УДК 004.681 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.3.21

Б. Р. ПОПОВИЧ
асистент кафедри медичної інформатики
Львівський національний медичний університет імені Данила Галицького
ORCID: 0000-0001-6259-2361

Р. Б. ПОПОВИЧ
доктор фізико-математичних наук, професор,
професор кафедри спеціалізованих комп'ютерних систем
Національний університет «Львівська політехніка»
ORCID: 0009-0006-0992-0825

ДИСКРЕТНА ЗАДАЧА ПОБУДОВИ ЕЛЕМЕНТІВ ВЕЛИКОГО ПОРЯДКУ В МУЛЬТИПЛІКАТИВНІЙ ГРУПІ СКІНЧЕННОГО ПОЛЯ

Стійкість до зламування низки відомих моделей розв'язання криптографічних задач ґрунтується на обчислювальній складності задачі дискретного логарифму у вибраній групі. Це забезпечується знаходженням у групі елементів великого порядку. Розглянуто різні варіанти розв'язання дискретної задачі побудови елементів великого порядку в мультиплікативній групі розширеного скінченного поля. У випадку, коли можна підбирати всі три параметри, які описують математичну модель такого поля, та многочлен розширення є двочленом, запропоновано підхід для підсилення нижньої межі для порядку елементів.

Цей підхід є комбінаторним за своєю суттю. Використано відомий факт, що степінь розширення є добутком двох величин. Тому із збільшенням однієї з них інша зменшується. Залежно від співвідношення між цими величинами по-різному отримуємо нижню межу для порядку елемента. У першому випадку розглядаємо отримані як степені початкового елемента лінійні вирази, а в другому – нелінійні вирази. Знаходимо оцінку знизу для кількості попарно різних добутків таких виразів. Це і є нижня межа для порядку елемента. Такий підхід не вимагає розкладу кількості елементів групи на прості множники, дає елемент великого порядку та нижню межу для порядку цього елемента в явному вигляді.

Наведено деякі значення кількості елементів початкового поля та умови на степені розширення поля, для яких існують нерозкладні двочлени над цим полем. Отримано обчислювальні дані порівняння відомої та отриманої нижніх меж для порядку елемента розширеного поля для низки значень параметрів, які задають поле.

Ключові слова: *криптографічні задачі, дискретний логарифм, скінченне поле, степінь розширення, порядок елемента, математична модель, нижня межа, комбінаторний підхід.*

B. R. POPOVYCH
Assistant at the Department of Medical Informatics
Lviv National Medical University named after Danylo Halytskyi
ORCID: 0000-0001-6259-2361

R. B. POPOVYCH
Doctor of Physical and Mathematical Sciences, Professor,
Professor at the Department of Specialized Computer Systems
Lviv Polytechnic National University
ORCID: 0009-0006-0992-0825

DISCRETE PROBLEM OF CONSTRUCTING HIGH ORDER ELEMENTS IN MULTIPLICATIVE GROUP OF FINITE FIELD

The resistance to cracking of a number of known models for solving cryptographic problems is based on the computational complexity of the discrete logarithm problem in the chosen group. This is ensured by finding high order elements in the group. Various options for solving the discrete problem of constructing high order elements in the multiplicative group of an extended finite field are considered. In the case when it is possible to choose all three parameters that describe the mathematical model of such a field, and the extension polynomial is a binomial, an approach is proposed to strengthen the lower bound for the order of elements.

This approach is combinatorial in nature. The well known fact that the degree of expansion is the product of two quantities is used. Therefore, as one of them increases, the other decreases. Depending on the relationship between these quantities, we obtain the lower bound for the order of the element in different ways. In the first case, we consider linear expressions obtained as powers of the initial element, and in the second, nonlinear expressions. We find a lower bound for the number of pairwise different products of such expressions. This is the lower bound for the order of the element. The approach does not require the factorization of the number of elements of the group into prims, it gives the element of high order and the lower bound for the order of this element in explicit form.

Some values of the number of elements of the initial field and conditions on the degree of the field extension, for which there exist irreducible binomials over this field, are given. Computational data comparing the known and obtained lower bounds for the order of an element of the extended field for a number of values of the parameters, that define the field, are obtained.

Key words: *cryptographic problems, discrete logarithm, finite field, degree of expansion, order of an element, mathematical model, lower bound, combinatorial approach.*

Постановка проблеми

Відомо три базових задачі криптографії: узгодження таємного ключа через відкритий канал зв'язку; побудова асиметричних криптосистем; цифрове підписування [1]. Математичні моделі розв'язання першої задачі прийнято називати протоколами узгодження таємного ключа. Основна думка полягає в тому, що вибирають якусь групу (алгебраїчну структуру) та певні публічні елементи в ній. Далі випадковим чином утворюють свої приватні дані. Виконують обчислення над публічними та приватними даними, обмінюючись проміжними результатами. Остаточний результат (узгоджений ключ) не проходить через відкритий канал зв'язку.

