Institute of Information and Computational Technologies

ISSN : 2788-7677 (Online)
ISSN : 2788-7987 (Print)

ADVANCED TECHNOLOGIES AND COMPUTER SCIENCE

2022
№4

www.atcs.iict.kz

Institute of Information and Computational Technologies

Advanced Technologies and computer science

№4

Almaty 2022

ISSN: 2788-7677 (Online)
ISSN : 2788-7987 (Print)

Institute of Information and Computational Technologies,

Advanced Technologies and computer science

28 Shevchenko str., Almaty,Republic of Kazakhstan
7 (727) 272-37-11
atcs@iict.kz

About the Journal

Advance technologies and computer science is a bilingual scientific peer-reviewed, interdisciplinary, electronic journal of open access, including thematic areas:

- Section **"Applied mathematics, computer science and control theory"** includes papers describing modern problems in these areas.
- Section **"Information and telecommunication technologies"** also includes the following topics:
    - Data transmission systems and networks.
    - Internet technologies.
    - Cloud technologies.
    - Parallel computing.
    - Distributed computing.
    - Supercomputer and cluster systems.
    - Big data processing (Big-data).
    - Geographic Information Systems and Technologies.
- In the section **"Artificial intelligence technologies"** in addition to technology, there are works on topics:
    - Intelligent Management Systems.
    - Speech technology and computer linguistics.
    - Pattern Recognition and Image Processing.
    - Bioinformatics and biometric systems.
    - Human-machine interaction.
    - Machine learning.
    - Intelligent Robotic Systems.
- The section **"Information Security and Data Protection"** also covers topics:
    - Software and hardware information protection.
    - Mathematical methods for ensuring information security of complex systems.
- The section **"Modeling and optimization of complex systems and business processes"** may include:
    - Computational mathematics, numerical analysis and programming, mathematical logic.
    - Theory of Statistics.
    - Statistical Methods.

Contents

UDC 004.02
IRSTI 20.53.15

MODERN REVIEW OF PAST PROBLEMS IN APPLIED MATHEMATICS AND COMPUTER SCIENCE

Mirzakhmet Syzdykov
al-Farabi Kazakh National University, Almaty, Kazakhstan
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Abstract. In this article we present the novel model of studying the past problems in present. These problems are very well handled by many authors; however, the result remains unproved. The problems are as follows: Nash equilibria in co-operative games and P versus NP theorem by Stephen Cock. We show that there is a solution for both classical problem in a partial case for "P versus NP"-theorem and co-operative games equilibria for all cases. Since partial case for P-NP problem could be proved by showing that Bellman's dynamic programming (DP) is the most optimal algorithm for composite tasks and problems. We also show that same equation by Bellman within the pre-defined parameter can be valid for both P and NP classes of problem according to the ordered sets of arbitrary variables which are compound to Bellman's equation, which was studied well in prior works by the same author, who holds the position of IT-analyst at the present time.

Keywords: Nash equilibria, computational complexity, P versus NP, proof of concept.

Introduction

For the past time the Nash equilibria and economical drastically known results for co-operative games were well studied and, even, honored as a Nobel Prize; in this article we present the final equation for the past work and show that the equilibria is commonly tied to the meaning of probability and statistics, which is handled well by Applied Mathematics as one of the most important scientific disciplines – this fact is well-known by author due to Prof. Vinoo Cameron, who presently resides and United State of America (USA) and holds Medicine Doctor (MD) position at the Hope Clinic, Athens.

Meanwhile many researchers see a valuable perspective of the result proposed by John Forbes Nash [1].

More results are to come for showing that Nash equilibria from the computational point of view is NP-complete and, thus, cannot be handled by modern era computing technologies – this fact is due to the recurrently dependent nature of the Nash algorithm for co-operative games with only two sides as minimal. We prove the result for many players of these economical market games, which is an extended case and, thus, cannot be omitted. This question was first put in the science in [2]. Many other attempts were made towards the open question of the Nash equilibria for the arbitrary size of set of players [3, 4]. From all the above, we define the probability of the Nash theorem for the common or "full" case – for this purpose we use the statistical probability for each player.

Since we have worked out our concerns about Nash equilibria, it's time for another important question in Computer Science. As to author's concerns this question is somehow tied to the mathematics in common and is included as one of the Millennium Problem by the Clay Institute of Mathematics, along with, for example, Navier-Stocks equation and other most important problems well-studied and known in the modern age [5]. This problem is originated from the official theory by the Alan Mathison Turing Award recipient Stephen Cook [6]. We begin our study of this naturally important question from previous publication [7]. We also give a notion to the modern works for "P versus NP" theorem by Lance Fortnow [8] and M. Sipser [9], which are the one of the latest known results to the present time: to the opinion of Dr. Gennady Fedulov from ResearchGate™, most of the researchers consider the P-NP question unsolvable due to the poor theoretical background for the definition of the algorithm and NP-complete problem, however, the author of the past work [7] gives the definition of theory and

practice for the term “algorithm”. We will use the Bellman algorithm [10] as the starting point for the successful evaluation of the modern result, described in this work. We will also show further that according to Bellman results the algorithms can be successfully classified as P and NP complete.

Nash equilibria in Co-operative Games. The classical description of the co-operative game in economics and other financial sciences is due to the winning rate in case of getting the step on the matrix n x n for two players, where at each step the new row or column is taken by one of the players in periodical order: the values of winning or loosing are given as is by this matrix.

We state that the composition of the Nash equilibria or problem is NP-complete, since there are almost factorial number of combinations for the definition of the target function which by the opinion of John Forbes Nash gives the minimal difference between the score of the game for both players.

We also state that this opinion, besides the computational complexity of the “task”, was misinterpreted in past and for now the general case for n-players cannot be omitted.

We present the result according to probability model and the following consequence:

$$r_i = \frac{v_i}{\sum v_i} \cdot \sum s_i, \tag{1}$$

where R is a set of rational number, V is a set of values and S is a set of measures.

The equation defines the arbitrary function p(x) by the division operator of each value and sum of all values – this is a generalized case of the co-operative games, where the arbitrary number of players gain the positive result according to the pre-defined probability.

Thus, the main case holds true and isn’t NP-complete as the initial result obtained by Prof. John Forbes Nash.

The proof of the NP-completeness of the initial case as described above follows from the fact that, as it’s known, in the initial circumstances the function p(x) is given by the recurrent relation between each turn in a series recorded for both, or two, players – thus, the number of possible combinations to be considered leads to the computational explosion and is almost exponential and even, as stated before, is of, more preciously, factorial nature.

We propose the novel approach of solving the co-operative games for general case as the number of players is defined by the dimension of vector V in (1).

The proof of P-completeness of the general case and the similarity of the system of equations by Nash naturally follows from the re-formulation of problem and the definition of the statistical probability.

