Parallel implementation of algorithm for creating and verifying digital signature based on elliptic curves

P T Burtseva, L I Zelenina, L E Khaymina, E S Khaymin, I M Zashikhina
Northern (Arctic) Federal University named after M.V. Lomonosova, Arkhangelsk, Naberezhnaya Sev. Dviny str., 17, 163002, Russia
E-mail l.zelenina@narfu.ru

Abstract. The article discusses the use of parallel data processing in the implementation in the C++ programming language using the Visual Studio integrated development environment of an algorithm for information protection and authentication. Data processing is based on the method of discrete logarithm in a group of points of an elliptic curve. The studied case has been developed as Cost Optimization Program for an Oil and Gas Company and includes creating an Optimization Map information system. A part of the system is a module generating and verifying a digital signature. Due to the use of parallel data processing and the ECDSA algorithm for digital signature creation, oil and gas company will be able to increase its working efficiency and information security.

Keywords: Information security, Electronic signature, Discrete logarithm, ECDSA algorithm, Parallel data processing, Company’s work optimization

1. Introduction
Today, companies all around the globe strive to enhance their business potential and staff efficiency. Company managers, data security and R&D specialists, employ information technologies of the latest generation to ensure working processes’ congruence, enterprise’s safety and swift personnel reactions. One of the solutions is the use of a digital signature as a means of verifying and protecting information [1, 2, 3]. In Russia, to legalize the procedure of a digital signature use, a new standard for the electronic signature has been adopted, and the Law on Digital Signature has been issued. Western companies and regulatory agencies like Institute of Electrical and Electronics Engineers and National Institute of Standards and Technology (USA) adopted a new standard for digital signature ECDSA (Elliptic Curve Digital Signature Algorithm), based on the use of elliptic curves.

The digital signature of files or e-mail messages is performed following cryptographic algorithms that employ asymmetric keys, such as the “secret key”, used for the signature itself, and the “public” key, used to verify another person’s signature. The most famous schemes for creating an electronic digital signature are schemes like DSA, RSA, ElGamal, Rabin, Schnorr, Diffie-Lamport [4, 5]. A special advantage of DSA scheme, which represents elliptic curve cryptosystems is that they provide significantly higher security with equal labor intensity, or, conversely, significantly lower labor intensity with equal resistance as compared to the other algorithms [6, 7]. That is why DSA or ECDSA has attracted special attention of the researches worldwide [8, 9, 10, 11].

For a signature to be solid, it needs to be based on a hard-to-calculate mathematical problem. One of such problems is the problem of discrete logarithm in a group of points of an elliptic curve. Application
of methods of parallel data processing to an algorithm that implements labor-intensive stages of discrete logarithm methods allow for more efficient use of multiprocessor computing systems in the process of creating and verifying a digital signature [12]. The discrete logarithm problem, which determines the stability of cryptography algorithms, is complex; its solution requires rather large computing power. The larger the size of the initial data, the higher the complexity of the problem. Parallel algorithms that ensure effective use of multiprocessor computing systems in the process of creating an electronic signature can successfully implement time-consuming steps of mathematical methods of discrete logarithm [13, 14].

The study examines the case of parallel implementation of an algorithm for creating a digital signature using discrete logarithm in a group of points of an elliptic curve and its application to protect the data of optimization maps in an information system to balance the expenses of an oil and gas company. In this paper, we are studying the functionality of signing and verifying an electronic signature. We intend to present the results of an optimization map development in order to investigate the potential of cost optimization program in multiprocessor computing systems.

2. Information protection by means of digital signature, discrete logarithm problem and elliptic curve

One of the means of protecting information is a digital signature. This is the requisite of an electronic document obtained as a result of cryptographic information transformation, which allows checking the integrity of information in an electronic document. According to the GOST R 34.10-2018, it represents a string of bits resulting from the signature generation process. The discrete logarithm is a mathematical problem that uses an asymmetric encryption scheme. Asymmetric encryption scheme provides a basis for a digital signature. Its idea is based on the high computational complexity of the function inversion $F_\_ (n, a) (x) = a \^{x} \mod \,(n)$.

An elliptic curve $E$ over a field $F$ is the set of points $(x; y)$ whose coordinates belong to the field and satisfy the following cubic equation:

$y^2 + a_1 \,xy + 1a_3 \,y = x^3 + a_2 \,x^2 + a_4 \,x + a_6, \,a_i \in F$.

