

Оцінка стійкості криптографічних протоколів заснованих на складності задачі дискретного логарифмування у скінченному полі $GF(p^m)$

Онай М. В.¹, Дичка А. І.²

¹Старший викладач кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет України «Київський Політехнічний Інститут», пр. Перемоги, 37, м. Київ, Україна, onay_nikolay_kpi@ukr.net

²Студент кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет України «Київський Політехнічний Інститут», пр. Перемоги, 37, м. Київ, Україна, andriydychka@gmail.com

Анотація – Розглянуто математичні операції на яких базується криптостійкість відомих протоколів асиметричної криптографії. Показано актуальність дослідження методів дискретного логарифмування як у скінченних полях, так і на еліптичних кривих, що визначені над полями Галуа. Проведені дослідження методів дискретного логарифмування на серверній ЕОМ. На основі проведених експериментальних досліджень сформульовано рекомендацію для вибору методу дискретного логарифмування у полі $GF(p^m)$ та на еліптичній кривій над цим полем. Визначено напрямки подальших досліджень методів дискретного логарифмування.

Ключові слова: еліптична криптографія, еліптична крива, поле Галуа, скінченне поле, криптостійкість, одностороння функція, дискретне логарифмування.

Evaluation of cryptographic protocols resistance based on the complexity of the discrete logarithm problem in the finite field $GF(p^m)$

Onai M. V.¹, Dychka A. I.²

¹Senior Lecturer of the Department of Computer Systems Software, National Technical University of Ukraine "Kyiv Polytechnic Institute", Peremogy Av., 37, Kyiv, Ukraine, onay_nikolay_kpi@ukr.net

²Student of the Department of Computer Systems Software, National Technical University of Ukraine "Kyiv Polytechnic Institute", Peremogy Av., 37, Kyiv, Ukraine, andriydychka@gmail.com

Abstract - Were considered the mathematical operations, which underlie the asymmetric protocols of cryptographic resistance. Showing the research relevance of discrete logarithm methods in finite fields and also on elliptic curves defined over Galois fields. The research of discrete logarithm methods was made on the server computer. Based on the experimental studies were formulated the recommendations for choosing the discrete logarithm method in the field $GF(p^m)$ and on the elliptical curve defined on it. Were defined the directions for further research in methods of discrete logarithm.

Keywords: elliptic cryptography, elliptic curve, finite field, strong cryptography, one-way function, discrete logarithm.

ВСТУП

Криптостійкість схеми обміну ключами Діффі-Хелмана, схеми електронного підпису Ель-Гамала, криптосистеми Месі-Омура та стандарту цифрового підпису DSA ґрунтується на односторонній функції дискретного піднесення до степеня [1-3]. Односторонньою називають функцію яка досить швидко обчислюється для заданого діапазону параметрів, але обернена до неї функція не може бути обчислена за прийнятний час наявними обчислювальними засобами. Прикладом такої функції є дискретне піднесення до степеня, тобто піднесення до степеня [3] на дискретній множині елементів. В якості дискретної множини елементів у

сучасній асиметричній криптографії зазвичай виступають елементи скінченного поля $GF(p)$ або $GF(p^m)$, а також елементи групи точок еліптичної кривої, що визначена над одним із зазначених полів [1-3].

ПОСТАНОВКА ЗАДАЧІ

На даний момент є широкоживаними та достатньо вивченими криптосистеми [1-5], що базуються на скінченному полі $GF(p)$ або $GF(2^m)$. Це пояснюється високою швидкістю виконання математичних операцій в цих полях, що виконуються при шифруванні та дешифруванні

даних, але в той же час використання таких полів порівняно з $GF(p^m)$, де $p \geq 3$, при однаковій довжині ключа, зменшує криптостійкість даної системи. Таким чином зі зростанням обчислювальної потужності ЕОМ є актуальною задача дослідження та оцінки криптостійкості систем, що ґрунтуються на складності задачі дискретного логарифмування у скінченному полі $GF(p^m)$ та алгебраїчних структурах, що визначені над ним.

СКІНЧЕННІ АЛГЕБРАЇЧНІ СТРУКТУРИ

Існує дві найбільш вживані [4] форми подання елементів поля $GF(p^m)$:

- степеневе:
 - у вигляді степеня примітивного елемента α поля з невід'ємним показником;
 - у вигляді степеня примітивного елемента α поля з від'ємним показником;
- многочленне.

Обидва способи подання елементів поля $GF(p^m)$ є тотожними, але при многочленному поданні є ускладненою операція множення, піднесення до степеня та пошуку мультиплікативно оберненого елемента, а при степеневому поданні неможливо (без побудови таблиць передобчислень) виконати операцію додавання двох елементів поля, тому зазвичай використовують многочленне подання елементів поля $GF(p^m)$.

