UDC 681.3.06.

ANALYSIS AND DEVELOPMENT OF EXISTING ALGORITHMS FOR SOLVING THE DISCRETE LOGARITHM PROBLEM

G. Vostrov, Yu. Bezrukova

Odessa national polytechnic university

Abstract. *In this article we have described the object of the discrete logarithm problem and spelled out the ways of the discrete logarithm theory implementation. Also there is the analysis of some methods by indication of the controversial points and adding missing steps. In this work, we suggest the alternative method that requires less computational complexity but at the same moment it has a disadvantage in meaning of program realization. So, it must be compared to the current method to provide the complex estimate.*

Key words: *discrete logarithm, finite field, primary root, cryptography, public key, electronic digital signature.*

Introduction

The discrete logarithm problem is the fundamental mathematical problem and in an applied sense it is the basis of the public key cryptography. The object of the discrete logarithm problem was proposed for determination of a public key cryptography in the Diffie-Hellman work. This subsequently became applicable as a basis of a better part of cryptography protocols and also as a fundamental aspect for the common electronic digital signature algorithm [1].

The basis of such systems is a computational complexity of some revert functions. In this case the discrete logarithm problem is a revert function to an exponential one. This asymmetric can be compared to the asymmetric of computational complexity of multiplication and factorization that is also used in the information security systems and cryptography. Finding the result of an exponential function is quite simple but counting the result of the discrete logarithm problem can be compared to the complexity of a factorization algorithm.

Now there is another one problem in an applied sense which means that the document can be signed by two or even more people who use their own electronic digital signatures. In this case there should be noted the possibility of rival opinions of all the participants. It means that we should develop some exactly new protocols of electronic digital signature and authentication systems to prevent the intruding.

We have a base e when counting simple logarithm that let us count it quite easy with the arbitrary accuracy. In the situation of a discrete logarithm problem there is no any base to count it as simple as in the case of logarithms in the fields of real numbers. There are a stack of methods that could be used to find a solution of a discrete logarithm problem but all of them are described with an exponential or a subexponential complexity. There is a point of view that the general and effective algorithm is still unknown [2].

Algorithms for the discrete logarithm problem solving

The discrete logarithm problem can be considered in the fields F_p^*, in multiplicative groups of residue classes $(Z/mZ)*$, in groups of points of elliptic curves [4] and in general in arbitrary groups [7]. Despite that fact that there is some isomorphism between fields and multiplicative groups of residues classes, the fields theory is wider than the theory of multiplicative groups of residues classes. In this work we analyze the algorithm that was described in [2, 3]. The task is to find the value of x, that can be described by the following equation

$$a \equiv t^x \pmod{q} \qquad (1)$$

where a, t and q - are the inputted values. These values can be presented as numbers and also as polynomials. The second case makes the theory much more complicated. The discrete logarithm can also be described as an index $x = ind_t a$. The fact of the existence of the algorithm for calculating a discrete logarithm remains an open question [2], it is not proved whether this problem has a solution or the general algorithm does not exist. The computational complexity of finding a discrete logarithm is also an open question.

Firstly, it should be noted that all the values a, t and q can be presented by any of a real number. We have to prove that the algorithm for all of the values exists and this algorithm lets us check whether the equation (1) has a solution. If the algorithm exists the solution must be found in a finite count of iterations. More over, the complexity of the algorithm will be described in this work and also the fact that it could not be simplified will be proved. The aim of this article is to provide a complex analysis of all the current algorithms and their computation complexities. Also there will be described some ways of algorithms improving.

In this part of work we will thoroughly analyze the algorithm from [2, 3]. The author noted that q is a prime number and t is a primary root is just to simplify the algorithm. The last notice is not correct at all and the notice about primary root just make the algorithm easier to complete. The requirement of q to be a prime number is not necessary even when talking about applied aspects of the discrete logarithm theory. If we follow the idea of the Diffie-Hellman protocol, which is the base of all other key exchange protocols in cryptography and information security systems, then it is not specified what conditions numerical values must satisfy. It should be noted that if q is not a prime number, there are some cases when t can be described as a relatively prime number to q or vice versa. The last case makes the task much more difficult.

In the following works we will analyze the case when q and t are real numbers. At this work we analyzing the following case: suppose, that q - is a prime number and t -is a primary root. Let it be proved that if $q-1$ is a “smooth” (for multipliers) number, the algorithm does not let to calculate the discrete logarithm more easily than if $q-1$ is not a «smooth» (for multipliers) number.

