для комутативних груп на некомутативний випадок. В роботі [1] наведено низку аналогів протоколу Діфі-Хелмана у загальній лінійній групі. У роботі [5] використано алгебру квадратних матриць фіксованого розміру, заповнених елементами простого скінченного поля, відносно операції множення. Стійкість цього протоколу до зламування ґрунтується на обчислювальній складності проблеми спряженості у вказаній алгебрі. Узагальнення цього протоколу на випадок довільного скінченного поля запропоновано в [9].

Для втілення асиметричних криптосистем , зокрема, запропоновано протоколи RSA, Ель Гамаля [3], Канвал-Алі [5], Устименка [10]. У [8] протокол Канвал-Алі узагальнено на випадок загальної лінійної групи над довільним скінченним полем. Для утворення й перевірки цифрового підпису також маємо низку протоколів, зокрема: цифровий підпис RSA, цифровий підпис Ель Гамаля, протокол Устименка.

Таким чином, на сьогодні є низка теоретичних пропозицій криптографічних примітивів над скінченними групами для вирішення кожної з трьох базових задач криптографії. Тому актуальним питанням стає підтвердження їх достовірності. Разом з тим, у більшості публікацій є лише окремі обчислювальні приклади, які ілюструють роботу протоколів [4, 5, 8, 9]. Для вирішення згаданої проблеми можна використовувати відомі програмні засоби: Matlab, Maple, GAP. Проте, їх використання ускладнене для випадків достатньо великих значень параметрів. Тому на нашу думку доцільно розробити програму, яка дозволить досліджувати особливості та робити перевірки достовірності криптографічних примітивів.

3. Постановка задачі

Метою роботи є розробка програми, що дозволить випробовувати різні криптографічні примітиви, які використовують у криптографії та які визначені над скінченними групами. Тобто йдеться як про дослідження особливостей відомих, так і про підтвердження достовірності нових запропонованих криптографічних примітивів шляхом їх програмної реалізації та наступних випробувань.

4. Реалізація операцій у скінченних групах

Розроблено програму, яка дозволяє виконувати операції додавання та множення над елементами скінченного поля та операції додавання та множення над елементами загальної лінійної групи над скінченним полем. Вказану програму реалізовано в середовищі C# версія 5.0 (.NET Framework 5).

При цьому для побудови відповідних скінченних полів та елементів великого мультиплікативного порядку в них використовуємо результати з робіт [2, 6, 7]. Для отримання елементів великого порядку в загальній лінійній групі над скінченним полем використовуємо результати з [8].

При виконанні обчислень слід додавати й множити елементи певного скінченного поля $F_{p^n} = F_p[x]/(f(x))$, де $f(x) = x^n + \sum_{i=0}^{n-1} f_i x^i$ – якийсь нерозкладний многочлен над простим полем F_p.

Кожен елемент скінченного поля зображаємо як цілочисельний масив довжини *n*. Нехай маємо два елементи скінченного поля: $U = \sum_{i=0}^{n-1} u_i x^i$ та $V = \sum_{i=0}^{n-1} v_i x^i$. Операцію додавання елементів U та V виконуємо очевидним чином:

$$U + V = \sum_{i=0}^{n-1} (u_i + v_i) x^i .$$

У цьому разі додавання чисел u_i та v_i виконуємо за модулем числа *p*.

Операцію множення елементів U та V виконуємо згідно з наведеним далі виразом:

$$U \cdot V = \left(\sum_{i=0}^{n-1} u_i x^i \right) \cdot \left(\sum_{i=0}^{n-1} v_i x^i \right) =$$

$$= \left(\sum_{i=0}^{n-1} u_i x^i \right) \cdot v_0 + \left(\left(\sum_{i=0}^{n-1} u_i x^i \right) \cdot x \right) \cdot v_1 + \left(\left(\left(\sum_{i=0}^{n-1} u_i x^i \right) \cdot x \right) \cdot x \right) \cdot v_2 + \ldots$$

$$+ \left(\ldots \left(\left(\left(\sum_{i=0}^{n-1} u_i x^i \right) \cdot x \right) \cdot x \right) \ldots \cdot x \right) \cdot v_n$$

Таким чином, множення двох елементів скінченного поля зводимо до послідовного множення першого многочлена-співмножника U на многочлен x, а потім на коефіцієнт v_i, та накопичення результату множення. Множення довільного многочлена $W = \sum_{i=0}^{n-1} w_i x^i$ на многочлен x здійснюємо наступним чином:

$$W \cdot x = \left(\sum_{i=0}^{n-1} w_i x^i \right) \cdot x = w_{n-1} x^n + \sum_{i=1}^{n-1} w_{i-1} x^i .$$

