Non-profit joint stock company

"L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY "

**(**NJSC "L.N. Gumilyov ENU")

|  |  |
| --- | --- |
| UDC 004.9  IRSTI 81.96.00  № state registration 0121РК00560  Inventory number. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | APPROVED  Member of the Management Board - Vice-Rector for Science, Commercialization and Internationalization  NJSC "L.N. Gumilyov ENU")  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ G. Merzadinova  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2021 г. |

stamp

REPORT

ABOUT RESEARCH WORK

AP09559249 «RESEARCH AND DEVELOPMENT OF METHODS FOR THE SECURE USE OF EXTERNAL SERVERS TO SOLVE COMPUTATIONALLY-COMPLEX PROBLEMS WITH SECRET PARAMETERS»

(final)

|  |  |  |
| --- | --- | --- |
| Project manager,  Ph.D. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ye.Seitkulov |  |

signature, date

Nur-Sultan 2021

**LIST OF PERFORMERS**

|  |  |  |
| --- | --- | --- |
| Project manager,  Ph.D., Associate Professor, Director of the IS&C Institute,  L.N. Gumilyov ENU | signature, date | Seitkulov Ye.N.  (abstract, introduction, all sections, conclusion) |
| Researcher,  1st year doctoral student on special "Information Security",  L.N. Gumilyov ENU | signature, date | Yergalieva B.B.  (1, list of sources used, appendices A, B) |
| Normocontroller | signature, date | Moldahmetova A.E. |

**ABSTRACT**

Report 25 p., 1 book., 24 refer., 2 append.

INFORMATION SECURITY, SECURE OUTSOURCING, CLIENT-SERVER INTERACTION, BIG DATA, COMPUTATIONALLY- COMPLEX PROBLEMS

The object of the research is linear programming problems with secret parameters, problems of finding the extremum of a function with secret parameters, problems of finding the value of an analytical function on a secret argument.

Goal and tasks of the project for 2021:

The goal of the project is to research and develop methods for the safe use of external servers to solve computationally-complex problems with secret parameters.

Tasks:

Develop new methods and algorithms for the safe use of external ones when solving:

- linear programming problems with secret parameters;

- the problem of finding the extremum of a function with secret parameters;

- the problem of finding the value of an analytical function on a secret argument.

Scope: information security.

Predictive assumptions about the development of the research object: the results of the work will serve as a source for further analysis and research in the development of methods for the safe outsourcing of computationally -complex tasks with secret parameters.

Within the framework of this small grant for 2021, 1 article was published in a foreign journal with a percentile in the Scopus database of 47, as well as 1 more article was submitted to the same journal. 2 reports were made at an international conference.

The research work was attended by 2 researchers, one of whom is a 1st year doctoral student in the specialty "Information Security".

**CONTENT**

|  |  |
| --- | --- |
|  |  |
| INTRODUCTION…………………………………...……………………………………. | 5 |
| 1 Methods and algorithms for the secure use of external servers to solve computationally-complex problems with secret parameters. ……………………………... | 7 |
| 1.1 Problems of Finding the Extremum of a Function with Secret Parameters ….. | 7 |
| 1.2 Linear Programming Problems with Secret Parameters …………………….. | 12 |
| 1.3 Problems of Finding the Value of an Analytic Function on a Secret Argument | 14 |
| CONCLUSION ……………………………………………………………....................... | 17 |
| LIST OF USED SOURCES ………………………………………………..…………….. | 18 |
| APPENDIX A List of published works for 2021 ………………………………………... | 20 |
| APPENDIX B Work Schedule for 2021 ……………………..………………………..…. | 22 |

**INTRODUCTION**

In this work, we study methods for the safe use of external insecure servers when solving computationally -complex problems with secret parameters. This problem is one of the important scientific directions in the field of information security of cloud computing. The paper presents methods of secure outsourcing for the following classes of computationally -complex tasks with secret parameters:

- Problems of finding the extremum of a function with secret functions;

- Linear programming tasks with secret functions;

- Problems of finding the value of an analytical function on a secret argument.