The algorithm from [2, 3] as it noted was developed for cases when all values of p are not extremely big numbers. They are the multipliers of $(q-1)$, where $(q-1)=\prod_{i=0}^{k-1} p_i$. We will give the full analyzing of this algorithm in this work.

We propose the definition of “smooth” numbers for such values of q in the sense of the factorization. So, q is a “smooth” number if all of the multipliers of $(q-1)$ could be approximated linearly. Due to the logarithmic law of the distribution of primes $\pi(x)=\frac{x}{\ln(x)}$. It means that multipliers cannot be represented in a linear form. The count of such numbers is very small, more over it will take an exponential computational complexity to find them.

So, using the theory of discrete logarithms can be complicated due to finding “smooth” numbers. If we will not require q to be a prime number, we will also use real numbers. They can be found more quickly but in the case of real numbers there are no guarantees that the algorithm works, because it could be so that the number does not have a primary root.

So, now we will describe the case when $(q-1)=\prod_{i=0}^{k-1} p_i$ - are not big multipliers which could be represented in a linear form and q - is a prime number. As it noted, the first requirement is a base of the algorithm. There can be some doubts due to the fact that a value size is not connected to the algorithmic complexity. To prove it we should analyze the steps of the algorithm.

The first step of the algorithm from [2,3] is counting all of the roots of the p degree for each of p due to the following formula

$$r_{p,j}=t^{\frac{j(q-1)}{p}} \quad \text{where} \quad j=\overline{0,p-1}.$$

It was proposed to use the method of re-calculating square values. It should be noted that there can be loosing of some intermediate values due to this method.

If we consider numbers that are usually used in cryptography, then the value of q consists of more than 200-250 numerical characters. So, the table that is created on condition of small values of p will not contain numbers of much smaller dimensions. It raises the question of the requirements for storage and further processing of the data obtained in the table. Also there is a disadvantage due to the fact that the table can not be used twice or more if we change the value of q . Otherwise if q and t are fixed, we can use table any times without re-counting, but this case is rarely used in applied aspects.

Next steps need the Chinese theorem of the remnants. We give the formulation of the theorem.

Suppose that - are the positive pairwise relatively prime modules and .

Let also be given corresponding deductions $r_{p,j}$. Then the system of equations and inequality $x \equiv x_i (\operatorname{mod} p_i),\ 0 \le x \le M$ has the only solution.

for their numerical values, but also for indicators of degree γ. The character of the indicators values is not defined and can vary from 1 to several hundreds. The dimension of the numbers can be compared to 10^{200}, such values are used in cryptography.

The next case to be considered is when all of $\gamma_p = 1$, then the algorithm can be improved and it will have fewer steps than in the cases of the degree $\gamma_p > 1$. In this case we can reduce the number of computations by avoiding the algorithm step that uses an expression (2).

Here is an algorithm that is based on the iterative process.

Suppose that q is a prime number and t is a primary root. The iterative process has the following structure

$$x_{n+1} \equiv t^{x_n} (\text{mod } q) \qquad (3)$$

Suppose that $x_0 = 1$. We obtain a set $\{z_0 = 1, z_1 = t(\text{mod } q), ..., z_{q-1} = 1\}$ as the result of the process due to the small Fermat theorem. If it noted that t - is a primary root, the length of a cycle $l = q$.

The next step is a search that is similar to the search from the algorithm from [2, 3]. We will compare the value of a to the values of the set elements and also suppose that x_i is defined by the index of a concrete element z_k. The last step also uses the Chinese theorem on the remnants.

Thus, the general case method was given. It solves the problem when at least one of the indicators of degree $\gamma_p > 1$. Also there was given its simplification, provided that the degrees of power are equal to 1, as well as the method that uses the iterative process.

The algorithm from [2, 3] consists of the following steps :

1) Counting the values of the table $r_{p,j} = t^{\frac{j(q-1)}{p}}$ where $j = \overline{0, p-1}$, $q - 1 = \prod_{i=0}^{k} p_i$;
2) Counting $a_i^{(q-1)/p^{i+1}} = t^{(x_1 + x_{i+1}p + ...)(q-1)/p} = t^{x_1(q-1)/p} = r_{p.x_i}$, $q - 1 = \prod_{i=0}^{k} p_i$, $i = \overline{0, \gamma - 1}$;
3) Using the Chinese theorem on the remnants;

The iterative algorithm has some advantages compared to the algorithm from [2, 3], but there are also some disadvantages in means of the realization. In practical using we have to store and to process a large array that defines the resulting set. More over there is a problem of effective search.