Враховуючи рівність $x^n = -\sum_{i=0}^{n-1} f_i x^i$, яка описує приведення (корекцію) за модулем многочлена $f(x)$, остаточно отримуємо

$$W \cdot x = \sum_{i=1}^{n-1} (w_{i-1} - w_{n-1} f_i) x^i - w_{n-1} f_0 .$$

Це означає, що для множення многочлена на елемент x масив його коефіцієнтів зсуваємо вправо на одну позицію. Молодший коефіцієнт цього масиву заповнюємо нульовим значенням. Тоді враховуємо згадану заміну доданка x^n на відповідний многочлен. Усі множення та додавання цілих чисел виконуємо за модулем числа *p*.

Відповідна блок-схема множення елементів скінченного поля F_{p^n} наведена на рис. 1. Змінні U та V позначають два елементи скінченного поля, які треба перемножити. Зображаємо їх як цілочисельні масиви довжини n. Масив res довжини n використано для формування результату множення U на V.

Масив buf довжини *n* зберігає проміжне значення, яке отримуємо при послідовному множенні многочлена U на многочлен x. Позначення left shift(buf) означає зсув масиву buf вліво (в сторону

старшого коефіцієнта) на один розряд із заповненням наймолодшого коефіцієнта нульовим значенням. Старший коефіцієнт масиву (який пропадає при виконанні вказаного зсуву) враховуємо при виконанні приведення за модулем многочлена $f(x)$.

Масив cor довжини n потрібний для врахування наведеної раніше коректуючої за модулем многочлена $f(x)$ рівності. Вказаний масив містить усі коефіцієнти многочлена $f(x)$, крім найстаршого коефіцієнта при степені x^n, тобто цей масив має вигляд $(f_{n-1}, f_{n-2}, ..., f_0)$. Змінна d використана для зберігання поточного значення найстаршого коефіцієнта масиву buf.

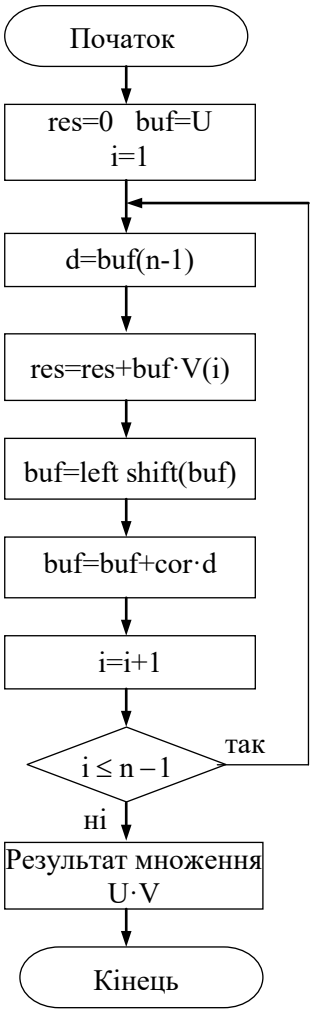

Рис. 1. Блок-схема множення елементів скінченного поля

Загальна лінійна група над довільним скінченним полем $GL(m, F_q)$ – це матриці розміру $m \times m$ заповнені елементами поля F_q, $q = p^n$, та з ненульовим визначником відносно операції множення матриць. Кожен елемент цієї групи зображаємо як двовимірний масив розміру $m \times m$, елементами якого є одновимірні цілочисельні масиви довжини n. У результаті кожен елемент групи це тривимірний цілочисельний масив розміру $m \times m \times n$.

Додавання елементів загальної лінійної групи виконуємо поелементним додаванням відповідних цілочисельних елементів тривимірних масивів за модулем числа p. Множення виконуємо як множення двовимірних матриць, використовуючи при цьому множення та додавання елементів скінченного поля.

Для реалізації примітивів також потрібне знаходження оберненого для ненульового елемента скінченного поля та оберненої матриці до матриці A, яка є елементом загальної лінійної групи над скінченним полем. Для вирішення цього завдання можна використати різні можливі підходи.

Зокрема, обернену матрицю до матриці A можна знайти з використанням LU-розкладу матриці A. Вказаний спосіб означає розклад матриці в добуток двох матриць: нижньої трикутної матриці L та верхньої трикутної матриці U. Тоді з рівності $A = LU$ випливає $A^{-1} = U^{-1}L^{-1}$.