Еліптична крива над довільним полем це множина точок, що задовольняють рівнянню [1]

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

разом з точкою на нескінченності. Всі коефіцієнти даного рівняння є елементами поля над яким визначена крива.

Еліптична крива над полем $GF(p)$ задається наступним рівнянням:

$$y^2 = x^3 + ax + b$$

де $p \neq 2, 3$; $4a^3 + 27b^2 \neq 0$ – умова несингулярності кривої та $a, b \in GF(p)$.

Для поля $GF(2^m)$ розрізняють два види еліптичних кривих:

- суперсингулярні

$$y^2 + ay = x^3 + bx + c$$

де $a, b, c \in GF(2^m)$;

- несуперсингулярні

$$y^2 +axy = x^3 + bx + c$$

де $a, b, c \in GF(2^m)$.

У криптографічних системах використовують не суперсингулярні криві, оскільки суперсингулярні криві дозволяють легко обчислювати їх порядок, що спричиняє низьку криптостійкість таких кривих.

ЗАДАЧА ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ ТА МЕТОДИ ЇЇ РОЗВ'ЯЗАННЯ

Математично дискретний логарифм це ціле число x , що є розв'язком рівняння [4-5]

$$a^x = b$$

де a та b елементи скінченної групи. Якщо необхідно обчислити дискретний логарифм від елементів поля $GF(p^m)$, то елементи a та b належать полю $GF(p^m)$. При використанні многочленного подання елементів поля $GF(p^m)$ всі математичні операції над елементами даного поля необхідно виконувати за модулем незвідного многочлена степеня m .

Оскільки точки еліптичної кривої утворюють адитивну групу, то задача дискретного логарифмування на еліптичній кривій формується таким чином: знайти ціле число x таке, що

$$b = x \cdot a$$

де a та b є точками еліптичної кривої, що визначена над скінченним полем. Математичні операції над координатами точок виконуються за правилами визначеними у відповідному скінченному полі.

Для розв'язання задачі дискретного логарифмування використовують метод Шенкса, метод Поліга-Хелмена та λ -метод Поларда.

Метод Шенкса [6] заснований на поданні шуканого показника степеня x у вигляді $x = i \cdot m - j$, де $m = \lceil \sqrt{n} \rceil + 1$, n – порядок циклічної групи. Таке подання тотожне наступному:

$$a^{im} = b \cdot a^j.$$

Згідно даного методу потрібно спочатку обчислити набір значень a^{im} , $i = 1..m$ та зберігти отримані значення у структурі даних, що дозволяє організувати ефективний пошук. Далі необхідно виконати перебір всіх можливих значень $b \cdot a^j$ починаючи з $j = 1$ до моменту отримання $b \cdot a^j$ такого, що дорівнює одному зі значень у побудованій таблиці, звідки легко обчислити шуканий дискретний логарифм.

При реалізації методу Поліга-Хелмана [7] на початку роботи алгоритму необхідно знайти розкладення на прості множники порядку n циклічної групи в якій відбувається логарифмування. Далі потрібно знайти значення логарифму у кожній підгрупі простого порядку та

визначити дискретний логарифм у початковій групі за китайською теоремою про остачі.

Досить ефективним для розв'язання задачі дискретного логарифму є λ -метод Поларда [8], ще його називають «kangaroo-method». Суть цього методу полягає у тому, щоб запустити два детерміновані випадкові блукання і перше почати від числа – чий дискретний логарифм ми шукаємо, друге від іншого числа, чий дискретний логарифм ми знаємо. Якщо ці два блукання зійдуться, то можна буде легко обчислити шуканий логарифм.

Розглянуті методи застосовують як для дискретного логарифмування в полі $GF(p^m)$ так і для логарифмування на еліптичній кривій, що визначена над полем $GF(p^m)$.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

Для проведення експериментальних досліджень було обрано систему комп'ютерної математики Sage [9], реалізованої на мові програмування Python, що видається з ліцензією GNU GPL. Дана система дозволяє виконувати операції над елементами скінченних полів та еліптичними кривими. Для заміру часу використовувалась стандартна функція мови Python – *timeit*, яка за рахунок багатократного запуску дозволяє нівелювати вплив різноманітних процесів, що виконуються операційною системою та підвищити репрезентативність отриманих даних.

Експериментальні дослідження проводились на віртуальній машині з операційною системою *Ubuntu 14.4* з такими технічними характеристиками CPU *VCPU 4x3.3Ghz*, оперативна пам'ять *13Gb DDR3*, що запущена на сервері з такими параметрами: CPU *Intel Xeon E3-1230 V2 4x3.3Ghz*, оперативна пам'ять *16Gb DDR3*.

З метою проведення дослідження було сформовано множину з 5 пар випадкових операндів для кожного зі скінченних полів, що було обрано для дослідження з подальшим усередненням отриманих часових показників. У даному дослідженні обрано поля Галуа характеристики 2, 3 та 5, показник степеня для поля з характеристикою 2 обирався таким, щоб бітова довжина операндів не перевищувала 18, 22, 27 та 32 біта, а для характеристики 3 та 5 таким чином, щоб кількість елементів цих полів була співрозмірною з відповідною кількістю елементів полів з характеристикою 2.