Other algorithm of discrete logarithm problem solving was described in the work [6]. There is also a cases when the discrete logarithm task is trivial. This case described in [6]. It is a situation in which we have to count the value of the discrete logarithm in the additive group $G = Z / nZ$ with the primary root $g = 1$; in this case there is no such big computational complexities required.

Although the algorithms for calculating the discrete logarithm can be compared to the factorization algorithms by complexities, one can confidently say that the computational complexity of the discrete logarithm problem solving is more complicated because its steps predict the decomposition of the number into simple factors in themselves. Sometimes factorization helps to achieve so-called smaller cases, for which calculations will generally be in order of less complexity, but for some methods, even those that work with "smooth" numbers, the work with a subgroup can be the same complex in terms of computational complexity as well as work with a complete group [6].

Most of the algorithms for solving the problem of discrete logarithm has one general problem, which is associated with a huge load of the machine memory, which makes the problem of theirs automation. Therefore, when developing new algorithms or improving existing ones it is necessary to take into account the fact that the data that is required during the calculations must be stored and processed. It requires a large amount of memory and the definition of the optimal types of data for storage and further processing, or, perhaps, the most optimal is to recalculate data as needed. This issue needs to be solved by comparing machine costs for storage and computing. These problems are also very important because all the methods are only the mathematical theory at this stage and they should be confirmed by practical results.

Conclusion

As it was noted earlier, the problem of calculating a discrete logarithm is not only purely mathematical, but is applied in nature. The variety of problems and issues that arise in the process of studying the theory of discrete logarithms is given in [7]. In addition to the applied aspects that will be discussed in more detail below, [7] there explains the theoretical possibilities of using the theory of discrete logarithms in hash constructions as well as in search encryption systems. These questions constitute the newly discovered problems of mathematics and cryptography. A separate topic for analysis is the calculation of a discrete logarithm on elliptic curves. The complexity of such algorithms is theoretically evaluated as lower than those considered in this paper.

The widest use of the discrete logarithm theory is related to information security systems. It also can be used in authentication systems. Electronic digital signature systems are being built on this theory and also they takes into account the computational complexity of the discrete logarithm problem.

As it was noted earlier, the most interest and complicated at the same time case is when there are some electronic digital signatures in the document. It is a common case in economic obligations, where each of the participants has its own interests. The improvement of a key exchange protocols must be considered in such a case due to the fact that someone may want to change the original document context. This situation will be analyzed and described in details in future work.

Most of the algorithms for electronic digital signature and key exchange protocols have similar foundations. The basis of keys exchange protocols is the Diffie-Hellman protocol. The stability of this algorithm is provided by calculating the value, which in essence is a discrete logarithm. This value is a $g^{ab}(\text{mod } p)$, where g and p - are jointly defined numbers that are known for both the participants, and also b and a - are their secret keys that must be kept in a secret.

Electronic digital signature systems are also based on the same principles. That is, if the problem of the discrete logarithm was solved, and the exact and universal algorithm was automated, most cryptographic systems would be forced to change the basic algorithms because of their instability.

References

1. Diffie, F., Hellman, M. E., (1976), New directions in cryptography, IEEE Trans. Info. Theory, IT22(6):644–654 p.
2. Manin, Yu., Panchishkin, A., (2009), Introduction to the modern theory of numbers, [Vvedenie v sovremennuyu teoriyu chisel] - Moscow: MSC-MO, 552 p.
3. Koblitz, N. (2001), Course of number theory and cryptography, Moscow: Scientific publishing house PTA, 254 p.
4. Crandall, R., Pomerance, K., (2011), Prime numbers: cryptographic and computational aspects, Transl. from English / Ed. and with a preface by V. Chubarikova, - Moscow: URSS: Book House "LIBROKOM", 664 p.
5. Nesterenko, Y., (2001), Discrete logarithm. Introduction to cryptography, [Discretniy logarifm. Vvedenie v kriptografiyu] – SPB.: Pitersburg, – 288 c.
6. Pomerance, C., (2008) Algorithmic Number Theory, MSRI Publication, Volume 44, – 12 p.
7. https://crypto.stackexchange.com/questions/tagged/discrete-logarithm
8. Vostrov, G., Opyata, R., (2017), Effectivity of calculation the structure of dynamic processes of primes forming, - ELTECS, – 7 p.