Проте, для спрощення реалізації використано простіший підхід, пов'язаний з властивістю елементів скінченної групи: якщо група має s елементів, то для будь-якого елемента g групи виконується рівність $g^s = e$, де e нейтральний елемент групи. Ця властивість є наслідком з теореми Лагранжа для скінченних груп [3]. Виходячи з останньої рівності, обернений до елемента g можна знаходити згідно з виразом $g^{-1} = g^{s-1}$. Тобто, для знаходження оберненого елемента треба реалізувати піднесення елемента групи до степеня натурального числа.

При знаходженні обернених елементів та при реалізації примітивів потрібні операції піднесення елемента до степеня великого натурального числа. Тому реалізовано операції піднесення елемента скінченого поля (многочлена) та елемента загальної лінійної групи (матриці, заповненої елементами скінченого поля) до степеня натурального числа. Для цього використано швидкий (так званий індійський або повторюваного піднесення до степеня) алгоритм [3], який прийнято застосовувати для піднесення чисел до великого степеня за меншу кількість множень, ніж цього вимагає визначення степеня.

Насправді у незначно видозміненому вигляді цей алгоритм можна використати для піднесення елемента g будь-якої групи до натурального степеня s. Вважаємо, що маємо групу, яка задана в мультиплікативній формі, тобто операція групи є умовним множенням. Для обчислення елемента g^s в такій групі необхідно виконувати обчислення в такій послідовності:

- записуємо число s в двійковому вигляді: $s = s_0 \cdot 2^r + ... + s_{r-1} \cdot 2 + s_r$, де s_i ($i = 1,2,...,r$) – числа, що дорівнюють 0 або 1, $s_0 = 1$;
- приймаємо $g_0 = g$;
- для $i = 1,2,...,r$ обчислюємо $g_i = g_{i-1}^2 \cdot g^{s_i}$.

Елемент g_r є потрібним результатом.

Наведений алгоритм потребує близько $2\log_2 s$ множень елементів відповідної групи. Описаний алгоритм повторюваного піднесення до квадрату можна вважати мультиплікативним аналогом схеми Горнера обчислення значення многочлена, записаного у вигляді суми одночленів, при заданому значенні змінної.

5. Реалізація криптографічних примітивів

Спираючись на реалізацію описаних у розділі 4 операцій, втілено такі криптографічні примітиви:

- протокол Діфі-Хелмана узгодження таємного ключа через відкритий канал зв'язку (над мультиплікативною групою скінченного поля);
- протокол Діфі-Хелмана узгодження таємного ключа через відкритий канал зв'язку (над загальною лінійною групою над скінченним полем);
- протокол Стікеля узгодження таємного ключа через відкритий канал зв'язку (над загальною лінійною групою над скінченним полем);
- протокол Лізами-Ромеро узгодження таємного ключа через відкритий канал зв'язку (над загальною лінійною групою над скінченним полем);
- асиметричну криптосистему Канвал-Алі (над загальною лінійною групою над скінченним полем).

Реалізовано в двох різних варіантах протокол Діфі-Хелмана [3]. До початку роботи протоколу користувачі погоджують G – скінченну групу з q елементами та елемент g великого порядку $ord(g)$ в цій групі. Послідовність дій при реалізації цього протоколу в компактному вигляді показана на рис. 2. Аліса та Боб обмінюються утвореними ними елементами g^a та g^b і тоді обчислюють однаковий елемент $(g^b)^a=(g^b)^a$, який не проходить через відкритий канал зв'язку й не може бути обчислений зловмисником. Цей елемент може слугувати як таємний ключ при симетричному шифруванні.

В першому варіанті протокол реалізовано над мультиплікативною групою скінченного поля. При цьому використано збудованих в [2, 6, 7] скінченні поля та елементи g великого мультиплікативного порядку в цих полях. Оскільки при реалізації слід неоднократно підносити елемент g до степеня великого цілого числа, то використано швидкий алгоритм піднесення до степеня, який описано в розділі 4.