The theory of secure outsourcing of scientific computing is rapidly developing in various fields, since in modern conditions, the processing of big data is no longer possible to imagine without the use of powerful computing resources. That is why leading scientists in the field of information security offer a variety of methods for the secure outsourcing of scientific computing [1-24].

The main idea of ​​the new approach in solving computationally-complex problems with secret parameters is the use of external computing resources. However, at the same time, on the client side, preliminary transformations of the original computational problem are carried out. That is, before sending a task to the server, the client needs to hide the secret parameters so that the server (or information interception) cannot determine these parameters. Then this transformed computationally complex task is sent to the server. Let's solve the obtained problem, the server returns the given intermediate solution to the client, and the client should be able to restore the solution of the original computationally-complex problem within a reasonable time.

Note that our main goal is to demonstrate new methods of secure outsourcing of scientific computing, so we model classes of problems in such a way as to clearly show the essence of these methods.

In Section 1.1 we will study several problems of finding the extremum of a function with secret functions. At the same time, we offer several examples, generalizing them step by step, and moving on to non-trivial problem statements.

Subsection 1.2 deals with linear programming problems with secret parameters. Such problems arise, for example, in production planning, which, as well-know, can be mathematically represented as a problem of determining the maximum value of a linear function under certain constraints. Also presented is one mathematical programming problem where the objective function is not a linear function.

Subsection 1.3 presents a solution to the problem of finding the value of an analytical function of several complex variables on a secret argument. For an approximate solution of this problem using a server, we used Osgood's lemma and the generalized Cauchy integral formula from the theory of functions of several complex variables.

**1 Methods and algorithms for the secure use of external servers to solve computationally-complex problems with secret parameters**

**1.1 Problems of finding the extremum of a function with secret parameters**

In this subsection, we will consider methods for secure finding the extremum of a function with secret parameters using external servers. At the same time, in order to show the essence of the methods, we will demonstrate them with specific examples.

First, consider a real function of one variable:

(1)

Suppose that this function is twice differentiable on some interval . Then the critical points , are known to be determined from the condition

Therefore, the main difficulty in finding the extremum of a function is to find the critical points, after which it is easy to calculate the value of the extremum of the function by the formula (1).

Example No 1. Suppose that it is necessary to find the critical point for the function

(2)

using an insecure server, while some of the parameters are the client's secret numbers.

Option 1. Let the number is a secret, and the rest of the parameters are not secret. Then is sent to the insecure server the following equation: If is the solution to this equation, then the client finds the extreme value by calculating the value at that point.

Option 2. Let the number is a secret, and the numbers are not a secret. Then, to find the critical point on an insecure server, we can use the following protocol:

Step 1. The client chooses a random secret number and calculates the numbers and . And then sends to the server the following equation:

Step 2. Insecure server finds a solution of the equation , and returns this solution to the client.

Step 3. The client finds a solution to the equation by the formula.

We can, of course, give other options, for example, consider that the number a is a secret parameter or, or all parameters at once are a secret, but, in fact, they are solved in a similar way.

Example No 2. Suppose we need to find the critical point for a function of two variables.

(3)

The critical point of this function is found by solving the system of equations

That is, it is necessary to solve the linear equation

(4)

There can also be various options here, but we will consider only one option, when the numbers are the secret parameters of the client. To solve equation (4) using a server, we can use the following protocol:

Step 1. The client chooses a secret vector at random

and calculates the vector

Then the client calculates the vector

;

and sends the equation to the server

(5)

relatively unknown

Step 2. The server solves equation (5) and returns the solution to the client. We denote this solution .

Step 3. The client finds a solution to equation (4) according to the following formula

.

Example No. 3. Consider an arbitrary twice continuously differentiable function y= on the segment . It is necessary to find the extremum of this function, while we will assume that the function itself is a secret.

