DYNAMIC METHODS OF SIGNATURES AUTHENTICITY PROTECTION BASED ON A DISCRETE LOGARITHM IN FINANCIAL LIABILITIES

G. Vostrov *Ph. D., Associate Professor*,
Y. Bezrukova

Odessa National Polytechnic University.

Abstract: In this article we have analyzed the problem of electronic signatures authentication the construction of which is based on the theory of a discrete logarithm. This problem is considered in the field of financial documents, but it can be extended independently to other industries. In the course of the work it was proved that the standard protocols and algorithms for key distribution and information protection are incorrect for the case of the existence of several electronic signatures in one financial document. Specific methods for improving the cryptographic stability of the algorithm based on discrete logarithm by selecting the number of a specific class are given.

Key words: electronic digital signature, open key, discrete logarithm, secret key, financial liabilities.

The cognitive nature of decision-making in the financing of science-intensive and costly projects is the fundamental basis for developing the modern world economy. Stock markets are instable as an investment tool for such purposes. Monitoring of the financial direct investment effectiveness is poorly developed in our time. Finances in the form of currency asset are withdraw away from the country then they are placed into the biggest international banks and became almost unacceptable for their relocation control. The analysis showed that relocation and direct investments are always accompanied by financial documents where the obligations of all participants are reflected.

On this assumption there is a need of instrument which could uniquely identify all the participants of a deal. More over, such an instrument should be possessed of opportunity to confirm the integrity and also it should guarantee that the document could not be corrected by one of participant. It is important because all the participants could have competing interests.

All of those requirements are being implemented in the electronic digital signature. The liabilities of all the participants are signing by electronic digital signatures which means that the participants are authorized and that all of changes in the document are known for each of participant.

Some fact should be detected while developing an electronic digital signature algorithm. First of all, it is necessary to take into account the fact that as the projects and their realizations develop, the interests of the parties involved may come into conflict. That is, it is necessary to ensure access to the document and its direct adjustment only if all the signatories agree to this. Such situations raise the issue of protecting the interests of all participants in the process.

There is a scheme of an electronic digital signature with only one participant in [2]. At the moment, a great interest for the study direct for the option of signing the document by a group of participants. This means that the document is stapled with two or more electronic signatures, each of which must comply with the above requirements. This situation is not standard and does not allow using of existing key exchange protocols, such as Diffie-Hellman. It also requires the construction of special cryptographic hash functions due to the fact that each of the participants, pursuing the goal of providing additional protection, can encode the document in various ways. Such a problem exists because the value of the result of a hash function over the document is one of the parameters of the standard algorithm for computing the electronic signature.

A variant when the document is authenticated by two electronic signatures was investigated in details. It is assumed that a document can be accessed, for example, for a co-ordinated adjustment if and only if both sides open their signatures. It has been established that with the increasing number of signatures, the complexity of their consistent disclosure increases, subject to the use of modified protocols.

One of the main mathematical devices in information security and authentication systems is the theory of discrete logarithms. The stability of the Diffie-Hellman protocol and many algorithms of electronic digital signature is based on the intractability of the discrete logarithm problem.

In [2] the notion and algorithm for calculating the discrete logarithm was given. However, all existing algorithms have significant drawbacks. Firstly, they are defined for a special category of numbers. In [3, 4] a formal definition of such numbers called "uniform" is given. Secondly, each of the algorithms has a feature: with increasing the value of a prime number, the complexity of the algorithm exponentially grows.

We have established that none of the algorithms determine the situation of unsolvability of the problem of a discrete logarithm. It is known that the value of the discrete logarithm x which is defined for a reversible residue $a(\mathrm{mod}\, q)$ according to the formula $a \equiv t^x(\mathrm{mod}\, q)$ where $x \in [0, q-1]$, and a, t, q - known quantities. In the course of the work, it was established that the value t must be a primitive root. Otherwise, the iteration cycle length $l_t q$ will be less than the value $(q-1)$. This means that while performing the final step of defining components x_i in the formula $x \equiv x_0 + x_1 p + \ldots + x_{\gamma-1} p^{\gamma-1} (\mathrm{mod}\ p^{\gamma})$ according to the algorithm in [2], we get that the line may not contain a value with the index which determines the value x_i.

Thus, in the absence of additional conditions imposed on numbers-known parameters when solving the problem of discrete logarithm, this problem may turn out to be unsolvable.

Proceeding from the above justification, we obtain that for each value q it is necessary to find its set of primitive roots $\{t_1 \ldots\ldots t_k\}$. When the algorithm for calculating the discrete logarithm begins, the check for belonging to a given value t to the set

$\{t_1.....t_k\}$ will give an answer to the question of the possibility of applying the existing algorithm for specified parameters.

This justification determines the need for solving one more problem. This is the task of determining the whole set $\{t_1.....t_k\}$. Also an important issue remains the possibility of generalizing the algorithm for the case when t does not belong to the set $\{t_1.....t_k\}$.

The algorithm which was given in [2] can be used many times even when changing the values t,q in the sense that the values of prime divisors p will not. Consequently, with the same t the table will have the same components. The main changes will be only on the stage of determining the components $x \equiv x_0 + x_1 p + ... + x_{\gamma-1} p^{\gamma-1} (\mathrm{mod}\ p^{\gamma})$ for prime numbers p due to the change in the value a.

In the course of the work, a strategy for selecting simple or composite numbers to form the authentication of electronic signatures based on the discrete logarithm theory was developed.

In financial and economic systems one of the main criteria for choosing a number is the amount of loss due to unauthorized access to the text of the document.

It was proved that for the algorithm of the discrete logarithm, regardless of the area of the generated document, to ensure cryptographic stability it makes sense to choose numbers from the class P_2, which has the following structure $p_* = 2 \cdot p + 1$.

Using the numbers of this class, as indicated in [3], it is possible to significantly improve the robustness of the algorithm with respect to unauthorized access, but the definition of numbers that belong to a particular class requires the construction of a special hash function.

References:

1. Diffie, F., Hellman, M.E. New directions in cryptography [Text], - IEEE Trans. Info. Theory, IT-22(6):644-654, 1976.
2. Vostrov, G., Bezrukova, Y. Modeling of dynamic data protection systems based on a theory of a discrete logarithm [Text], - ELTECS – 2017.
3. Vostrov, G., Bezrukova, Y. Calculation the discrete logarithm in contemporary cryptography [Text], - ELIT – 2017/.
4. Vostrov, G., Opyata R. Effectivity of calculation the structure of dynamic processes of primes forming, - ELTECS, 2017. – 7 p.
5. Balan AS A conceptual adaptive model of the information-analytical system for investment decisions / O.S. Balan // Економічні інновації: Зб. scientific. etc. – Odessa, 2013. – Vip. 52. – P. 30-35.
6. Sokolovskaya Z.M. Expert systems in economic research: [monograph] / Z.M. Sokolovskaya – Odessa: Astroprint, 2005. – 240 p.Lingur L. N., Iesina O. G. The information security software in business //Економіка: реалії часу. – 2013. – №. 5. – С. 175-180.