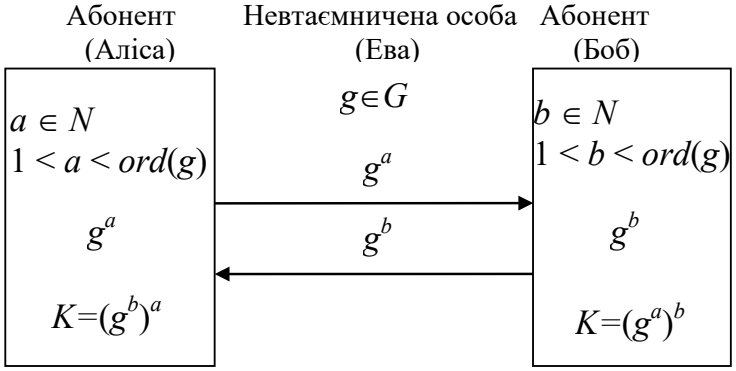

Рис. 2. Протокол Діфі-Хелмана.

У другому варіанті протокол реалізовано в загальній лінійній групі над скінченним полем. У цьому разі використано збудований у [8] елемент g великого порядку в загальній лінійній групі над скінченним полем. Оскільки слід неоднократно підносити елемент g (матрицю) до степеня великого цілого числа, то використано модифікований для матриць швидкий алгоритм піднесення до степеня.

Реалізовано протокол Стікеля [3] в загальній лінійній групі над скінченним полем. До початку роботи протоколу користувачі погоджують G – скінченну неабелеву групу з q елементами та два елементи A і B великого порядку в цій групі, які не комутують, тобто виконується умова $AB \neq BA$. Послідовність дій у вказаній реалізації в компактному вигляді показано на рис. 3.

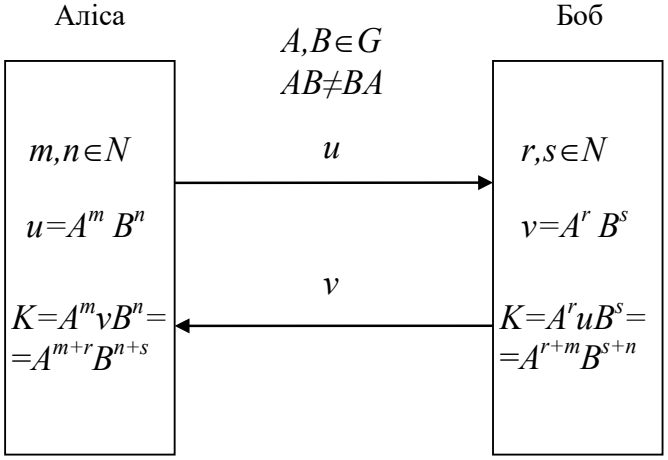

Рис. 3. Протокол Стікеля.

У цьому разі використано два елементи A, B великого порядку у згаданій групі, які не комутують. Побудова таких елементів описана в [8]. Використано модифікований для матриць швидкий алгоритм піднесення до степеня.

Реалізовано запропоноване в [9] узагальнення некомутативного протоколу Лізами-Ромеро [5] для загальної лінійної групи над довільним скінченним полем. До початку роботи протоколу користувачі погоджують G – скінченну неабелеву групу з q елементами (загальну лінійну групу) та

два елементи u, v великого порядку в цій групі, які не комутують та не діагоналізовні. Матриці u, v повинні бути не діагоналізовними, виходячи з міркувань уникнення атаки на протокол [5]. Побудова таких елементів описана в [9]. Послідовність дій у вказаній реалізації схематично показана на рис. 4. Використано модифікований для матриць швидкий алгоритм піднесення до степеня.

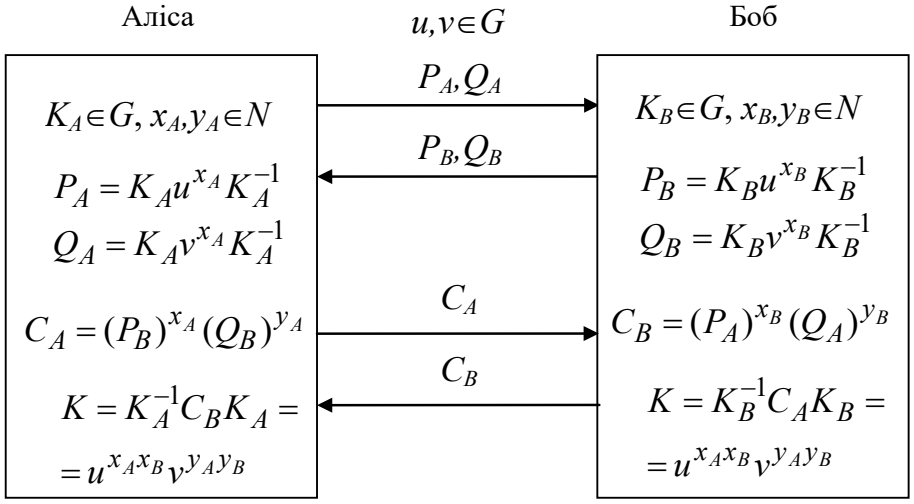

Рис. 4. Протокол Лізами-Ромеро.

