НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет прикладної математики

Кафедра програмного забезпечення комп'ютерних систем

"На правах рукопису"
УДК 004.021

«До захисту допущено»
Науковий керівник кафедри

_____ І.А. Дичка
(підпис)

"___" _____ 2017 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 8.05010302 "Інженерія програмного забезпечення"

на тему: МЕТОД ОБЧИСЛЕННЯ ПОРЯДКУ ЕЛІПТИЧНОЇ КРИВОЇ НАД ПОЛЕМ $GF(2^m)$

Виконав: студент 6 курсу, групи КП-52м
Ничепорук Олександр Анатолійович _____
(підпис)

Науковий керівник доц., доц., к.т.н. Жабіна В.В. _____
(підпис)

Рецензент доц., к.т.н., доц. Ткаченко В.В. _____
(підпис)

Рецензент доц., к.т.н., доц. Орлова М.М. _____
(підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2017

РЕФЕРАТ

Актуальність теми. На сьогоднішній день, у рамках сучасної криптографічної науки, розглядається два види еліптичних кривих над скінченним полем. До першого виду, відносять еліптичні криві над Z_p – кільцем лишків за модулем простого числа. Другий вид – еліптичні криві над полем $GF(2^m)$ – бінарним скінченним полем.

Еліптичні криві над полем $GF(2^m)$ мають перевагу: елементи поля $GF(2^m)$ легко можуть бути представлені у вигляді n-розрядних двійкових слів, що дозволяє збільшити швидкість апаратної реалізації алгоритмів на еліптичній кривій.

Усі математичні операції на еліптичних кривих над скінченним полем виконуються за законами скінченного поля, над яким побудована еліптична крива. Тобто, для обчислення, наприклад, суми двох точок кривої E над кільцем лишків Z_p, всі операції проводяться за модулем числа p.

У зв'язку з можливістю появи квантового комп'ютера існує загроза злому існуючих криптосистем квантовим алгоритмом Шора, що потребує створення нових криптосистем. Оскільки криптостійкість залежить від порядку еліптичної кривої, задача обчислення порядку є важливим етапом пошуку криптостійких еліптичних кривих.

Для того, щоб забезпечити криптостійкість відносно квантового алгоритму Шора, потрібно вибирати еліптичні криві над полем $GF(2^m)$, де $m \in [1021;1031]$. Вирішення задачі обчислення порядку для таких кривих найшвидшим із існуючих методів – методом Харлі – відбувається за 150 секунд.

Оскільки на практиці потрібно перебирати багато випадкових кривих, серед яких лише 5-10% можна буде використати для подальшого аналізу, то прискорення методів обчислення порядку еліптичних кривих є актуальною науково-практичною задачею.

Об’єктом дослідження є процес знаходження порядку еліптичної кривої над полем $GF(2^m)$.

Предметом дослідження є методи обчислення порядку еліптичної кривої над полем $GF(2^m)$.

Мета роботи: розроблення методу обчислення порядку еліптичної кривої над полем $GF(2^m)$.

Для досягнення поставленої мети у межах роботи необхідно виконати такі завдання:

- проаналізувати існуючи методи та їх модифікації, виявити сильні та слабкі сторони;
- розробити метод обчислення порядку еліптичної кривої над полем;
- розробити програмний комплекс для дослідження та аналізу розробленого та існуючих методів.

Методи дослідження. В якості методів дослідження застосовувалися: теорія алгоритмів, теорія складності обчислень; апарат вищої алгебри і теорії чисел; комп'ютерне моделювання.

Наукова новизна роботи полягає в наступному:

1. Удосконалено метод Харлі на етапі визначення кореня рівняння Артіна-Шреєра, що дає приріст швидкодії для задачі обчислення порядку еліптичної кривої над полем $GF(2^m)$ на 1.3%.
2. Запропоновано модифікований метод обчислення порядку еліптичної кривої над полем $GF(2^m)$, який є комбінацією удосконаленого методу Харлі та методу Сато-Ск’єрна-Тагучі і відрізняється від методу Сато-Ск’єрна-Тагучі тим, що замість підняття Техмюллера використовується модифікований ітераційний метод Ньютона, та від методу Харлі тим, що відновлення сліду ендоморфізма Фробеніуса обчислюється за методом нормування Сато замість арифметико-геометричного

методу. Розроблений метод дає приріст швидкодії на 7.2% порівняно з методом Харлі та у 4.8 рази порівняно з методом Сато-Ск'єрна-Тагучі.