Для дискретного логарифмування на еліптичній кривій для кожного скінченного поля над яким визначена еліптична крива було сформовано 5 трійок (еліптична крива із заданими параметрами та дві точки еліптичної кривої, які є операндами при логарифмуванні) з подальшим усередненням результатів.

Згідно описаної методики побудовано табл. 1 та табл. 2.

Таблиця 1 – Час роботи алгоритмів дискретного логарифмування у скінченному полі, мс

Поле	Метод Шенкса	Метод Поліга-Хелмана	λ -метод Поларда
$GF(2^{18})$	1,56	0,37	4,34
$GF(2^{22})$	6,35	0,49	15,12
$GF(2^{27})$	37,44	2,01	66,08
$GF(2^{32})$	210,74	1,26	464,57
$GF(3^{11})$	57,24	9,09	186,63
$GF(3^{14})$	336,77	9,05	973,13
$GF(3^{17})$	2146,43	43,17	4954,75
$GF(3^{18})$	3138,23	6,43	10248,25
$GF(5^8)$	86,70	2,78	165,95
$GF(5^{10})$	392,63	4,28	1281,17
$GF(5^{12})$	959,37	514,29	2515,85
$GF(5^{14})$	5246,80	2821,12	14152,89

Таблиця 2 – Час роботи алгоритмів дискретного логарифмування на еліптичній кривій, що визначена над скінченним полем, мс

Поле	Метод Шенкса	Метод Поліга-Хелмана	λ -метод Поларда
$GF(2^{18})$	91,58	15,33	200,27
$GF(2^{22})$	76,87	16,52	207,54
$GF(2^{27})$	1947,40	22,46	2850,81
$GF(2^{32})$	5493,18	68,82	16499,10
$GF(3^{11})$	58,47	33,32	160,09
$GF(3^{14})$	290,63	21,44	636,55
$GF(3^{17})$	1936,10	117,56	4057,84
$GF(3^{20})$	1838,75	42,44	3621,93
$GF(5^8)$	55,16	14,46	140,34
$GF(5^{10})$	251,50	19,76	582,47
$GF(5^{12})$	161,11	27,03	442,52
$GF(5^{14})$	12495,24	72,21	23043,24

ВИСНОВКИ

З отриманих експериментальних результатів видно, що найкращі результати показує метод Поліга-Хелмана як для дискретного логарифмування у скінченному полі $GF(p^m)$ так і для дискретного логарифмування на еліптичній кривій, що визначена над полем $GF(p^m)$.

В той же час звертає на себе увагу той факт, що при однаковій кількості елементів, логарифмування у полі з більшою характеристикою займає суттєво

більший час. З огляду на це є доцільним використання у криптографічних додатках скінченних полів з характеристикою $p > 2$. Окрім цього проведене дослідження підтвердило доцільність використання еліптичних кривих у системах захисту інформації, оскільки їх застосування дозволяє значно збільшити час дискретного логарифмування не змінюючи скінченне поле. Подальші дослідження слід зосередити на побудові паралельних алгоритмів реалізації методу Поліга-Хелмана та λ -методу Поларда.

ЛІТЕРАТУРА REFERENCES

- [1] Darrel Hankerson, Alfred Menezes, Scott Vanstone Guide to Elliptic Curve Cryptography – 2004, Springer – Verlag New York Inc. – 205 p
- [2] N.Koblitz, Elliptic Curve Cryptosystems [Text]/ Neal Koblitz//Mathematics of Computation – Volume 48 – Number 177 – January 1987 – pp. 203-209
- [3] Cetin Kaya Cok, Cryptographic Engineering – Springer Science+Business Media, LLC 2009 – 171 p
- [4] Василенко О. Н., Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. – 178 с.
- [5] Richard Crandall, Prime Numbers, a computational perspective – 2005 Springer Science+Business Media, Inc – 604 p
- [6] D. Shanks, The infrastructure of a real quadratic field and its applications [Text] / Proceedings of the Number Theory Conference (Boulder, CO, 1972) – pp. 217–224 – , Univ. Colorado, Boulder, 1972.
- [7] S. Pohlig, M. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and it's cryptographic significance [Text] / S. Pohlig, M. Hellman, // IEEE Transactions on Information Theory –Volume:24 – Issue: 1 – pp 106-110
- [8] Pollard J.M., Monte Carlo Methods for Index Computation (mod p) [Text]/ J.M.Pollard / Mathematics of Computation – Volume 32 – number 143 – July 1978, – pp 918-924
- [9] SageMath ,free open-source mathematics software system licensed under the GPL – Режим доступу: <http://www.sagemath.org/> – (15.02.2016)