Thus, in this section we have shown the importance of the newly obtained results described in this work.

In the next section we will learn about the Millennium Problem proposed by Stephen Cook, which is remains open in the modern age.

P versus NP in Computational Complexity. We state that if there's an order in the target function for the set of variables, then, P doesn’t equal NP according to the dynamic programming which is the most optimal way of solving the combinatorial problems using its recurrent function at each step of the algorithm.

The problem was first stated by Stephen Cook, from that time on now we have no defined answer if there's the possibility of finding the polynomial solution for NP-complete problems.

We assume that the growing speed of polynomial and non-polynomial functions is compared to each other:

$$O(n^t) \prec O(2^n) \prec O(n!) \prec O(n^n), \tag{2}$$

From the equation (2) it also naturally follows the classification of P and NP complete classes like P-complete nt and exponential and further 2n.

Since there's no known algorithms whose polynomial speed is faster than the speed of

growth of non-polynomial functions like power-set or factorial, then it naturally follows that if P and NP are equal, then speed of algorithm steps in P is equal or greater than number of steps required for the NP-complete task:

$$\frac{\partial x^t}{\partial x} \geq \frac{\partial 2^x}{\partial x} \rightarrow P = NP \quad , \qquad (3).$$

The same applies to the factorial function and its equivalent value as function in form xx. As t is a free parameter then we see that:

$$t \cdot x^{t-1} < \ln(2) 2^x \quad , \qquad (4).$$

The inequality (4) is true for factorial also.

Thus, from (3) and (4) it naturally follows that the P and NP classes are different as the speed of growing non-polynomial function is much bigger than the same speed defined by derivative of polynomial function in P.

The plot of P and NP functions along with their derivatives can be seen on Figure 1.

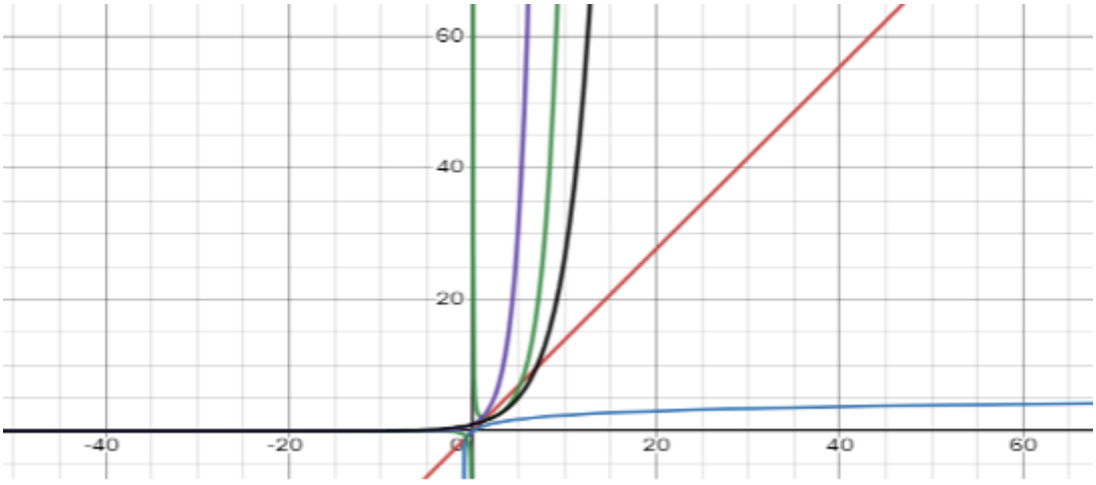

Figure 1 - Graphical plot of functions and derivatives

From all the above, it still doesn't follow that P != NP, however, for ordered set there's no optimal solution in P as the fastest possible algorithm's complexity is O(n) for iterative methodology, as it's presented at each step before inclusion at the stage set using dynamic programming, which is the most optimal as it's defined by recurrence relation at each stage.

We have shown that classes P and NP are different over the fact of derivatives defining the speed of the polynomial and non-polynomial functions respectively. It naturally follows that even for infinite order of derivative comparison the speed of non-polynomial functions is still increasing while the speed of polynomial function converges to absolute zero:

$$\lim_{n \to \infty} \frac{\partial^n x^t}{\partial t^n} < \lim_{n \to \infty} \frac{\partial^n 2^x}{\partial t^n} < \lim_{n \to \infty} \frac{\partial^n x^x}{\partial t^n} \quad , \qquad (5).$$

If there exist the ordered set in target function like in Traveling Salesman Problem (TSP), then P != NP according to the obvious statement that dynamic programming cannot cover all the space of possible cases.

The Bellman function is defined as follows for the set of variables without any order:

$$U_i(t, s_i) = arg_t \, opt \{U_{i-1}(t - t_{0,} s_{i-1}) + F_i(t_0)\} \quad , \qquad (6)$$

Since, there's no order in the target function Un, the (6) gives the polynomial solution to the problem. However, when there's an order we cannot use the ordered set for optimization problem on tape position t on the Turing automaton and, thus, P != NP – this is the final proof of Millennium theorem.

Conclusion

In this work we have shown the general case of the Nash equilibria in co-operative games for arbitrary number of players and proposed the ways of proving the correctness of this statement basing upon the applied mathematics sciences like statistics and theory of probability.

We have also shown the way of considering the partial case for “P versus NP” theorem as per the dynamic programming algorithm by Bellman.

Acknowledgements

The author expresses gratitude to all the members of scientific community of ResearchGate™, and specially to Prof. Gennady Fedulov for their valuable comments and interest in the problems known from past and gone to the present times.

References

[1] Holt C. A., Roth A. E. The Nash equilibrium: A perspective. Proceedings of the National Academy of Sciences. 2004. 101(12). 3999-4002.

[2] Daskalakis C., Goldberg P. W., Papadimitriou C. H. The complexity of computing a Nash equilibrium. SIAM Journal on Computing. 2009. 39(1). 195-259.

[3] Kreps D. M. Nash equilibrium. Game Theory. Palgrave Macmillan, London. 1989. 167-177.

[4] Myerson R. B. Refinements of the Nash equilibrium concept. International journal of game theory. 1978. 7(2). 73-80.

[5] Cook S. The P versus NP problem. Clay Mathematics Institute. 2000. 2.

[6] Cook S. The importance of the P versus NP question. Journal of the ACM (JACM). 2003. 50(1). 27-29.

[7] Syzdykov M. Functional hypothesis of complexity classes. Advanced technologies and computer science. 2022. 3. 4-9.

[8] Fortnow L. The status of the P versus NP problem. Communications of the ACM. 2009. 52(9). 78-86.

[9] Sipser M. The history and status of the P versus NP question. Proceedings of the twenty-fourth annual ACM symposium on Theory of computing. 1992. 603-618.