We make the following types of change of variables:

- shift along the abscissa: , where is some fixed number that provides a shift of the function graph along the abscissa axis;

- shift along ordinates: , where is a some fixed number that provides a shift of the function graph along the ordinate axis;

- compression of the function along the abscissa axis: is a compression ratio along the abscissa;

- compression of the function along the ordinate axis: - compression ratio along the ordinate.

Now we will make sequentially all these types of change of variables:

Suppose that at the interior point extreme value is reached , then the function reaches its extremum at the point

in this case, the extreme value will be equal to

Now finding the extremum of a function can be described by the following protocol.

Step 1. The client transforms the original function , successively applying all of the above types of variable substitutions, and the numbers keeps secret. Next, it sends to the server next function and interval .

Step 2. The server finds the breaking point and extremum for function jn the interval and passes a couple of numbers ( to the client .

Step 3. The client finds the critical point and extremum of the original function using the following simple formulas

Example No. 4. Let us now consider the general case. Note that instead of a simple shift along the abscissa axis, we can make the following change of variable:

,

where , and function is a any strictly increasing continuously differentiable function on some segment and let at all points the strict inequality holds

Suppose that the conditions

Further, since

,

and , then the problem of finding the extremum of the function on the segment is reduced to the problem of finding the extremum of the function

On the segment .

So, we need the following types of variable changes:

- replacement of dependent variable: *,* where is a new explanatory variable;

- shift along ordinates: , where is a some fixed number that provides a shift of the function graph along the ordinate axis;

- compression of the function along the ordinate axis: - compression ratio along the ordinate.

Now, making sequentially all these types of change of variables, we get as a result the function

Suppose that at the interior point the extremal value is reached, then the function reaches its extremum at the point such that .In this case, the extreme value will be equal to

Now finding the extremum of a function can be described by the following protocol.

Step 1. The client transforms the original function , successively applying the described types of change of variables, while the function , as well as numbers keeps secret. Next, it sends a function and interval to the server.

Step 2. The server finds the extreme point and extremum for function jn the interval and passes a couple of numbers ( to the client.

Step 3. The client finds the extreme point and extremum of the function by the following simplest formulas

Example No. 5. In some cases, when modeling economic problems, we get a certain optimization problem, where it is required to find the extremum of a function under certain constraints. Consider the following problem of determining the extremum of a function

|  |  |  |
| --- | --- | --- |
|  |  | (6) |

and impose communication conditions

|  |  |  |
| --- | --- | --- |
|  |  | (7) |

where .

The Lagrange function will have the form:

Differentiating the Lagrange function with respect to each variable and taking into account the constraint condition, we compose the following system of equations:

Let us denote by matrix

Then we obtain the system of linear algebraic equations

, (8)

where is right column, is a unknown vector. As we see, the problem of finding the critical point is reduced to solving equation (8).

The client needs to find the extremum of the function (6) under the condition of communication (7) using the computational means of an unsafe server. In this case, the server does not need to know the following secret client parameters: *,* and *P*. And the decision itself must also remain a secret.

To solve this equation, you can use the following protocol:

Step 1. The client takes the secret vector at random and the secret invertible matrix :

and calculates a new matrix , and sends to the server the equation

|  |  |  |
| --- | --- | --- |
|  |  | (9) |

Step 2. The server solves the system of linear algebraic equations (9) and returns the solution to the client .

Step 3. Then the client finds a solution to equation (8) by the formula

That is, it finds the critical point for function (6) under the condition of connection (7).

Note that in the case when for the client the numbers and are not secret, then instead of the matrix the identity matrix is taken.

**1.2 Linear Programming Problems with Secret Parameters**

Now we will consider the general problem of production planning, which, as you know, can be mathematically represented as the problem of determining the maximum value of the function

(10)

with restrictions (terms of communication)

Here are some constants.

Suppose that the coefficients are the client's secret numbers, and the numbers are not a secret. Also suppose the solution must also be kept secret.

Let is a positive diagonal matrix of the following form

Let's make the change of variables

Then we get the following problem

(13)

with restrictions (terms of communication)

Here .