Стійкість відомих моделей [2–6] до зламування ґрунтується на обчислювальній складності задачі дискретного логарифму у вибраній групі. Це забезпечується знаходженням у групі елементів великого порядку. Для моделей асиметричних криптосистем або цифрового підпису також потрібні елементи великого порядку. Широко використовувані групи: мультиплікативна група скінченного поля [7], загальна лінійна група над скінченним полем. Для отримання елементів великого порядку в загальній лінійній групі над скінченним полем можна використати елементи великого порядку з мультиплікативної групи цього поля [2].

Аналіз останніх досліджень і публікацій

Через F_r позначаємо скінченне поле з r елементів. Мультиплікативна група скінченного поля – це множина $F_r^* = F_r \setminus \{0\}$ його ненульових елементів. Математична модель розширеного скінченного поля має вигляд:

$$F_{q^n} = F_q[x] / f(x),$$

де q – кількість елементів початкового поля, n – степінь розширення, $f(x)$ нерозкладний над F_q многочлен степеня n. Можливі такі варіанти підбирання параметрів у вказаній моделі.

1) числа q та n не можна підбирати: вони довільні (вже задані). Дозволено підбирати лише многочлен розширення з тих міркувань, щоб у розширеному полі отримати елемент великого порядку.

Вказаний многочлен підбираємо так, щоб він був дільником деякого зручного многочлена. Цей зручний многочлен може залежати:

а) лише від одного многочлена $g(x)$ якнайменшого степеня (один степінь свободи) [8] з умовою $f(x)$ ділить $x^{q^m} - g(x)$, де m – найближче більше ціле число до $\log_q n$. Власне підбираємо многочлен $g(x)$;

б) від двох многочленів (два степені свободи) [9] з умовою $f(x)$ ділить $h(x)x^{q^m} - g(x)$. Власне підбираємо два многочлени $g(x), h(x)$ якнайменшого степеня.

2) числа q, n та многочлен розширення можна підбираємо так, щоб у розширеному полі отримати елемент великого порядку.

У цьому разі розглядаємо такі підходи:

а) знайти такі q та n, щоб кількість ненульових елементів розширеного поля $q^n - 1 = uv$, де u – невелике натуральне число, а v – велике просте число. Тоді можна скористатися наслідком із теореми Лагранжа для скінченних груп. Многочлен розширення довільний;

б) параметри q, n вибираємо так, щоб многочлен розширення був нерозкладним двочленом $x^n - a$, тобто $F_{q^n} = F_q[x] / (x^n - a)$. Найкраща відома нижня межа для порядку елемента такого поля дорівнює $5^{\sqrt[3]{n/2}} = 3{,}5873^{\sqrt[3]{n}}$ [10].

Формулювання мети дослідження

Метою роботи є: отримати підсилення нижньої межі для порядку елементів у випадку, коли можна підбирати всі три параметри, які описують математичну модель скінченного поля, та многочлен розширення є двочленом.

Викладення основного матеріалу дослідження

Розглядаємо скінченні поля вигляду $F_{q^n} = F_q[x] / (x^n - a)$. Для них справедлива рівність $x^n = a$. Відомо [10], що двочлен $x^n - a$ нерозкладний над F_q тоді і тільки тоді, коли виконуються такі дві умови: 1) кожен простий дільник числа n ділить порядок e елемента a в F_q^*, але не ділить $(q-1)/e$; 2) якщо n ділиться на 4, то $q-1$ ділиться на 4.

Як розвиток цього результату, маючи число *q*, описано, для яких степенів *n* існують нерозкладні двочлени, а також явно будують елемент *a*. Більш точно, кожен простий дільник числа *n* ділить $q-1$ та якщо *n* ділиться на 4, то $q-1$ ділиться на 4. Коли $q \geq 5$ є непарним, то можна будувати розширення для нескінченної кількості *n*.

Виходячи з описаних умов, в табл. 1 наведено деякі значення $q < 1000$ кількості елементів початкового поля F_q та умови на степені розширення *n*, для яких існують нерозкладні двочлени над цим полем. У цій таблиці *r*, *s*, *t* – довільні невід'ємні цілі числа.