Elliptic curves are used as a basis for constructing cryptosystems. Since the initial standardization of Elliptic Curve Cryptography, significant progress has been made in terms of the efficiency and security of curves. Some elliptic curves allow faster calculations in modular arithmetic. As part of the implementation of the parallel algorithm, the Weierstrass elliptic curve P-256 can be used to create an electronic signature and its verification. This curve provides an adequate level of security and software efficiency.

3. Cost optimization program and optimization activity map

For the practical application of the algorithm, the information system Cost Optimization Program for an Oil and Gas Company was chosen. The software aims at the improvement of costs’ regulation and increasing the efficiency of oil production processes. Within the Cost Optimization Program for an Oil and Gas Company information system, the section Optimization Map has been developed.

Optimization Map (OM) is a plan for finding and putting into operation the optimal solution in order to increase the efficiency of oil production processes.

The life cycle of Optimization Map is divided into 4 main blocks:

- Creation of Optimization Map, its correction;
- Negotiation of Optimization Map. At this stage, the map is signed using the digital signature;
- Approval and implementation of Optimization Map;
- Completion of the work cycle.

The matching block in the system is divided into several stages. At each stage, the official will work only on the part of the map which belongs to their field of responsibility.
To implement the module for creating and verifying a digital signature, the ECDSA algorithm was chosen. The algorithm is based on the complexity of solving the discrete logarithm problem in a group of points of an elliptic curve.

Figure 2. Scheme for signing and verifying a digital signature using the ECDSA algorithm

The following components are involved in the process of signing an electronic document (Figure 3):
• Database that stores records of the document is signed by the user. It includes the hash-sum of the signature, the date and information about the person who signed it. The rest of the system data is also stored in the database.

• Information system of cost optimization for an oil and gas company. In this system, the Optimization Map is edited and approved. The information system records information into the database. It also provides users with functionality for working and approving documents.

• Digital Signature Module is a dynamic package connected to the Creatio CRM system, written in the C++ programming language, which implements the functionality of signing and verifying a digital signature in the process of the Optimization Map approval.

• CRM Creatio is a CRM system serving as a basis for the information system of Cost Optimization Program for an Oil and Gas Company development [15].

4. Parallel implementation of the algorithm for creating a digital signature
As part of the development of an information system for cost optimization, the Service Creatio CRM solution is used. To implement the parallel algorithm, the Open Multi-Processing (OpenMP) library in C++ in the integrated environment Visual Studio 2019 was chosen.

4.1 Description of the module that implements the functions of creating and authenticating electronic signature
For the processes of generating and verifying a digital signature, the signer must have a means of cryptographic protection of information containing public and private keys Q (xq; yp). The private key is stored on a cryptographic security facility, while the public key is known to all participants in the workflow and is stored in the database. As it is described in GOST R 34.10-2018, the variables used in the scheme for verifying and signing an electronic signature are:

- $V_i$ - the set of all binary vectors of length 1 bits;
- $V^*$ - the set of all binary vectors of arbitrary finite length;
- $M$ - signed initial data, $M \in V$;
- $h(M)$ - hash-sum of the original data, represented as binary vectors of length 1 bits
- $\alpha$ - coefficient of the binary vector of the hash sum $h$;
- $q$ - the order of the cyclic subgroup of the group of points of an elliptic curve;
- $P$ - point of the elliptic curve of order $q$;

Figure 3. Diagram of Cost Optimization Program for an Oil and Gas Company system’s components
\( r \) and \( s \) are the values of the digital signature;
\( \nu \) - electronic signature parameter;
\( d \) - the value of the signature private key;
\( Q \) - public key of the signature;
\( \xi = (r \parallel s) \) – a concatenation of two binary vectors \( r \parallel s \), corresponding to the values of the electronic signature \( r \) and \( s \).

To obtain the values \( r \) and \( s \) of the digital signature for the signed initial data on the set of all binary vectors of arbitrary finite length (\( M \in V^* \)), the algorithm for generating a digital signature is performed (view Figure 4). The input parameters of this process are the private signature key \( d \) and the signed initial data \( M \); the calculated result is a digital signature. The method of parallel data processing is used to calculate the point of the elliptic curve and determine the value of the digital signature.

![Figure 4. Diagram of the sequence of a digital signature generation](image)

When verifying the digital signature \( \xi \) under the data \( M \), the input parameters are the signed data \( M \), the electronic signature \( \xi \) and the public key of the signature \( Q \). The calculated result is the validity or unreliability of the signature. In this case, parallel data processing is used to calculate the coefficients determining the point of the elliptic curve. The sequence diagram of digital signature verification is shown in Figure 5.
System interface
The section register is a list of entries for the Optimization Map block with brief information on each card.