Now we can imagine a protocol for solving the problem (10-12):

Step 1. The client takes a random diagonal matrix

and makes the change of variables Now sends to the server a task (13-15).

Step 2. The server solves the problem (13-15) and sends the solution to the client.

Step 3. The client finds a solution of the task (10-12) by the formula

Now we present a typical economic optimization problem in which the objective function is not linear, but which can only be solved using the computing power of the servers.

Let is a is a positive matrix, and the numbers are positive numbers.

It is required to find a vector , maximizing function

(16)

with restrictions

(17)

(18)

Where are upward convex scalar functions of one variable (this is necessary to be able to use general convex optimization methods, for example, the natural logarithm is a convex upward function).

So, suppose the client needs to solve problem (16) - (18). The secret elements are the matrix *C,* numbers and vector solution ). The vector = () is not secret.

*Protocol*

Step 1. The client randomly chooses secret diagonal matrices

and calculates Further, at calculates , and sends to the server a task (19) − (21) :

(19)

|  |  |  |
| --- | --- | --- |
|  |  | (20) |
|  |  | (21) |

Step 2. The server solves problem (19) - (21), and an approximate solution returns to the client.

Step 3. The client finds a solution to problem (16) - (18) by the formula

|  |  |  |
| --- | --- | --- |
|  |  | (22) |

It is easy to see that this protocol solves the original problem. Let's make the change of variables

Then, considering that

,

then (16) - (17) take the form (19) - (20), respectively. Further, since are positive numbers, then condition (18) can be written in the form of condition (21).

Protocol security. Insecure server gets a system of equations

, ,

Since the system of equations (23) contains unknowns, and the number of equations themselves in this system is , system (23) is ambiguously solvable, that is, the server will not be able to unambiguously determine the secret parameters of the client.

**1.3 Problems of Finding the Value of an Analytic Function on a Secret Argument**

Consider a computationally complex complex function defined in some open subset , where is cartesian product of copies of the complex plane. We need to approximately calculate the value of the complex function , using the computing resources of the server.

Suppose the function is a continuous in an open set and is holomorphic with respect to each variable separately, then according to the well-known Osgood lemma, this function is holomorphic in the entire domain . Let the closed polydisk . Then, using repeatedly the Cauchy integral formula for a function of one variable, we obtain

valid for any interior point .

Without loss of generality, suppose that . Then the value of the complex function on the secret argument can be calculated approximately by the following integral sum:

where the points are uniformly selected at the boundaries of the disks respectively, where , , .

Now the approximate calculation of the value of the analytic function on the secret argument can be represented by the following protocol:

Step 1. The client chooses large enough numbers as well as points , uniformly selected along the boundaries accordingly, and sends the function to the server .

Step 2. The server calculates the value of the function at every point: , And also calculates numbers . Calculated numbers server sends to client.

Step 3. The client calculates the approximate value of the function on the secret argument by the formula

Note that this method assumes that the server calculates the values quickly enough , at every Then the client performs fairly simple arithmetic operations.

**CONCLUSION**

In this work, new methods and algorithms for the safe use of external unsafe servers in solving computationally-complex problems with secret parameters are obtained. Namely, methods of secure outsourcing were presented for the following classes of computationally-complex tasks with secret parameters:

- linear programming problems with secret parameters;

- the problem of finding the extremum of a function with secret parameters;

- the problem of finding the value of an analytical function on a secret argument.

The level of scientific elaboration. For the first time, methods and algorithms were proposed for solving the problem of finding the extremum of a function with secret parameters, solving a linear programming problem with secret parameters, as well as solving the problem of finding the value of an analytical function of several variables on a secret argument.

The prospect of using the results of this study. The research results can serve as a source for further analysis and research in the development of methods for the safe outsourcing of computationally-complex tasks with secret parameters.

Completeness of results. The results of the research work were published:

- In the Indonesian journal "Indonesian Journal of Electrical Engineering and Computer Science", which has a CiteScore percentile in the Scopus database - 47, the project manager E. Seitkulov is the first author, and is also an author for correspondence, IRN AP09559249 is the first in the information line about financing.