Практична цінність дослідження полягає в тому, що розроблений метод обчислення порядку еліптичної кривої може використовуватися для пошуку нових криптостійких кривих. У даній дисертаційній роботі наведено комплексний аналіз існуючих методів обчислення порядку еліптичної кривої над полем $GF(2^m)$ та продемонстровано, що розроблений метод працює швидше. Отримані результати можуть бути використані розробниками як один з етапів методу генерування еліптичної кривої, для алгоритмів створення електронного цифрового підпису та шифрування.

Апробація роботи. Основні положення і результати роботи були представлені та обговорювались на IX науковій конференції магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2017 (Київ, 19-21 квітня 2017р.) та опубліковані у збірнику тез за результатами конференції.

Структура та обсяг роботи. Магістерська дисертація складається з переліку умовних скорочень, вступу, п'ятьох розділів, висновків та додатків.

У вступі надано загальну характеристику роботи, виконано оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень.

У першому розділі розглянуто загальні поняття криптографії, характеристики еліптичних кривих у полі $GF(2^m)$, описані математичні моделі еліптичної криптографії, операції над точками кривої, підходи до вирішення задачі обчислення порядку канонічних еліптичних кривих, порядку кривих над розширеннями скінченних полів, визначено зв'язок між порядком еліптичної кривої та рівнем криптографічної стійкості.

У другому розділі докладніше розглянуто види еліптичних кривих, їхні вразливості, існуючі методи обчислення порядку на еліптичних кривих, проблеми даної задачі. Продемонстровані приклади вирішення даної задачі існуючими методами. Описані методи обчислення порядку еліптичної кривої над $GF(2^m)$ – Сато, Сато-Ск'єрна-Тагучі та Харлі – їхні модифікації, алгоритми, що реалізують дані методи.

У третьому розділі описані основні принципи розробленого методу, запропоновано засоби реалізації; обґрунтовано вибір структури даних, наведено діаграми класів; наведена реалізація основних допоміжних функцій, необхідних для обчислень, як окремої складової методу.

У четвертому розділі наведено результати експериментальних досліджень, розглянуто особливості програмної реалізації, проведено аналіз розробленого програмного комплексу, описані вимоги до технічних засобів. Показано, що розроблений метод дає приріст у швидкодії на 7.2% порівняно з методом Харлі та у 4.8 рази порівняно з методом Сато-Ск'єрна-Тагучі.

У п'ятому розділі наведено опис стартап-проекту, його сильних та слабких сторін. Наведено характеристику потенційних клієнтів, фактори загроз та можливостей. Проведено аналіз конкуренції та обґрунтування конкурентоспроможності.

У висновках проаналізовано отримані результати роботи.

У додатках наведено фрагменти програмної реалізації розробленого методу та комплексу для аналізу існуючих методів, презентація та копії графічних матеріалів.

Магістерська дисертація виконана на 97 аркушах, містить 3 додатки та посилання на список використаних літературних джерел з 23 найменувань. У роботі наведено 20 рисунків та 7 таблиць.

Ключові слова: порядок еліптичної кривої $GF(2^m)$, ендоморфізм Фробеніуса, p-адичне кільце, метод Сато, метод Харлі.

ABSTRACT

Actuality of theme. Today within the modern cryptographic science, two types of elliptic curves over a finite field are considered. The elliptic curves of the first type are assigned over a residue ring Z_q by the modulus of a prime number. The elliptic curves of the second type are above the binary finite field $GF(2^m)$.

The elliptic curves over $GF(2^m)$ have an advantage, the elements over $GF(2^m)$ can easily be represented as *n*-bit binary words, which allows to increase the speed of hardware implementation of algorithms on an elliptic curve.

All mathematical operations on elliptic curves over a finite field are executed according to the group law over the field that an elliptic curve is constructed. For instance, to calculate the sum of two points of the curve E over the residue ring Z_p, all operations are reduced by modulo *p*.

Now there is a threat of hacking existing cryptosystems by quantum Shor's algorithm when quantum computer will be released that requires the creation of new cryptosystems. Since cryptostability depends on the order of the elliptic curve, the task of counting points is an exciting stage in the search of curves, that provide stability.