[10] Bellman R. Dynamic programming. Science. 1966. 153(3731). 34-37.

ҚОЛДАНБАЛЫ МАТЕМАТИКА МЕН ИНФОРМАТИКАДАҒЫ ӨТКЕН МӘСЕЛЕЛЕРГЕ ЗАМАНАУИ ШОЛУ

Мырзахмет Сыздықов
Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Аңдатпа. Бұл мақалада біз өткеннің қазіргі кездегі мәселелерін зерттеудің жаңа моделін ұсынамыз. Бұл мәселелерді көптеген авторлар өте жақсы шешеді; дегенмен, нәтиже дәлелденбеген болып қалады. Мәселелер келесідей: Нэштің кооператив ойындарындағы тепе-теңдігі және Стивен Коктың P-NP қатынасы туралы теоремасы. Біз "P vs NP" теоремасы үшін де, барлық жағдайларда кооператив ойындарының тепе-теңдігі үшін де классикалық есептің шешімі бар екенін көрсетеміз. P-NP тапсырмасының ішінара жағдайын Беллманның динамикалық бағдарламалауы (DP) күрделі есептер мен мәселелер үшін ең оңтайлы алгоритм екенін көрсету

арқылы дәлелдеуге болады. Біз сондай-ақ алдын ала анықталған параметр шегінде бірдей Беллман теңдеуі АТ позициясын ұстанатын сол автордың алдыңғы жұмыстарында жақсы зерттелген Беллман теңдеуі үшін құрама болып табылатын реттелген ерікті айнымалылар жиынтығына сәйкес P және NP есептер кластары үшін жарамды болуы мүмкін екенін көрсетеміз-қазіргі уақытта талдаушы.

Кілттік сөздер: Нэш тепе-теңдігі, есептеу күрделілігі, NP-мен салыстырғанда P, тұжырымдаманың дәлелі.

СОВРЕМЕННЫЙ ОБЗОР ПРОШЛЫХ ПРОБЛЕМ В ПРИКЛАДНОЙ МАТЕМАТИКЕ И ИНФОРМАТИКЕ

Мырзахмет Сыздыков
Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Аннотация. В этой статье мы представляем новую модель изучения проблем прошлого в настоящем. Эти проблемы очень хорошо решаются многими авторами; однако результат остается недоказанным. Проблемы заключаются в следующем: равновесие Нэша в кооперативных играх и теорема Стивена Кока о соотношении P и NP. Мы показываем, что существует решение как для классической задачи в частном случае для теоремы “P против NP”, так и для равновесий кооперативных игр для всех случаев. Поскольку частичный случай для задачи P-NP можно было бы доказать, показав, что динамическое программирование Беллмана (DP) является наиболее оптимальным алгоритмом для сложных задач и проблем. Мы также показываем, что одно и то же уравнение Беллмана в пределах заранее определенного параметра может быть справедливо как для P, так и для NP классов задач в соответствии с упорядоченными наборами произвольных переменных, которые являются составными для уравнения Беллмана, которое было хорошо изучено в предыдущих работах того же автора, который придерживается позиции ИТ-аналитик в настоящее время.

Ключевые слова: равновесия Нэша, вычислительная сложность, P в сравнении с NP, доказательство концепции.

Сведения об авторе:

Анг.: Syzdykov Mirzakhmet - al-Farabi Kazakh National University, Almaty, Kazakhstan

Каз.: Сыздықов Мырзахмет- әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.

Рус.: Сыздыков Мырзахмет- Казахский национальный университет имени аль-Фараби, Алматы, Казахстан.

UDC 004.02
IRSTI 20.53.15

EQUIVALENCE OF COMPLEXITY CLASSES VIA FINITE AUTOMATA DERIVATIVES

Mirzakhmet Syzdykov

al-Farabi Kazakh National University, Almaty, Kazakhstan
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Abstract. In this article practical, experimental and theoretical results of the conducted research are presented, these results refer to the main question in complexity theory like the “P versus NP” theorem, first proposed by Stephen Cook in his seminal paper, we give concise question of the equivalence of these classes from the state of conversion algorithm of non-deterministic finite automata (NFA) to deterministic finite automata (DFA), we do it by considering the canonical regular expression form presented by Schneider Klaus and do the derivative processing from the Berry-Sethi algorithm, the result gives P-complete algorithm along the canonical form of regular expressions when applying subset construction for specific regular expressions or NFA, DFA in this case remains applicable even for Turing tape machines, however, due to the past statement of the “P versus NP” theorem given by author in previous work this leads to the conclusion of the equivalence of complexity classes like P and NP as in canonical form the subset construction produces exponential growth of the number of states of DFA.

Keywords: subset construction, regular expression, P versus NP, derivatives.

Кіріспе

As we stated before the conducted research proves the equivalence of polynomial (P) and non-polynomial (NP) classes of complexity known as “P versus NP” theorem [1] on the sample of subset construction algorithm [2] by the derivative algorithm [3] on the canonical regular expression and NFA [4].

Previously we stated that the main theorem by Cook can be solved if for the given non-polynomial class of complexity in subset construction, which belongs to the exponential classes like EXPTIME and EXPSPACE, there exists the method to achieve it in polynomial time.

According to conducted research many scientists regard this notion as final and almost impossible to prove, however, we follow the same strategy presented before [5].

We do our statement on the regular expression experimental results [6]. These results lead to the observation that for canonical form of regular expression, leading subset construction algorithm to the exponential blow up of number of states in final DFA, there exist a practical and natural way of obtaining the rule which describes the problematic canonical form of regular expression in more practical way like polynomial or P-classes of computational complexity.

The ”P versus NP” is a classical example of unsolved theorems from the past works: it states that there exist no polynomial algorithm to solve the NP-complete problem, which were classified in past work [5].

Derivatives were first presented in [7, 8] in order to describe the algebraic properties of regular languages – this was, however, overcome by Berry and Sethi who presented an algorithmic approach in construction DFA directly from regular expression.

The Knapsack problem which is known to be co-NP complete is also presented in this article as it can be solved using Dynamic Programming (DP) [9].

Subset Construction on Single Fire Automata (SFA). As we have defined before in [6] that there exist the rules for SFA to apply DeMorgan law, in inverse, we can apply this rule to the not-starred logical “OR” operator, the changes aren’t made for the operator which is closed under Kleene closure.

In general, we do this for our experimental results on the one-step automata classes like SFA, the concept and design of which was first presented by the author of this work.

The subset construction on SFA gives the experimentation environment for building the DFA for canonical expression by Schneider [4], which is defined as:

$$(a + b)^*b(a + b)(a + b). \quad (1)$$

In the next section we will present the order of simplifying the regular expression (1) using the derivative algorithm by Berry-Sethi [3].