АНАЛІЗ ТА РОЗВИТОК ІСНУЮЧИХ АЛГОРИТМІВ РОЗВ’ЯЗАННЯ ПРОБЛЕМИ ДИСКРЕТНОГО ЛОГАРИФМА

Востров Г. М., Безрукова Ю. С.

Одеський національний політехнічний університет, Одеса, Україна

Анотація: *У даній роботі описана постановка та сутність задачі дискретного логарифмування, що є на даному етапі важливою математичною проблемою, а в прикладному аспекті – основою криптографії з відкритим ключем. Ця задача є базою для створення сеансового ключа у роботі Діффі-Хеллмана та багатьох криптографічних протоколах. У даній роботі прикладна сутність задачі дискретного логарифмування аналізується з точки зору створення алгоритмів електронного цифрового підпису, а зокрема описується проблема створення двох і більше електронних цифрових підписів на одному документі, що потребує не лише створення ефективних алгоритмів підпису, а й забезпечення надійності протоколів обміну ключами. У роботі описується класична математична постановка задачі дискретного логарифмування та проводиться детальний аналіз існуючого метода вирішення цієї проблеми. У ході аналізу позначаються недоліки запропонованого алгоритму та обґрунтування випадків, при яких цей алгоритм не може вирішити проблему дискретного логарифмування. Для більш детального дослідження проводиться аналіз алгоритму при різних вхідних значеннях. На основі цього було доведено, що при деяких значеннях алгоритм не має змоги вирішити проблему дискретного* *логарифмування. Цей факт дає змогу ставити під сумнів саме існування алгоритму вирішення задачі дискретного логарифмування для загального випадка. Більш того було доведено, що основні етапи алгоритму самі по собі складають задачі експоненційної складності. У роботі був запропонований алгоритм, що будується на основі певного ітераційного процесу. При зазначених умовах, що накладаються на вхідні данні, цей алгоритм має менше кроків та спрощенні обчислення у порівнянні з існуючим алгоритмом. Окрім цього, необхідно зазначити, що запропонований алгоритм має певні недоліки, що полягають у складнощах комп’ютерної реалізації. При практичному використанні такого методу необхідно зберігати та обробляти великий масив даних, окрім цього постає проблема створення ефективного методу пошуку конкретного числа у таких масивах даних. Окрім того, у роботі наведені сучасні проблеми, у яких запропоновано використовувати метод дискретного логарифмування.*

Ключові слова: *дискретний логарифм, кінцеве поле, первісний корінь, криптографія, відкритий ключ, електронний цифровий підпис.*

АНАЛИЗ И РАЗВИТИЕ СУЩЕСТВУЮЩИХ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ ДИСКРЕТНОГО ЛОГАРИФМИРИФМА

Востров Г. Н., Безрукова Ю. С.

Одесский национальный политехнический университет

Аннотация: *В данной работе описана постановка и сущность задачи дискретного логарифмирования, которая на данном этапе является важной математической проблемой, а в прикладном аспекте – основой криптографии с открытым ключом. В ходе анализа существующих алгоритмов были выяснены их неточности и приведены спорные моменты. Кроме того был предложен собственный алгоритм. Для более детального анализа приведены недостатки математических моделей и реализаций данных алгоритмов.*

Ключевые слова: *дискретный логарифм, конечное поле, первообразный корень, криптография, открытый ключ, электронная цифровая подпись.*

Received 20.03.201

George Vostrov, Ph. D. of Technical Sciences, Associate Professor of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: vostrov@gmail.com, mob. +380503168776

Востров Георгій Миколайович, кандидат технічних наук, доцент кафедри прикладної математики та інформаційних технологій Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: vostrov@gmail.com, тел. +380503168776

ORCID ID: 0000-0003-3856-5392

Yulia Bezrukova, Student of the Department of Applied Mathematics and Information Technologies, Odessa National Polytechnic University. Shevchenko ave., 1, Odessa, Ukraine.
E-mail: bezrukovajulia961@gmail.com, mob. +380500341872

Безрукова Юлія Сергіївна, студент кафедри прикладної математики та інформаційних технологій, Одеського національного політехнічного університету. Проспект Шевченко, 1, Одеса, Україна.
E-mail: bezrukovajulia961@gmail.com, тел. +380500341872

ORCID ID: 0000-0002-0577-2216