In order to provide cryptostability from the quantum Shor's algorithm, it is necessary to choose elliptic curves over $GF(2^m)$, where $1021 < m < 1031$. Solving the problem of computing order for such curves by the fastest of the existing methods – the Harley method – are performed in 150 seconds.

Since in practice it is necessary to take many random curves and filter it, the improvement of the methods for point counting of elliptic curves will allow to generate a new elliptic curve faster.

The object of the research is the process of point counting of an elliptic curve over $GF(2^m)$

The subject of the research is the methods for point counting of an elliptic curve over $GF(2^m)$.

Research objective: to develop a method for point counting of an elliptic curve over $GF(2^m)$.

In order to achieve the goal within the scope of work, the following tasks must be performed:

• analyze existing methods and their modifications, identify advantages and disadvantages;

• develop a method for point counting of an elliptic curve over a field;

• develop a software package for research and analysis of developed and existing methods.

Research methods. Such research methods have been used: theory of algorithms, the theory of complexity of calculations; the device of higher algebra and the theory of numbers; computer simulation.

The scientific novelty consists of the following:

1. The Harley method is improved at the stage of determining the root of the Artin-Schreier equation, which gives an increase in the speed for the problem of point counting of elliptic curve over $GF(2^m)$ by 1.3%.

2. A modified method for the point counting of elliptic curve over $GF(2^m)$, which is a combination of the improved Harley method and the Satoh-Skjernaa-Taguchi method, and differs from the Satoh-Skjernaa-Taguchi method by the fact that the modified General Newton's Lift method is used instead of the Techmuller lift, and from Harley method, that the restoration of the Frobenius track is calculated by the Satoh rationing method instead of the Arithmetic-Geometric method. The developed method gives an increase in performance of 7.2% compared to the Harley method and in 4.8 times compared to the Satoh-Skjernaa-Taguchi method.

The practical value of the study is that the developed method for point counting of an elliptic curve can be used to find new curves. A complex analysis of existing methods for calculating the order of an elliptic curve over $GF(2^m)$ is presented in this thesis and it is demonstrated that the developed method works faster. The results can be used by developers as one of the stages of the curve generation method or for algorithms for creating an electronic digital signature.

Approbation. The main positions and results of work were presented and discussed at the IX scientific conference of masters and postgraduates "Applied Mathematics and Computing", PMK-2017 (Kyiv, 19-21th of April, 2017) and published in the abstract following the results of the conference.

Structure and content of the thesis. The master's dissertation consists of a list of conditional abbreviations, an introduction, five chapters, conclusions and appendixes.

The introduction gives a general description of the work, an assessment of the current state of the problem is performed, the relevance of the research direction is substantiated.

In the first chapter is considered the general concepts of cryptogram, the characteristics of an elliptic curves over $GF(2^m)$, described the mathematical models of elliptic cryptography, operations on the points of the curve, approaches to solving the problem of point counting of canonical elliptic curves, the order of curves over extensions of finite fields. Defined the connection between the order of the elliptic curve and the level of cryptographic stability.

In the second chapter we consider in more detail the types of elliptic curves, their vulnerabilities, the existing methods for point counting of elliptic curves. There are examples of solutions to this problem demonstrated using existing methods. Methods for point counting of an elliptic curve over $GF(2^m)$ such Satoh, Satoh-Skjernaa-Taguchi and Harley, and their modifications, algorithms that implement these methods.

The third chapter describes the main principles of the developed method, the means of implementation are proposed; the data structure is substantiated, the class diagrams are given; the implementation of the main helpful functions necessary for computation of the method is given.

The fourth chapter presents the results of experimental studies, features of the program implementation, analyzed the developed software complex, described the requirements for the technical means. It is shown that the developed method gives a growth rate of 7.2% in comparison with the Harley method and 4.8 times in comparison with the Satoh-Skjernaa-Taguchi method.

In the fifth chapter the startup description, its strengths and weaknesses are presented. Also, the characteristic leads, opportunities and threats factors are presented. Analysis of competition and competitiveness study are executed.

In the conclusions the results of the work are presented.

The appendixes show fragments of the software implementation of the developed method and complex for analysis of existing methods, presentation and copy of graphic materials.

The master's dissertation is performed on 97 sheets, contains 3 appendices and a link to the list of used literary sources with 23 titles. There are 20 pictures and 7 tables in the work.