Реалізовано запропоноване в [8] узагальнення асиметричної криптосистеми Канвал-Алі [4] над загальною лінійною групою над довільним скінченним полем. Послідовність дій схематично показана на рис. 5.

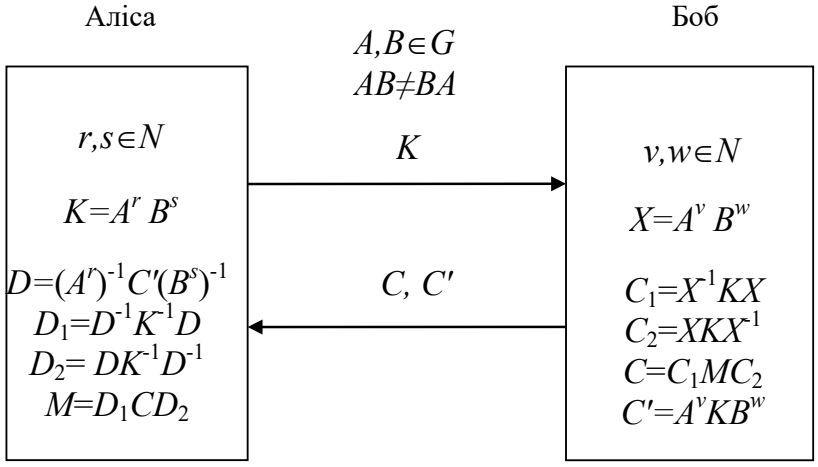

Рис. 5. Криптосистема Канвал-Алі.

Нами проведено тестування роботи програмної реалізації запропонованого нами в [9] узагальнення протоколу Лізами-Ромеро та запропонованого нами в [8] узагальнення криптосистеми Канвал-Алі. Випробування виконано для випадків: $q = 2,\ 2 \le n \le 500,\ 2 \le m \le 15$, $q = 3,\ 2 \le n \le 350,\ 2 \le m \le 10$, $q = 5,\ 2 \le n \le 200,\ 2 \le m \le 4$. Проведені випробування показали коректність роботи відповідних програмних реалізацій.

Зауважимо, що після шифрування інформації, слід захистити її від фізичних завад, які можуть виникнути при її передачі через канал зв'язку. Для цього треба додатково використати завадостійке кодування. Програмну модель завадостійких кодів Ріда-Соломона запропоновано в [11].

6. Результати дослідження

Отримані результати тестування підтвердили: достовірність узагальнення протоколу Лізами-Ромеро узгодження таємного ключа через відкритий канал зв'язку на випадок загальної лінійної групи над довільним скінченним полем та достовірність узагальнення асиметричної криптосистеми Канвал-Алі на випадок загальної лінійної групи над довільним скінченним полем. Випробування виконано для таких значень параметрів: $q = 2, 2 \le n \le 500, 2 \le m \le 15$, $q = 3, 2 \le n \le 350, 2 \le m \le 10$, $q = 5, 2 \le n \le 200, 2 \le m \le 4$.

7. Висновки

Розроблено в середовищі C# програму, яка дозволяє виконувати операції додавання, множення, піднесення до степеня великого натурального числа та знаходження оберненого відносно множення над елементами розширених скінченних полів та загальних лінійних груп над такими полями. Загальна лінійна група – це одна з неабелевих груп, застосування якої вивчають в криптографії у зв'язку з можливою появою квантових комп'ютерів. Користуючись вказаними операціями, в цій програмі реалізовано: протокол Діфі-Хелмана узгодження таємного ключа через відкритий канал зв'язку (як над скінченним полем, так і над загальною лінійною групою над скінченним полем), протокол Стікеля узгодження таємного ключа через відкритий канал зв'язку (над загальною лінійною групою над скінченним полем), узагальнений протокол Ромеро-Лізами узгодження таємного ключа через відкритий канал зв'язку (над загальною лінійною групою над довільним скінченним полем) та узагальнену асиметричну криптосистему Канвал-Алі з неабелевою базовою групою, а власне над загальною лінійною групою над скінченним полем. Програма дозволяє досліджувати особливості відомих та перевірку нових криптографічних примітивів. Проведені для різних значень параметрів випробування програмної реалізації недавно запропонованих у [8, 9] узагальненого протоколу Ромеро-Лізами та узагальненої асиметричної криптосистеми Канвал-Алі підтвердили достовірність цих узагальнень. Програму можна також використати для дослідження роботи примітивів, які з'являться в майбутньому.