Таблиця 1

Степені розширення n, для яких існують нерозкладні двочлени над Fq

№	*q*	*n*
1	5	2^r
2	7	$2\cdot3^r$
3	9	2^r
4	11	$2\cdot5^r$
5	13	$2^r\cdot3^s$
6	17	2^r
7	19	$2\cdot3^r$
8	23	$2\cdot11^r$
9	25	$2^r\cdot3^s$
10	27	$2\cdot13^r$
11	29	$2^r\cdot7^s$
12	31	$2\cdot3^r\cdot5^s$
13	49	$2^r\cdot3^s$
14	81	$2^r\cdot3^s$

№	*q*	*n*
15	103	$2\cdot3^r\cdot17^s$
16	121	$2^r\cdot5^s\cdot13^t$
17	125	$2^r\cdot31^s$
18	127	$2\cdot3^r\cdot7^s$
19	257	2^r
20	359	$2\cdot179^r$
21	401	$2^r\cdot5^s$
22	521	$2^r\cdot5^s\cdot13^t$
23	601	$2^r\cdot3^s\cdot5^t$
24	625	$2^r\cdot3^s\cdot13^t$
25	743	$2\cdot7^r\cdot53^s$
26	797	$2^r\cdot199^s$
27	881	$2^r\cdot5^s\cdot11^t$
28	937	$2^r\cdot3^s\cdot13^t$

Розглянемо для прикладу рядок 22 табл. 1. У цьому разі *q*=521 − просте число, а $q-1=520$ ділиться на числа 2^3, 5 та 13. Тому степінь розширення *n* може мати як дільник будь-який степінь чисел 2, 5 та 13.

Для підсилення вказаної в попередньому підрозділі відомої нижньої межі для порядку елемента в F_{q^n} нами використано такий відомий результат [10]: *n*=*kl*, де *k* є дільником $q-1$, *l* дорівнює порядку числа *q* за модулем *n* та всі різні степені *q* за модулем *n* можна записати у вигляді $jk+1$ ($j=0,1,...,l-1$). Оскільки добуток чисел *k* та *l* є фіксованим, то із збільшенням одного з цих чисел інше зменшується. Тому залежно від співвідношення між цими числами по-різному отримуємо нижню межу для порядку елемента *x* + *b*, де *b* – ненульовий елемент початкового поля.

Перший можливий випадок: *k*≥*l*

Зрозуміло, що в цьому випадку $k \geq \sqrt{n}$. Оскільки *l* – порядок числа *q* за модулем *n*, то $q^l = 1 \bmod n$, тобто $q^l = 1 + tn$ для деякого цілого числа *t*. Тоді:

$$x^{ql} = x^{tn+1} = (x^n)^t x = a^t x .$$

Елемент $x + b$ $(b \in F_q^*)$ можна розглядати як многочлен першого степеня від *x* (лінійний елемент). З нього послідовним піднесенням до степеня $2^{\sqrt{2l}} \approx 2^{\sqrt{n}} q^l$ утворюємо (з врахуванням початкового елемента) *k* лінійних елементів: $a^{it}x+b$ ($i=0,1,...,k-1$). Число *k* є найменшим натуральним числом, для якого *kt* є дільником $q-1$. Тоді $(k+1)$-й елемент повторює перший елемент (зауважимо, що $a^{q-1}=1$):

$$(x+b)^{qlk} = a^{kt}x+b = x+b ,$$

а всі попередні елементи є попарно різними.

Формуючи добутки, де кожен з цих елементів беремо не більше одного разу, отримуємо попарно різні елементи скінченного поля, бо степені цих добутків не перевищують $k < n$. Таких добутків можна утворити $2^k \geq 2^{\sqrt{n}}$. Таким чином, маємо нижню межу для порядку елемента *x* + *b* рівну $2^{\sqrt{n}}$.

Другий можливий випадок: *l* >*k*.

Як було сказано раніше, степені числа *q* за модулем *n* можна записати у вигляді $jk+1$ ($j=0,1,...,l-1$). Тоді для кожного *j*=0,1,…,*l*−1 знайдеться таке ціле число u_j, що $q^{u_j} \equiv (jk+1) \bmod n$, тобто $q^{u_j} \equiv (jk+1) + r_j n$ для деякого цілого r_j. Значить, виконується рівність

$$x^{q^{u_j}} = x^{jk+1}(x^n)^{r_j} = a^{r_j} x^{jk+1} .$$

Послідовно підносячи елемент $x+b$ до степеня *q*, отримуємо (з врахуванням початкового елемента) *l* нелінійних елементів вигляду $a^{r_j}x^{jk+1}+b, j=0,1,...,l$. Степені цих двочленів дорівнюють $1, k+1, 2k+1, ..., (l-1)k+1$.