Key words: order of elliptic curve $GF(2^m)$, Frobenius endorphism, p-adic ring, Satoh method, Harley method.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Алексеева О.В., Болотов А.А., Гашков С.Б., Лиссук М., Гашков С.Б., Лиссук М. «О методах вычисления кратных для точек эллиптических кривых над полями Галуа»// Вестник Московского энергетического института. — 2000. — № 4. — С. 97–100.
2. Долгов В.И., Лисицкая И.В. Теория групп и колец: Конспект лекцій з дисципліни ″Спеціальні розділи математики″. — Х.: ХТУРЭ, 2000.
3. Завало С.Т. и др. Алгебра и теория чисел. — К.: Вища шк., 1980. — Ч.2. — 402 с.
4. Ілясова О.Є. Порівняльний аналіз методів обчислення порядку еліптичної кривої при генерації параметрів криптосистем на еліптичних кривих / О.Є. Ілясова // Радіоелектронні і комп’ютерні системи. — 2007. — № 7 (26). — С. 129-133.
5. Хлебородов Д. С. Быстрые алгоритмы вычисления преобразований на основе эллиптиче- ских кривых с предварительными вычислениями // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». — 2015. — № 3. — С. 65-78.
6. Beth Y., Schaefer F. Non Supersingular Elliptic Curves for Public Key Cryptosystems. — Copyring © 1998, Springer-Verlag.
7. Blake, G. Seroussi, Smart N. Elliptic Curves in Cryptography. Cambridge University Press, 1999. London Mathe-matical Society Lecture Note Series 265.
8. Coppersmith D. Fast evaluation of logarithms in fields of characteristic two // IEEE Trans. Inform. Theory. — 1984. — IT 30. — P. 587-594.
9. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Transactions on Information Theory. — November 1976. — V.IT-22, n.6. — P. 644-654.

10. Elkies E. Elliptic and modular curves over finite fields and related computational issues / E. Elkies // Computational perspectives in number theory. — 1998. — P. 21-27.
11. Joux A. A one round protocol for tripartite Diffie-Hellman // W. Bosma, editor, Algorithmic Number Theory, IV-th Symposium (ANTS IV), Lecture Notes in Computer Science 1838. — Springer-Verlag, 2000. — P. 385-394.
12. Koblitz N. Constructing Elliptic Curve Cryptosystems in Characteristic 2. — Springer-Verlag, 1998.
13. Koblitz N. Eliptic Curve Cryptosystems // Mathematics of Computation. — 1987. — V. 48, № 177. — P. 203-209.
14. Lenstra H.W. Factoring integers with elliptic curves // Ann. Of Vath, (2) 126 (1987). — H. 674-745.
15. Lersier R. Counting the number of points on an elliptic curve over finite fields: strategies and performense / R. Lersier // Proc. Eurocrypt. — 1995. — P. 101-116.
16. Menezes A., Okamoto T., Vanstone S. Reducing Elliptic Curve Logarithms to a Finite Field // IEEE Trans. Info. Theory. — 1993. — 39. — P. 1603-1646.
17. Miller V.C. Use og Elliptic Curve in Cryptography // Cryptology: Proceedings of Crypto 85, Springer LNCS 218, 1986. — P. 417-426.
18. Sakai R., Ohgishi K., Kasahara M. Cryptosystems based on pairing // Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, January 2000.
19. Satoh T. Canonical lifting of elliptic curves and *p*-adic point counting. (theoretical background) / T. Satoh // Department of Mathematics, Faculty of Science, Saitame University. — 2001. — P. 1-21.
20. Silverman J. The Arithmetic of Elliptic Curves. — New York: Springer-Verlag, 1986.
21. Washington L.C. Elliptic Curves-Number Theory and Cryptography / L.C. Washington. — Chapman &Hall/CRC, edition, 2008.

22. Ганзя Р.С. Оцінка обчислювальної складності методів підрахунку кількості точок на еліптичній кривій / Р.С. Ганзя // Системи обробки інформації. — 2016. — Вип. 8. — С. 92-99. — Режим доступу: http://nbuv.gov.ua/UJRN/soi_2016_8_22.
23. Ничепорук О.А. Модифікований метод множення точки еліптичної кривої над полем $GF(2^m)$ з використанням швидкого перетворення Фур'є. — IX наукова конференція магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2017. — Київ, 2017.