Generally, derivatives were also studied by Janusz Brzozowski [7] and Valentin Antimirov [8], however, definitive algorithm is due to Gerard Berry and Ravi Sethi.

As derivatives were first proposed by above authors, they still remain the point of interest of the modern research according to the Berry-Sethi algorithm.

We use this approach for our canonical form to prove the existence of polynomial algorithms to solve NP-complete problem.

Schneider proves that canonical regular expression (1) for subset construction is NP-complete, however, our research shows that it can be solved by extending the automata with feasible rule set which can be applied to the parameters like input and the canonical form.

The number of post OR-operators after marked symbol in (1) is defined as a parameter t in this work.

Schneider proves [4] that the algorithm to convert NFA to DFA has exponential complexity of O (2t+1).

Thus, the canonical form (1) lies in EXPSPACE and EXPTIME class which is more that class NP. By proving the P-completeness of the overall question we can make a decision that P-complete rule for NP-complete problem by Schneider solves the question as NP-class lies inside EXPTIME-class of the computational complexity.

Application of Derivatives to the Canonical Form

The regular expression (1) can be approximated by the doubled or invariant derivatives, the main idea is based on the past research [3].

Thus, we get the following rules to be applied to the canonical exponential form:

$$[Canonical\ Form]\ da\ db. \quad (2)$$

We apply the rule (2) until we reach the mark in (1) defined by single arbitrary symbol on the binary alphabet.

Thus, we get the result which leads to the equation of the mark to be matched in any case, meanwhile the pre- and post-expressions of canonical form (1) represent the fully defined set over the closed alphabet under binary notation.

Thus, the resulting rule will be defined as:

$$I\ [n - t] = \text{"b"}, \quad (3)$$

where I is an input string, n is a current position on given input and t is the number of post-repetitions of the fully defined OR-operator on the canonical form (1).

Thus, we have defined the final rule which is applicable even for Turing tape machines and other type of automata due to the presence of the mark symbol in the canonical regular expression (1).

Experimental Results on Extended Regular Expressions

As it follows from the result in previous section, we have also conducted the research on the SFA with OR-rewriting rule as it was presented in [6] with respect to the Kleene closure

under which the OR-remains not re-written.

DeMorgan's law is extended in this article for OR-operators as well as this leads to the composition of SFA in general, giving the possibility to the states to be fired once at a time as in this case we can avoid the state explosion effect or, simply, "blow up" which leads to the steady exponential increase of the number of states for the canonical form – in the original paper [4] t = 2, however, the author makes proof towards any value of the free parameter t.

Bellman's Dynamic Programming [9] doesn't approximate to the P-class too as it was shown in another publication of the author of this article. This fact is due to the recurrence relation in the common case of Bellman's equation as the number of steps required to solve NP-complete problem grows faster than the recurrent function and, thus, the problem cannot be solved in the minimal polynomial time. We have seen this effect before when classical Knapsack problem cannot be solved for the arbitrary values of weights in the given input data.

The experimentation has also showed that SFA are more compact for subset construction rather than Berry-Sethi algorithm which produces the same exponential number of states for canonical regular expression.

We obtain the following resulting diagram of DFA obtained from SFA on the Figure 1.

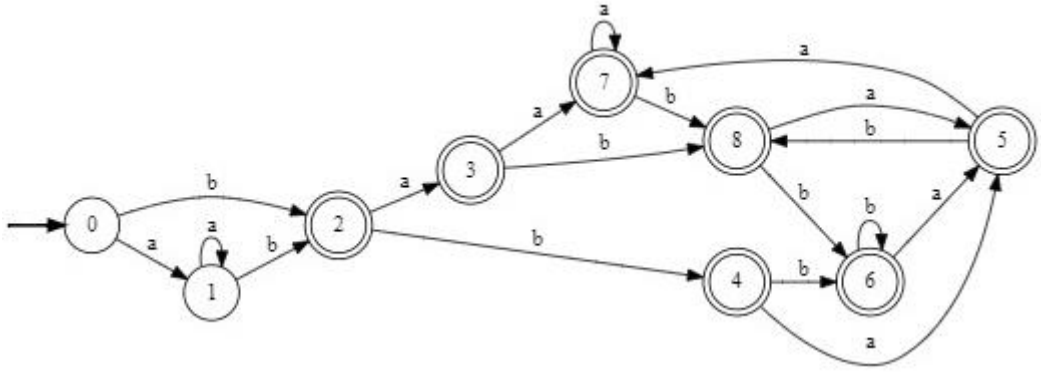

Figure 1 – DFA from SFA of the canonical regular expression

After minimization the obtained DFA is defined as:

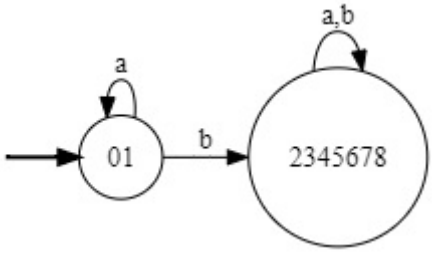

Figure 2 – Sample DFA after minimization of number of states

Obviously, the DFA on Figure 2 can be re-written in the regular expression form as:

$$a^*b(a + b)^*. \qquad (4)$$

The experimentation was made on the "Regex+" software package that demonstrates high feasibility not only for extended regular expressions as well as for a canonical form – the result from above figures (1) and (2) is the result obtained by the program.

On the Figure 2 the last state is final accepting the language (4).

Conclusion

We have demonstrated the steps required to simplify the canonical regular expression which was proved to be NP-complete along the subset construction.

Our research gives the result of the existence of the Fixed Input Automata (FIA), which can describe Schneider's canonical form.

The complexity of the presented sample FIA is O(n), where n is the number of input string to be matched against canonical regular expression – which, in case, is polynomial and belongs the P-class of complexity.

Thus, P equals NP according to the derivative application for simplification of the canonical form.

We make the final step in the discussion of the "P versus NP" theorem as the modified subset construction leads to the experimental evaluation of the canonical rule for the regular expression which was presented in this article.

By the term "proof" we mean the statement which cannot be argued due to the recent results on the question of relation between complexity classes, as NP is less than EXPTIME and the solving algorithm solves the problem in the EXPTIME, we conclude that P and NP classes are equal due to the fact that NP-class is bigger than P in order of magnitude as it was previously classified.

Thus, the classes of computational complexity like P and NP are equal due to the existence of the derivative solution for NP-complete problem of getting finite automaton for the canonical regular expression.

As we have defined the final point of the "P versus NP" theorem by giving not arguable argument towards the case when they're equal, we can conclude that algorithmic part of this question was studied less and rarely to give the algorithm which can solve the NP-complete problem in polynomial time.