На даному етапі дослідження основний наголос було зроблено на підтвердженні достовірності двох недавно запропонованих криптографічних примітивів. Автори не ставили за мету оптимізацію програмного коду з точки зору часу виконання і/або використання ресурсів. Це може бути змістом подальшої роботи.

Список літератури

1.Biletskyi A. Ya., Biletskyi A. A., Kandyba R. Yu. Matrychni analohy protokolu Diffi-Khellmana / Herald of Lviv Polytechnic National University, series "Automation, measurement and control". – 2012. – No 741. – P. 128–133. (in Ukrainian)

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

3.Galbraith S. D. Mathematics of Public Key Cryptography / S. D. Galbraith. – New York: Cambridge University Press, 2012. – 630 p.

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

5.Lizama-Pérez L. A., Romero M. L. Non-Commutative Key Exchange Protocol / Preprints 2021, 2021030716. DOI: https://doi.org/10.20944/preprints202103.0716.v2.

6.Popovych B. R. Kompiuterna perevirka prypushchennia Gao, poviazanoho z otrymanniam elementiv velykoho poriadku v skinchennykh poliakh / Herald of Lviv Polytechnic National University, series "Computer systems and networks". – 2018. – No. 905. – P. 106–110. (in Ukrainian) DOI: https://doi.org/10.23939/csn2018.905.106.

7.Popovych B. R Elementy velykoho multyplikatyvnoho poriadku v rozshyrenykh skinchennykh poliakh na osnovi modyfikovanoho pidkhodu Gao / Scientific journal of Lviv Polytechnic National University "Computer systems and networks". – 2019. – Issue. 1, No 1. – P. 63–68. (in Ukrainian) DOI: https://doi.org/10.23939/csn2019.01.063.

8.Popovych B. R, Popovych R. B. Elementy velykoho poriadku dlia kryptosystem z neabelevymy bazovymy hrupamy / Herald of Khmelnytskyi National University, series "Technical sciences". – 2023. – No 4. – P. 278–285. (in Ukrainian) DOI: https://www.doi.org/10.31891/2307-5732-2023-323-4-278-285.

9.Popovych B. R, Popovych R. B. Uzahalnennia nekomutatyvnoho protokolu uzghodzhennia kliucha / Herald of Khmelnytskyi National University, series "Technical sciences". – 2024. – No 4. – P. 137–141. (in Ukrainian) DOI: https://doi.org/10.31891/2307-5732-2024-339-4-22.

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

11. Vavruk E. Y., Popovych B. R, Popovych R. B. Programna model kodiv Rida-Solomona / Scientific journal of Lviv Polytechnic National University "Computer systems and networks". – 2021. – Issue. 1, No 1. – P. 1–6. (in Ukrainian) DOI: https://doi.org/10.23939/csn2021.01.001.

PROGRAM IMPLEMENTATION OF CRYPTOGRAPHIC PRIMITIVES

***B.R. Popovych*[1,2], *R.B. Popovych*[1]**

[1]Lviv Polytechnic National University
department of specialized computer systems
[2]Lviv National Medical University named after Danylo Halytskyi
department of medical informatics
E-mail: bogdan.r.popovych@lpnu.ua,roman.b.popovych.lpnu.ua

Developed on the C# platform (.NET Framework 5.0), which provides high flexibility in work, a program for performing operations (addition, multiplication, raising to the power of a large natural number, finding the inverse relatively to multiplication) on elements of extended finite fields and general linear groups over such fields. The general linear group is one of the well-known non-Abelian groups, the application of which is actively studied in the field of post-quantum cryptography. Using these operations, a number of cryptographic primitives have been implemented: the well-known Diffie-Hellman, Stickel secret key exchange protocols, and recently proposed generalizations of the Lizama-Romero protocol and the Kanwal-Ali asymmetric cryptosystem. The program allows you to explore the features of known and verify new cryptographic primitives. Using it, the trustiness of the two mentioned new primitives for different values of parameters was confirmed.

Key words: finite field, general linear group, cryptographic primitive