To go to the map of a specific event one has to select its title.
The *Optimization Map* is divided into several blocks: Basic information, Calculation, Economic efficiency, etc. A definite company manager signs one of the blocks.

Each block is negotiated separately. Users who need to negotiate a certain block of *Optimization Map* have access to the buttons “Agree” and “Reject”. These buttons enable them to place their digital signature. After clicking the “Approve” button, a modal window with the confirmation of the *Optimization Map* approval is displayed.

5. Conclusion
In this article, we have presented the results of developing *Optimization Map* section as a part of *The Cost Optimization Program for an Oil and Gas Company* information system. During the development process, we investigated the most efficient way for an oil and gas company’s productivity. The developed *Optimization Map* system consists of repeating stages. One of the stages includes...
Optimization Map’s verification with a digital signature. Optimization map builds on the module that enables signing and verifying a digital signature. In this case, digital signature creation has been accessed with the use of the ECDSA algorithm. The chosen algorithm depends on the complexity of solving the discrete logarithm problem in a group of points of an elliptic curve. The method of parallel data processing has been used to calculate the point of the elliptic curve and determine the value of the digital signature.

The improved performance of a company is associated with the distribution of functions and responsibilities among its staff. In the presented scheme, a separate company’s manager will take responsibility for a specific stage of the Optimization Map information system. The advantages of the present study are connected with the reduced work time of the company’s employees and boosted potential of their activities. This has become possible due to the Optimization Map information system developed with the use of parallel data processing and the ECDSA algorithm for digital signature creation.

References
[1] Davidson A 2018 Electronic signatures. 10.1017/cbo9781316182796.016.
[2] Cano M D & Cañavate-Sanchez A 2020 Preserving Data Privacy in the Internet of Medical Things Using Dual Signature ECDSA. Security and Communication Networks. 1-9. 10.1155/2020/4960964.
[3] Bohm N & Mason S 2019 Electronic signatures and reliance. Amicus Curiae. pp. 2-6. 10.14296/ac.v2017i110.5033.
[4] Aleshnikov S I & Gorbachev A A 2019 Methods of Algebraic Curves over finite fields in Public Key Cryptography and Coding Theory. Nauka. Society. Defense. 1 (18). 10.24411/2311-1763-2019-10179
[5] Komarova A V, Menshchikov A A & Korobeinikov A G 2017 Analysis and comparison of electronic digital signature algorithms. GOST R. 34.10-1994, GOST R 34.10-2001 and GOST R 34.10-2012. In: Cybersecurity Issues. 1 (19). 10.21581/2311-3456-2017-1-51-56
[6] Lamba S & Sharma M 2013 An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA) pp. 179-183. 10.1109/ICMIRA.2013.41.
[7] Filat O & Yemelianenko T 2020 Implementing Elliptic Cryptography to Create a Digital Signature. 10.36074/05.06.2020.v3.30.
[8] Toradmalle D, Singh R, Shastri H, Naik N & Panchidi V 2018 Prominence Of ECDSA Over RSA Digital Signature Algorithm. pp. 253-257. 10.1109/I-SMAC.2018.8653689.
[9] Rybalov A N 2018 On the Generic Complexity of the Discrete Logarithm Problem in Point Groups of Elliptic Curves Over Finite Fields. Application. https://doi.org/10.17223/2226308X/11/41
[10] Jin H, He D & Jianhua Ch 2010 An Identity-Based Digital Signature From ECDSA. Education Technology and Computer Science, International Workshop pp. 627-630. 10.1109/ETCS.2010.159.
[11] Mehibel N & Hamadouche M 2019 A New Enhancement of Elliptic Curve Digital Signature Algorithm. Journal of Discrete Mathematical Sciences and Cryptography 23. 1-15. 10.1080/09720529.2019.1615673
[12] Trobec R & Kosec G 2015 Parallel Implementation. 10.1007/978-3-319-17073-2_8.
[13] Zhang J & Chen L Q 2009 An Improved Algorithm For Discrete Logarithm Problem chapter 2 pp 658-661. 10.1109/ESIAT.2009.457.
[14] Saxena S & Kishore N 2017 PRDSA: Effective Parallel Digital Signature Algorithm for GPUs. International Journal of Wireless and Microwave Technologies. 7. 14-21. 10.5815/ijwmt.2017.05.02.
[15] CRM-system Creatio. Accessed online: https://www.terrasoft.ru/page.crm-products/ [14.06.20].