We have reached the final result of the theorem and now it's time to solve other NP-complete problems by the experience of the research presented in this article.

Acknowledgements

The author expresses gratitude to the ResearchGate™ community for collaboration in presenting this work as well as for other scientists who contributed to the "P versus NP" theorem.

Funding

The work was fully supported by an educational grant of the Ministry of Education and Sciences of Republic of Kazakhstan during author studying at Satbayev University and during studying at the Institute of Problems in Informatics and Control.

References

[1] Cook, Stephen. The importance of the P versus NP question. Journal of the ACM (JACM) 50.1. 2003. 27-29.

[2] Rabin, Michael O., Dana Scott. Finite automata and their decision problems. IBM journal of research and development 3.2. 1959. 114-125.

[3] Berry, Gerard, Ravi Sethi. From regular expressions to deterministic automata. Theoretical computer science. 1986. 48. 117-126.

[4] Schneider, Klaus, Jimmy Shabolt, John G. Taylor. Verification of reactive systems: formal methods and algorithms. Heidelberg: Springer, 2004.

[5] Syzdykov, Mirzakhmet. Functional hypothesis of complexity classes. advanced technologies and computer science. 2022. 3. 4-9.

[6] Syzdykov, Mirzakhmet. Membership Problem in Non-deterministic Finite Automata for Extended Regular Expressions in Linear Polynomial Time. Advanced technologies and computer science. 2021. 4. 14-17.

[7] Brzozowski, Janusz A. Derivatives of regular expressions. Journal of the ACM (JACM). 1964. 11.4. 481-494.

[8] Antimirov, Valentin. Partial derivatives of regular expressions and finite automaton constructions. Theoretical Computer Science. 1996. 155.2. 291-319.

[9] Bellman, Richard. The theory of dynamic programming. Bulletin of the American Mathematical Society. 1954. 60.6. 503-515.

АҚЫРЛЫ АВТОМАТТАРДЫҢ ТУЫНДЫЛАРЫ АРҚЫЛЫ КҮРДЕЛІЛІК КЛАСТАРЫНЫҢ ЭКВИВАЛЕНТТІЛІГІ

Мырзахмет Сыздықов
әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Аңдатпа. Бұл мақалада жүргізілген зерттеудің практикалық, эксперименттік және теориялық нәтижелері келтірілген. Бұл тұжырымдар күрделілік теориясындағы негізгі сұраққа сілтеме жасайды. Мысалы, Стивен Кук өзінің негізгі мақаласында алғаш рет ұсынған "P және NP" теоремасы, біз осы сыныптардың эквиваленттілігі туралы қысқаша сұрақ қоямыз. түрлендіру күйі анықталмаған ақырлы автоматтар алгоритмі (NFA) үшін детерминирленген ақырлы автоматтар (DFA), біз мұны Шнайдер Клаус ұсынған тұрақты өрнектің канондық формасын қарастыра отырып жасаймыз және Берри-Сети алгоритмінен алынған өңдеуді орындаймыз, нәтиже p-complete алгоритмін тұрақты өрнектердің канондық формасы бойынша белгілі бір тұрақты өрнектерге немесе NFA-ға ішкі жиынның құрылысын қолданған кезде береді, бұл жағдайда DFA тіпті Тьюринг таспа машиналарына да қатысты болып қалады, алайда автор алдыңғы жұмыста келтірген "P vs NP" теоремасының бұрынғы тұжырымына байланысты бұл эквиваленттілік туралы қорытындыға әкеледі. P және NP сияқты күрделілік кластары үшін канондық түрде Ішкі жиынды құру DFA күйлерінің санының экспоненциалды өсуіне әкеледі.
Кілттік сөздер: Ішкі жиынды құру, тұрақты өрнек, NP-мен салыстырғанда P, туындылар.

ЭКВИВАЛЕНТНОСТЬ КЛАССОВ СЛОЖНОСТИ ЧЕРЕЗ ПРОИЗВОДНЫЕ КОНЕЧНЫХ АВТОМАТОВ

Мырзахмет Сыздыков
Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
mspmail598@gmail.com
ORCID ID: https://orcid.org/0000-0002-8086-775X

Аннотация. В этой статье представлены практические, экспериментальные и теоретические результаты проведенного исследования, эти результаты относятся к основному вопросу в теории сложности, такому как теорема “P против NP”, впервые предложенная Стивеном Куком в его основополагающей статье, мы кратко задаем вопрос об эквивалентности этих классов из состояния преобразования алгоритм недетерминированных конечных автоматов (NFA) для детерминированных конечных автоматов (DFA), рассматривая каноническую форму регулярного выражения, представленную Шнайдером Клаусом, и выполняем производную обработку из алгоритма Берри-Сетхи, результат дает алгоритм P-complete вдоль канонической формы регулярных выражений при применении построения подмножества для конкретных регулярных выражений или NFA, DFA в этом случае остается применимым даже для ленточных машин Тьюринга, однако, из-за прошлой формулировки теоремы “P против NP”, приведенной автором в предыдущей работе, это приводит к выводу об эквивалентности классов сложности, таких как P и NP, поскольку в канонической форме построение подмножества приводит к экспоненциальному росту числа состояний DFA.
Ключевые слова: построение подмножества, регулярное выражение, P в сравнении с NP, производные.

Сведения об авторе:

Анг.: Syzdykov Mirzakhmet - al-Farabi Kazakh National University, Almaty, Kazakhstan

Каз.: Сыздықов Мырзахмет- әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.

Рус.: Сыздыков Мырзахмет- Казахский национальный университет имени аль-Фараби, Алматы, Казахстан.

УДК 004.056.5
ГРНТИ 81.93.29

«HBC-256» ХЕШТЕУ АЛГОРИТМІНДЕГІ S-БЛОКТАРДЫҢ ДИФФЕРЕНЦИАЛДЫ КРИПТОТАЛДАУДАҒЫ КРИТИКАЛЫҚ НҮКТЕЛЕРІН ЗЕРТТЕУ

С. Нысанбаева[1], Қ.Сақан[1,2]
[1]Ақпараттық және есептеуіш технологиялар институты ҒК БҒМ, Алматы, Қазақстан,
[2]әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан
E-mail: kairat_sks@mail.ru
[1]ORCID ID: https://orcid.org/0000-0002-5835-4958
[2]ORCID ID: https://orcid.org/0000-0002-6812-6000