Формуючи добутки степеня меншого n, де кожен з l елементів беремо не більше одного разу, отримуємо попарно різні елементи скінченного поля. Виберемо найбільше натуральне число v таке, що $\sum_{i=0}^{v}(ik+1) < n$. Зауважимо, що $k > 2$. Оскільки

$$\sum_{i=0}^{v}(ik+1) = (vk+2)(v+1)/2 < k(v+1)^2/2,$$

то вибираємо v з умови $k(v+1)^2 < 2n$, тобто $v = \sqrt{2n/k} - 1$. Беручи кожен з перших v многочленів не більше одного разу та утворюючи їх добутки, отримуємо різні елементи скінченного поля. Кількість таких добутків дорівнює $2^{v+1} = 2^{\sqrt{2l}}$.

Якщо l близьке до n, то. Залишається не розглянутим теоретично проміжний випадок, коли $l > k$, але l не є близьким до n. Проведені для певних випадків комп'ютерні обчислення показали, що для нього також справедлива вказана нижня межа.

Отже, у цьому випадку також маємо нижню межу для порядку елемента $x + b$ рівну $2^{\sqrt{n}}$. Таким чином, в обидвох розглянутих випадках маємо нижню межу для порядку елемента $x+b$ рівну $2^{\sqrt{n}}$, що є підсиленням відомого результату $5^{\sqrt[3]{n/2}}$.

Далі наведено простий числовий приклад, який ілюструє наведені теоретичні міркування. Беремо початкове скінченне поле з $q = 11$ елементів. Оскільки $q - 1 = 10 = 2 \cdot 5$, то степінь розширення може дорівнювати $2 \cdot 5^r$. Для прикладу беремо $n = 2 \cdot 5^2 = 50$. Вибір a=2 (порядок 2 в F_{11} дорівнює 10) забезпечує, що многочлен $x^{50} - 2$ є нерозкладним над F_{11}. Таким чином, маємо розширене поле $F_{11}[x]/(x^{50} - 2)$.

У ньому справедлива рівність $x^{50} = 2$. Число l=5 є порядком q=11 за модулем n=50. Оскільки $n = kl$, то $k = 10$. Так як $11^5 = 161051 = 1 + 3221 \cdot 50 \equiv 1 \bmod 50$, то $t = 3221 = 21 \bmod 50$ та $a^t = 2^{21} = 2$.

Розглядаємо елемент розширеного поля $x+3$. Послідовним піднесенням цього елемента до степеня 11^5 отримуємо лінійні многочлени $2x+3$, $4x+3$, $8x+3$, $16x+3$, $32x+3$, $64x+3$, $128x+3$, $256x+3$, $512x+3$. Послідовним піднесенням вказаного елемента до степеня 11, отримуємо такі нелінійні многочлени:

$$(x+3)^{11} = x^{11} + 3$$

$$(x^{11}+3)^{11} = x^{121} + 3 = (x^{50})^2 x^{21} + 3 = 4x^{21} + 3$$

$$(4x^{21}+3)^{11} = 4x^{231} + 3 = 4(x^{50})^4 x^{31} + 3 = 4 \cdot 2^4 x^{31} + 3 = 9x^{31} + 3$$

$$(9x^{31}+3)^{11} = 9x^{341} + 3 = 9(x^{50})^6 x^{41} + 3 = 9 \cdot 2^6 x^{41} + 3 = 4x^{41} + 3$$

У табл. 2 наведено обчислювальні дані порівняння відомої та отриманої нижніх меж (в бітах) для порядку елемента $x+b$ поля F_{q^n} для деяких значень q та n.

Таблиця 2

Порівняння відомої та отриманої нижньої межі для різних значень q та n

Кількість елементів поля q	Степінь розширення n	Відома нижня межа	Отримана нижня межа
5	2048	23	45
5	4096	29	64
5	8192	37	90
7	1458	20	38
7	4374	30	66
7	13122	43	114
11	1250	19	35
11	6250	33	79
11	31250	58	176

Висновки

Виконано аналіз математичних моделей скінченних полів з точки зору отримання в них елементів великого порядку. У випадку, коли можна підбирати всі три параметри, які описують математичну модель скінченного поля, та многочлен розширення є двочленом, запропоновано комбінаторний підхід для підсилення нижньої межі для порядку елементів. Такий підхід не вимагає розкладу кількості елементів групи на прості множники, дає елемент великого порядку та нижню межу для порядку цього елемента в явному вигляді.