- Two talks at The III International Turkic World Congress on Science and Engineering.

LIST OF USED SOURCES

1. Seitkulov Ye., New methods of secure outsourcing of scientific computations // The Journal of Supercomputing, 2013. - Vol. 65. - Issue 1. - P. 469-482. Doi: 10.1007/s11227-012-0809-3.
2. Yu Jianhua, Wang Xueli, Gao Wei, Improvement and applications of secure outsourcing of scientific computations // Journal of Ambient Intelligence and Humanized Computing, 2015. - Vol. 6. - P.763–772. Doi: 10.1007/s12652-015-0280-0.
3. Hu Xing and Tang Chunming Secure outsourced computation of the characteristic polynomial and eigenvalues of matrix // Journal of Cloud Computing, 2015. - URL: https://eprint.iacr.org/2014/442.pdf. - Doi: 10.1186/s13677-015-0033-9.
4. Wang C., Ren K., Wang J. Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming // IEEE Transactions on Computers, 2016. -Vol. 65. - Issue 1. - P. 216-229. Doi: 10.1109/TC.2015.2417542.
5. Vyas Ronak, Singh Alok, Singh Jolly, Soni Gunjan, Purushothama B. R. Design of an efficient verification scheme for correctness of outsourced computations in cloud computing // Security in Computing and Communications, Springer*,* 2015. - Vol. 536. - P. 66–77. Doi: 10.1007/978-3-319-22915-7\_7.
6. Atallah M. and Frikken K. Securely outsourcing linear algebra computations // ASIACCS '10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010. -P.48-59. Doi: 10.1145/1755688.1755695.
7. Benjamin D. and Atallah M. Private and cheating-free outsourcing of algebraic computations // Proceedings of 6th conference on privacy, security, and trust (PST), 2008. -P. 240-245. Doi: 10.1109/PST.2008.12.
8. Matsumoto Tsutomu, Kato Koki, Imai Hideki Speeding Up Secret Computations with Insecure Auxiliary Devices // In: Goldwasser S. (eds) Advances in Cryptology — CRYPTO’ 88. Lecture Notes in Computer Science*,* 1990. *-*Vol. 403. –P. 497-506. Doi: 10.1007/0-387-34799-2\_35.
9. Thierry Mefenza, Damien Vergnaud Cryptanalysis of Server-Aided RSA Protocols with Private-Key Splitting // The Computer Journal, 2019. - Vol. 62. - Issue 8. -P. 1194–1213. Doi: 10.1093/comjnl/bxz040.
10. Zhou Kai, Afifi M.Y., Ren Jian ExpSOS: Secure and Verifiable Outsourcing of Exponentiation Operations for Mobile Cloud Computing // IEEE Transactions on Information Forensics and Security, 2017. - Vol.12. - Issue 11. - P. 2518-2531. Doi:10.1109/TIFS.2017.2710941.
11. Hohenberger S. and Lysyanskaya A. How to Securely Outsource Cryptographic Computations //In: Kilian J. (eds) Theory of Cryptography. TCC, Lecture Notes in Computer Science, 2005. - Vol. 3378. - P. 264–282. Doi: 10.1007/978-3-540-30576-7\_15.
12. Béguin P. and Quisquater J.-J. Fast Server-Aided RSA Signatures Secure Against Active Attacks // In: Coppersmith D. (eds) Advances in Cryptology — CRYPT0’ 95. Lecture Notes in Computer Science, 1995. - Vol. 963. - P. 57-69. Doi: 10.1007/3-540-44750-4\_5.