Аңдатпа. Бұл жұмыста ҚР БҒМ КН Ақпараттық және есептеуіш технологиялар институтында жасалған хештеу алгоритмдерінің бірі «HBC-256» алгоритміне дифференциалдық криптоталдау жүргізу қарастырылған. HBC-256 алгоритмі қысу функциясының CF (Compression Function) блоктық шифры негізінде жасалған және ұзындығы 256 биттік хэш мәнін шығарады. Кез келген жаңа криптографиялық схема сияқты HBC-256 алгоритмі оның де криптографиялық қасиеттерінің оң екендігін растау үшін мұқият зерттеуді қажет етеді, атап айтқанда: қайтымсыздық және бірінші және екінші типтегі коллизияға төзімділік. Жұмыстың нәтиже алу үшін барысында C++ бағдарламалау тілдерін қолдана отырып, жаңа хэштеу алгоритмін бағдарламалық қамтамасыз ету жүзеге асырылды. HBC-256 хэштеу алгоритмі үшін сызықтық емес хештеу түйіндерінің (s-блоктарының) дифференциалдық қасиеттері қарастырылады. Раундтық сипаттамаларды құрудың әртүрлі нұсқалары қарастырылады. Дифференциалды криптоанализдің негізгі қасиеттерін ескере отырып және басқа ғылыми жұмыстардың қорытындыларына сүйене отырып, ашық және сәйкес жабық мәтіндер жұптарының критикалық нүктелердегі жай-күйі зерттелген. Мақаланың қорытындысында хештеу алгоритмнің S-блоктары айырымдар кестесіндегі критикалық нүктелер арқылы коллизия тудыруға мүмкін болатын жағдайларға төзімді деген тұжырым жасалады.

Кілттік сөздер: хештеу алгоритмдері, хештеу алгоритмдеріне қойылатын талаптар, криптоталдаудың негізгі әдістері, дифференциальды криптоталдау.

Кіріспе

Қазіргі ақпараттық әлемде ақпараттың сенімділігі мен қауіпсіздігін қамтамасыз ету басты құндылықтардың бірі болып табылады. Әртүрлі қауіпсіздік мәселелеріне қатысатын негізгі криптографиялық түрлендірулердің бірі болып хеш-функциялар саналады – кел-келген еркін ұзындықтағы кіріс деректер массивін бекітілген ұзындықтағы бірегей тізбегіне түрлендіретін бір жақты математикалық түрлендірулер. Қазіргі заманғы хеш-функциялар пайдаланушылар аутентификациясы [1-5], деректердің тұтастығын бақылау [1, 6, 7], электрондық қолтаңба [1, 8], криптовалюта операцияларын қалыптастыру [9-12] сияқты ақпараттық қауіпсіздіктің әртүрлі процедураларын жүзеге асыру үшін қолданылады. Пайдаланушы аутентификация мәселелерін хеш мәндерінің деректерге кездейсоқ компонентті («криптографиялық тұз») міндетті түрде қосу арқылы тексерушіде аутентификация туралы ақпаратты қауіпсіз сақтау үшін пайдаланылады. Бұрын есептелген хеш мәндерін үлкен деректер жиындарының тұтастығын жылдам тексеруді қамтамасыз ету немесе стегоконтейнерлердің тұтастығын тексеру үшін де пайдалануға болады. Электрондық қолтаңбаны генерациялау кезінде хеш-функциялар қол қойылған деректердің бекітілген ұзындықтағы бірегей бит тізбегіне салыстыруын генерациялау үшін пайдаланылады, бұл болашақта олардың өзгермейтіндігіне сенімділік берілген кепілдікпен деректерге қол қою жылдамдығын арттыруға мүмкіндік береді.

Криптографиялық хэш функцияларына қойылатын талаптар:

Өнімділік: кез келген M хабарламасы үшін нақты уақытта h хэш мәнін тиімді

есептеуге болады.

Қайтымсыздық (бірбағыттылық): h хеш мәнін ескере отырып, h=H(M) болатындай

M хабарламасын табу есептеуде қиын болуы тиіс.

Әлсіз мағынада беріктілік: бізге белгілі M хабарламасы берілгенде, h=H(M)=H(M') болатындай M' хабарламасын қалыптастыру (есептеу) қиын болуы тиіс.

Күшті мағынада беріктілік: H(M)=H(M') болатындай M және M' кездейсоқ хабарламаларын табу қиын болуы тиіс.

Қазіргі уақытта хештеу функцияларын жасау келесі архитектуралық нұсқаларды пайдалануға негізделген:

1) әртүрлі сызықты емес (биттік) бульдік функцияларды қолдану;

2) блоктық симметриялық шифрлау алгоритмдері түріндегі қысу функциясына негізделген Меркле-Дамгард құрылымын пайдалану;

3) «Криптографиялық губка» құрылымын пайдалау;

4) арнайлы бағытталған құрылымдар.

Ақпараттық қауіпсіздік саласындағы ұсыныстарға, стандарттарға және халықаралық тәжірибеге сүйене отырып, хеш-функциялардың криптографиялық алгоритмдерінің беріктілігін талдау бойынша зерттеулер өзекті болып табылады және осы білім саласындағы ағымдағы жағдайды бағалау бойынша қолданылатын әрбір алгоритмге немесе оның модификациясына қатысты үздіксіз жұмысты талап етеді деп айтуға болады.

Әлі күнде де блоктық шифр ақпараттың құпиялылығын қамтамасыз етудің маңызды құралы болып табылады. Симметриялы блокты алгоритмдердің құрылымы сызықты және сызықты емес түйіндерден тұрады. Тәжірибеде сызықты емес түйін мәселесін S-блок ауыстырулары көп пайдаланылуда. Қазіргі уақытта радиожиілікті сәйкестендіру жүйелері (RFID) сияқты шектеулі ресурстарға ие құрылғылардың қауіпсіздігін арттыруға үлкен мәселелер туындауда. Аз ресурсты құрылғыларда көбінесе 4 биттік S-блок ауыстырулары пайдаланылады.

Талдау мен нәтижелер

Біз ұсынып отырған HBC-256 хештеу алгоритміндегі жаңа CF шифрлау алгоритмінде оның бағдарламалы-аппараттық және аппараттық тұрғыда икемді жүзеге асырылу мақсатында және бұл алгоритмді блоктық шифрлар негізінде хеш алгоритмдерін жасауда пайдалануды ойластыра отырып, S-блок ауыстыруларын басқа жолмен іске асыру қарастырылған. Осы алгоритм құрамындағы қолданылатын төрт 4-биттік S-блоктарды матрица элементтерінің орналасу жаңдайына байланысты белгілі бір тәртіппен қолдану - ұсынылған алгоритмнің құрылысының, соның ішінде кілт жасау алгоритмінің де ажырамас бөлігі болып табылады [13].

HBC-256 хештеу алгоритмінде сызықты емес биективті түрлендіру S-блок SBOX процедурасы арқылы анықталады. S0, S1, S2, S3 төрт алмастыру берілген, мұнда $S_i: \mathbb{Z}_{2^4} \rightarrow \mathbb{Z}_{2^4}, i = 0, \dots, 3$.. Жұмыс үшін кестеге сәйкес төрт «алтын» S-блок таңдалды. Олар төменгі Кесте-1-де көрсетілген.