Наведено деякі значення кількості елементів початкового поля та умови на степені розширення цього поля, для яких існують нерозкладні двочлени над цим полем. Отримано обчислювальні дані порівняння відомої та отриманої нижніх меж для порядку елемента розширеного поля для низки значень параметрів, які задають поле.

Список використаної літератури

1. Galbraith S. D. Mathematics of public key cryptography. New York: Cambridge University Press, 2018. 696 p.

2. Попович Б. Р., Попович Р.°Б. Елементи великого порядку для криптосистем з неабелевими базовими групами. *Вісник Хмельницького національного університету. Серія "Технічні науки"*. 2023. Т. 323, № 4. С. 278–285. DOI: https://www.doi.org/10.31891/2307-5732-2023-323-4-278-285

3. Попович Б. Р., Попович Р. Б. Узагальнення некомутативного протоколу узгодження ключа. *Вісник Хмельницького національного університету. Серія "Технічні науки"*. 2024. Т. 339, № 4. С. 137–141. DOI: https://doi.org/10.31891/2307-5732-2024-339-4-22

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

5. Lizama-Pérez L. A., Romero J. M. L. Non-commutative key exchange protocol. Preprints 2021, 2021030716. DOI: https://doi.org/10.20944/preprints202103.0716.v2

6. 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

7. Dose V., Mercuri P., Pal A., Stirpe C. High order elements in finite fields arising from recursive towers. *Designs, Codes and Cryptography.* 2022. Vol. 90. P. 1347–1368. DOI: https://doi.org/10.1007/s10623-022-01041-3

8. 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, no. 1. P. 71–76. DOI: http://dx.doi.org/10.17654/NT042010071

9. Попович Б.Р. Елементи великого мультиплікативного порядку в розширених скінченних полях на основі модифікованого підходу Гао. *Науковий журнал "Комп'ютерні системи та мережі". Національний університет "Львівська політехніка"*. 2019. Вип. 1, № 1. С. 63–68. DOI: https://doi.org/10.23939/csn2019.01.063

10. Bovdi V., Diene A., Popovych R. Elements of high order in finite fields specified by binomials, *Carpathian Mathematical Publications.* 2022. Vol. 14, no. 1. P. 238–246. DOI: https://doi.org/10.15330/cmp.14.1.238-246

References

1. Galbraith S. D. (2018) Mathematics of public key cryptography. New York: Cambridge University Press. 696 p.

2. Popovych B. R, Popovych R. B. (2023) Elementy velykoho poriadku dlia kryptosystem z neabelevymy bazovymy hrupamy [Elements of high order for cryptosystems with non-abelian platform groups] [in Ukrainian] *Herald of Khmelnytskyi National University. Technical sciences*. 323(4), 278–285. DOI: https://www.doi.org/10.31891/2307-5732-2023-323-4-278-285

3. Popovych B. R, Popovych R. B. (2024) Uzahalnennia nekomutatyvnoho protokolu uzghodzhennia kliucha [Generalizations of non-commutative key exchange protocol] [in Ukrainian] *Herald of Khmelnytskyi National University. Technical sciences*. 339(4), 137–141. DOI: https://doi.org/10.31891/2307-5732-2024-339-4-22

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

5. Lizama-Pérez L. A., Romero J. M. L. (2021) Non-commutative key exchange protocol. Preprints 2021, 2021030716. DOI: https://doi.org/10.20944/preprints202103.0716.v2

6. Ustimenko V. (2021) On computations with double Schubert automaton and stable maps of multivariate cryptography. *Interdisciplinary Studies of Complex Systems*. 19, 18–32. DOI: https://doi.org/10.31392/iscs.2021.19.018

7. Dose V., Mercuri P., Pal A., Stirpe C. (2022) High order elements in finite fields arising from recursive towers. *Designs, Codes and Cryptography.* 90, 1347–1368. DOI: https://doi.org/10.1007/s10623-022-01041-3

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

9. Popovych B. R. (2019) Elementy velykoho multyplikatyvnoho poriadku v rozshyrenykh skinchennykh poliakh na osnovi modyfikovanoho pidkhodu Gao [Elements of high multiplicative order in extended finite fields on a base of modified Gao approach] [in Ukrainian] *Scientific journal of Lviv Polytechnic National University. Computer systems and networks*. 1 (1), 63–68. DOI: https://doi.org/10.23939/csn2019.01.063

10. Bovdi V., Diene A., Popovych R. (2022) Elements of high order in finite fields specified by binomials. *Carpathian Mathematical Publications.* 14 (1), 238–246. DOI: https://doi.org/10.15330/cmp.14.1.238-246

Дата першого надходження рукопису до видання: 25.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025