13. Lim C.H. and Lee P.J. Security and Performance of Server-Aided RSA Computation Protocols // In: Coppersmith D. (eds) Advances in Cryptology — CRYPT0’ 95. Lecture Notes in Computer Science*,*1995. *-* Vol. 963. - P.70–83. Doi: 10.1007/3-540-44750-4\_6.
14. Castelluccia C., Mykletun E., Tsudik G. Improving Secure Server Performance by Re-balancing SSL//TLS Handshakes // ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security, 2006. - P.26–34. Doi: 10.1145/1128817.1128826.
15. Chen X., Li J., Ma J., Tang Q., Lou W. New Algorithms for Secure Outsourcing of Modular Exponentiations //In Foresti, S., Yung, M. and Martinelli, F. (eds.) ESORICS, Lecture Notes in Computer Science, 2012. - Vol. 7459. - P. 541–556. Doi: 10.1007/978-3-642-33167-1\_31.
16. Wang Y. and et al. Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage//In Kutylowski, M. and Vaidya, J. (eds.) ESORICS, Lecture Notes in Computer Science, 2014. - Vol. 8712. - P.326–343. Doi: 10.1007/978-3-319-11203-9\_19.
17. Nguyen P.Q. and Shparlinski I. On the Insecurity of a Server-Aided RSA Protocol // In: Boyd C. (eds) Advances in Cryptology — ASIACRYPT 2001. Lecture Notes in Computer Science, 2001. - Vol. 2248. - P. 21–35, 2001. Doi: 10.1007/3-540-45682-1\_2.
18. Merkle J., Multi-round Passive Attacks on Server-Aided RSA Protocols // CCS '00: Proceedings of the 7th ACM conference on Computer and Communications Security, 2000. - P. 102–107. Doi: 10.1145/352600.352616.
19. Pfitzmann B. and Waidner M. Attacks on Protocols for Server-Aided RSA Computation *//*In: Rueppel R.A. (eds) Advances in Cryptology — EUROCRYPT’ 92. Lecture Notes in Computer Science, 1993. - Vol.658. -P. 153–162. Doi: 10.1007/3-540-47555-9\_13.
20. Jakobsson M. and Wetzel S. Secure Server-Aided Signature Generation // In: Kim K. (eds) Public Key Cryptography. PKC 2001. Lecture Notes in Computer Science, 2001. -Vol. 1992. -P. 383–401. Doi: 10.1007/3-540-44586-2\_28.
21. Merkle J. and Werchner R. On the Security of Server-Aided RSA Protocols // In: Imai H., Zheng Y. (eds) Public Key Cryptography. PKC 1998. Lecture Notes in Computer Science, 1998. - Vol. 1431. - P. 99–116, 1998. Doi: 10.1007/BFb0054018.
22. Aono Y. A New Lattice Construction for Partial Key Exposure Attack for RSA // In Jarecki, S. and Tsudik, G. (eds.) PKC, Lecture Notes in Computer Science, 2009. - Vol. 5443. - P. 34–53. Doi: 10.1007/978-3-642-00468-1\_3.
23. Blömer J.and May A. New Partial Key Exposure Attacks on RSA // In Boneh, D. (ed.) CRYPTO, Lecture Notes in Computer Science, 2003. - Vol. 2729. -P. 27–43. Doi: 10.1007/978-3-540-45146-4\_2.
24. Ernst M., Jochemsz E., May A., de Weger B. Partial Key Exposure Attacks on RSA up to Full Size Exponents // In Cramer, R. (ed.) EUROCRYPT Lecture Notes in Computer Science, 2005. - Vol. 3494. - P. 371–386. Doi: 10.1007/11426639\_22.

**APPENDIX A**

**List of published works for 2021**

1. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Gulden B. Ulyukova, Banu B. Yergaliyeva, Dina Satybaldina Methods for secure cloud processing of big data // Indonesian Journal of Electrical Engineering and Computer Science, Vol. 22, No. 3, June 2021, pp. 1650-1658, ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i3.pp1650-1658(**Percentile** **Scopus CiteScore - 47; the project manager Ye. Seitkulov - the first author, and also the author for correspondence; IRN AP09559249 is the first in the information line about financing**).
2. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Banu B. Yergaliyeva Secure Outsourcing a Linear Programming Task with Secret Parameters // Book of abstracts of the III International Turkic World Congress on Science and Engineering 14-15 June 2021, Niğde – Turkey, - p. 29.
3. Yerzhan N. Seitkulov, Seilkhan N. Boranbayev, Ainur Zhetpisbayeva Secure Outsourcing of Finding the Extremum of a Function with Secret Parameters // Book of abstracts of the III International Turkic World Congress on Science and Engineering 14-15 June 2021, Niğde – Turkey, - p. 30.
4. Banu B. Yergaliyeva, Yerzhan N. Seitkulov, Dina Satybaldina Secure methods for solving computationally-complex problems using auxiliary computers Indonesian // Indonesian Journal of Electrical Engineering and Computer Science (**Percentile Scopus CiteScore - 47; project manager E. Seitkulov - is the author for the correspondence, at the time of approval and submission of the report (14 October, 2021) the article is under review**).

**APPENDIX B**

**Work schedule for 2021**





Appendix 1.14

to this agreement

No. 313 / 12-2 dated June 22, 2021

**CALENDAR PLAN**

**1. Non-profit joint-stock company "LN Gumilyov Eurasian National University"**

**1.1 By priority:** 4. Information, communication and space technologies**.**

**1.2 By sub-priority:** 4.5.2. Methods and algorithms for ensuring information security of complex systems and data**.**

**1.3 On the topic of the project: AP09559249 -** Research and development of methods for the secure use of external servers to solve computationally-complex problems with secret parameters**.**

**1.4 The total amount of the project for 2021:** 5,000,000 (five million) tenge, for the performance of work in accordance with clause 3.

**2. Characteristics of scientific and technical products by qualification characteristics and economic indicators**

**2.1 Direction of work:** Information security**.**

**2.2 Scope:** Information protection**.**

**2.3 The final result for 2021:** new methods and algorithms for the safe use of external servers will be developed when solving classes of linear programming problems and the problem of finding the extremum of a function with secret parameters, as well as the problem of finding the value of an analytical function on a secret argument**.**

At least 1 (one) article published, accepted for publication or submitted to a peer-reviewed scientific publication included in the Science Citation Index Expanded or Social Science Citation Index in the Web of Science database and (or) having a CiteScore percentile in the Scopus database of at least 35 (thirty five).

**2.4 Patentability:** Not expected**.**

**2.5 Scientific and technical level (novelty):** High.

**2.6 The use of scientific and technical products is carried out:** Joint use in accordance with the legislation of the Republic of Kazakhstan.

**2.7 Type of use of the result of scientific and (or) scientific and technical activities:** The results obtained will be used in the planned R&D for the development of information security means when using external computing systems**.**

**3. Name of work, terms of their implementation and results**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Job code, stage | | Name of work under the Agreement and the main stages of its implementation | | Deadline | | | Expected Result | |
| Start | | End |  | |
| **2021** | | | | | | | | |
| 1 | | develop new methods and algorithms for the secure use of external servers when solving the following tasks:  - linear programming problems with secret parameters;  - the problem of finding the extremum of a function with secret parameters;  - the problem of finding the value of an analytical function on a secret argument. | Май 2021 | | | Декабрь 2021 | | New methods and algorithms for the safe use of external servers will be developed when solving classes of linear programming problems and the problem of finding the extremum of a function with secret parameters, as well as the problem of finding the value of an analytical function on a secret argument.  At least 1 (one) article published, accepted for publication or submitted to a peer-reviewed scientific publication included in the Science Citation Index Expanded or Social Science Citation Index in the Web of Science database and (or) having a CiteScore percentile in the Scopus database of at least 35 (thirty five). |
|  | | | | | | | | |
| By customer:  State Institution "Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan"  \_\_\_\_\_\_\_\_\_\_\_\_\_\_Zh. Kurmangaliyva | | | | From the Contractor:  Vice-rector for Science and Innovation  ENU them. L.N. Gumilyov  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ye. Sydykov    Familiarized with:  Scientific supervisor of the project (s)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ye. Seitkulov  (sign) | | | | |