Кесте 2 – төрт «алтын» S-блоктар

Зерттеу жұмысы Кесте-2-дегі төрт S-блоктарға дифференциалдық талдау әдісі арқылы ұсынылған HBC-256 хештеу алгоритмінің коллизияларға төзімділігін бағалауға бағыттаймыз.

Дифференциалды криптоталдау әдісін алғаш рет DES шифрлау стандартын талдау үшін Э.Бихам мен А.Шамир ұсынған [14, 15].

Дифференциалды криптоталдау шифрлаудың әртүрлі кезеңдеріндегі шифрланған мәндер арасындағы айырмашылықтарды түрлендіруді зерттеуге негізделген. Айырмашылық ретінде, әдетте, разрядтық қосынды модулі 2 операциясы (xor операциясы) қолданылады, оның ішінде $2n$ модулінің айырмасын талдау да мүмкін. Дифференциалды талдау симметриялық блоктық шифрларды және басқа криптографиялық примитивтерді, атап айтқанда хеш-функцияларды және ағындық шифрларды криптоталдау әдісі болып табылады [16]. Талдаудың бұл түрін қолдану үшін алгоритмнің барлық сызықтық емес элементтері – S-блок алмастыру блоктары негізінде xor операциясы немесе 2n қосу модулі немесе басқалары үшін дифференциалдық қасиеттердің кестелерін (xor операциясы үшін – айырымдар кестелерін) құру қажет.

Жалпы жағдайда, кез-келген шифрлау немесе хештеу алгоритмдеріне қатысты дифференциалды криптоталдау әдісін қолдану келесі қадамдарды жүргізуге негізделген:

1. Сызықты емес элементтерді талдау және олар үшін ең ықтимал айырымдарын анықтау.

2. Қарапайымнан күрделіге, яғни 1 раундтан n раундқа дейін көп раундты сипаттаманы (кіріс айырымы – шығыс айырымы) тұрғызу. Құрылған сипаттаманың пайда болу ықтималдығын анықтау.

3. Мәтіндердің дұрыс жұптарын, яғни кіріс мәндерінің қосындысы кіріс айырмасының мәніне сәйкес келетін мәтіндерді, ал шығыс мәндерінің қосындысы шығыс айырымдарымен сәйкес келетін мәтіндерді іздеу процесін жүргізу.

Бірінші кезекте қарастырылып отырған төрт S-блок алмастыруының xor операциясына қатысты айырымдар кестесін тұрғызайық (Кестелерде критикалық нүктелер қызыл боямен ерекшеленген):

Кесте 2 – S0-блок айырымдар кестесі

Кесте 3 – S1-блок айырымдар кестесі

Кесте 4 – S2-блок айырымдар кестесі

Кесте 5 – S3-блок айырымдар кестесі

Енді критикалық нүктелерлің кейбіреулеріне талдау жасап көрейік. Мысалы, S0-блогі үшін (1,5) қиылысындағы 4 рет кездесетін айырымдар жұбы: d1=1 және d2=5 үшін критикалық нүктелер төмендегідей болады.

Кесте 5 – S0-блок айырымдар кестесі негізінде критикалық нүктелерді анықтау

Po+ P1=1= d1	S0(Po)+ S0(P1)= d2	Критикалық нүктелер
0001+0000	1111=F	
0010+0011	0111=3	
0100+0101	0101=5= d2	0100 және 0101
0110+0111	0101=5= d2	0110 және 0111
1000+1001	1100=C	
1010+1011	0110=6	
1101+1100	1101=D	
1110+1111	1011=B	

Біз талдауды жалғастырайық. Ол үшін біз критикалық нүктелер 4=0100, 5=0101, 6=0110, 7=0111 ескеріп, тек басында ғана ерекшеленетін 4 ашық мәтінді таңдайық:

P1=4030303030303030303030303030303130303030303030303030303030303230303030303030303030303030303031

P2=5030303030303030303030303030303130303030303030303030303030303230303030303030303030303030303031

P3=6030303030303030303030303030303130303030303030303030303030303230303030303030303030303030303031

P4=7030303030303030303030303030303130303030303030303030303030303230303030303030303030303030303031

НВС-256 алгоритмінің 1 циклін жүргізген соң сәйкес шифрмәтіндерді аламыз:

1-ші раундтан кейін 2-ші және 3-ші блоктардағы бірдей бөлімдер, өйткені олар өзгерістерге ұшырамайды (ерекше бояумен боялған бөліктер):

C1=DD9251EA6DC04DA02A2C4DEEEF69ECDDEF631837B7A0C6DE4CDF315B04046EFA48A13E7F1519D0E4301FC9CB1F095F87

C2=CB9251816DC0CDA02A7A4DEEB169EC6CEF630437B7D0C6DE38DF31A6040463FA48F23E7FF419D047301F74CB1FCC5F87

C3=029251AD6DC074A02AEC4DEEFB69EC65EF63ED37B78DC6DEEFDF31020404CFFA484A3E7F2D19D0C6301FBECB1FFC5F87

C4=D49251E26DC0D0A02AE54DEE7B69EC53EF630037B7D4C6DEE6DF314C040485FA486A3E7F3919D03F301FE2CB1F6F5F87

2-раундтан кейін:

C1=9CDEC25066B9042733D96A00DF1E41D2C925FE1A17E36DA0410F99D0FC8771EC1CD548511F9CE480B85D6545939291FE

C2=2F3A1FCE0D3EC0E03B8CFCA1F6C40DEF065E898CE8F7F7A0E6C981EB0E6A404EF6E4FC22F56317F9916381DEBD86854F4

C3=C2B0F90A4EE751A8A9343F39599CE898DB899BC9C7EC81088E02EAE155E36DEC26B28FD5EBA181F8FA296DD5196DE22D

C4=27EDE0D4201E4D1E86C3ECD02D00D1CB262957A70695EB9B0009F592862711314D0A44B0FD5AA76B5D42FA847A3ABCBE

3-раундтан кейін:

C1=F0175EB6D6E05EC15057A967AD9472462393E9228D2B6EC4BC92AE075F24EEC73E47BB3CC31FD8CFC89DAC792E41BF02

C2=35D28BDCEC9A548BBAFCD062F672AC04E315CE3FCB8A2717970B193B0BEDEDD0E0550F2AAB2D5E5EDCF85351F5AC98E1

C3=46F39EEF58E341DEB34D2337B1800FAEFD48F0DD92B1525C5077528D75785D540ABF4238D8D143D48146FD3E3E27A404

C4=4E408A76F2D99AC06E1B920362DA32C87EFB76C7EE4C9CEEAC9FAC7283972B513E40101EC9E7860C48EDF9F17A894DB4

4-раундтан кейін:

C1=C8CDDC1EE712FE904DD228FEE42679568D69B879389D74069682FC3248F2B512BAE37311E1492D05F8AEDB868D51647D

C2=CFBBE27FA5D8FACDD3F119548E3E3023F07A7B61783649D87730FE3B25CC76798DECA53A147A8B91B3240EE5D8E67147

C3=449C5018D2C2ED8BD10E83CCAF3F3D77D20F8FF5BFBCD3440CC17ABD42215DDE3E807F88E8C10B2FD05B1843F80566F3

C4=68A1B2F3150B831C1D2DFBE2E9A0FFBE7BADE06766B8D0BB4FA3F6EB00074CCAD264FB99021841634ED8082E0B78185D

Енді 4-раундты D21= C1+C2, D22= C3+C4 ескеріп талдайық:

D21=07763E6142CA045D9E2331AA6A1849757D13C31840AB3DDEE1B202096D3EC36B370FD62BF533A6944B8AD56355B7153A

D22=2C3DE2EBC7C96E97CC23782E469FC2C9A9A26F92D90403FF43628C5642261114ECE48411EAD94A4C9E83106DF37D7EAE

Нәтижедегі мәндерді салыстырсақ, 23-байты кездейсоқтық сәйкестік.

Қорытынды: D21≠ D22 болғандықтан, критикалық нүктелер хештеу процесінен кейін коллизия тудындатпайды.

Келесі критикалық нүктелерді қарастырайық. Ол үшін S0-блоктағы 4 рет кездесетін (6,8) қиылысын қарайық. d1=6=0110 и d2=8=1000 үшін критикалық нүктелерді табайық:

Значений Po =>

Po+ P1=1= d1	S0(Po)+ S0(P1)= d2	Критикалық нүктелер
0000+0110	0110=6	
0001+0111	1100=C	
0010+0100	0111=7	
0011+0101	0001=1	
1000+1110	1000=8	1000=8, 1110=E
1001+1111	1111=F	
1010+1100	1000=8	1010=A, 1100=C
1011+1101	0011=3	

Әрі қарай біз критикалық нүктелер 8=1000, E=1110, A=1010, C=1100 ескеріп, тек басында ғана ерекшеленетін 4 ашық мәтінді таңдайық:

P1=80303030303030303030303030303130303030303030303030303030303032303030303030303030303030303031

P2=E0303030303030303030303030303130303030303030303030303030303032303030303030303030303030303031

P3=A0303030303030303030303030303130303030303030303030303030303032303030303030303030303030303031

P4=C0303030303030303030303030303130303030303030303030303030303032303030303030303030303030303031

Сәйкес шифрмәтіндер 1-раундтан соң төмендегідей болады:

C1=639251F26DC0C8A02AA24DEEB969EC07EF636A37B797C6DE05DF314A040421FA48E33E7F7319D0CA301FCCCB1FED5F87

C2=A69251F16DC090A02A9C4DEE2569EC0EEF631D37B74BC6DE64DF31590404D9FA48253E7F1A19D055301F48CB1FF95F87

C3=8C9251266DC0EFA02A504DEE2269ECAEEF63F837B70DC6DE72DF311804044BFA48CD3E7FDF19D065301F2BCB1F4C5F87

C4=6992515F6DC04CA02AAA4DEE1769ECB5EF637E37B7F0C6DE16DF31690404C8FA48F03E7F3319D0B8301FEECB1F4E5F87

4-раундтан соңғы шифрмәтін:

C1=90C5CA858FB3DEB493AE795C1A2D6044B89F0A08334AAE8A636C408E2406DC83022D971DA1B7B8B5CA57EDC16C9784B7

C2=1DB82C755A45E8C6ADC8FB414869D8A1CC8DF69D5C2374400683965D59E62C811F01146B3109B5621C5BF8132D0C3DDE

C3=9BA8F543FA45553C425ED785949943CE75D2E778E7AD852DC200DD519E099E13024A23D3ECFF81217AA8FBE181017ACF

C4=14A83D9FFF052C972BE94A043DF63A7EA65D635B53E69ECA25D6D5C371D37ED487EE91C036782561361A364DEEED75E6

Осы нәтижені D21= C1+C2, D22= C3+C4 тексерейік, сонда:

D21=8D7DE6F0D5F636723E66821D5244B8E57412FC956F69DACA65EFD6D37DE0F0021D2C837690BE0DD7D60C15D2419BB969

D22=8F00C8DC054079AB69B79D81A96F79B0D38F8423B44B1BE7E7D60892EFDAE0C785A4B213DA87A4404CB2CDAC6FEC0F29

Бұл мысалда да D21≠D22 болғандықтан, қарастырылған критикалық нүктелер – 1000=8, 1110=E, 1010=A, 1100=C хештеу процесінен кейін коллизия тудындатпайды.

Қорытынды

Бұл мақалада жаңа CF симметриялық блокты шифрлау алгоритміне негізделген НВС-256 хештеу алгоритмінде қолданылатын сызықты емес криптографиялық приминив - төрт 4-биттік S-блок зерттелген. Қазіргі уақытта алгоритмнің криптоберіктілігін қамтамасыз ететін осы компоненттер дифференциялдық криптоталдау әдісі арқылы беріктілігі бағаланды. Айырымдар кестесіндегі критикалық нүктелерге тәжірибе жүзінде талдау жүргізіліп, алғашқы бейнелер арасында коллизия туындату жағдайы талданды. Осындай талдауды барлық төрт S-блоктағы критикалық нүктелер үшін жүргізіп шығуға болады. Егер де алынған нәтиже D21= C1+C2, D22= C3+C4 есептелініп, D21≠D22 орындалатын болса, хештеу алгоритмдегі сызықты емес түрлендіру S-тар тудыратын критикалық нүктелер коллизия туындауға мүмкіндік бермейді. Зерттеу барысында D21= C1+C2, D22= C3+C4 мәндерін теңдіктердің салыстырмалы түрде орындалуы

ықтималдығын да ескерген жөн.

Алғыс

Жұмыс OR11465439 «Электрондық цифрлы қолтаңба үшін еркін ұзындықтағы хэштеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау» бағдарламалық-нысаналық қаржыландыру ғылыми жобасы аясында жүргізілді.

Әдебиеттер тізімі:

[1] Nita, S.L., Mihailescu, M.I. Hash Functions. In: Cryptography and Cryptanalysis in Java. Apress, Berkeley, CA. 2022. https://doi.org/10.1007/978-1-4842-8105-5_8

[2] Kheshaifaty N., Gutub A., Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication. Journal of Engineering Research. https://kuwaitjournals.org/jer/index.php/JER/article/download/13761/2687

[3] Farshim, P., Tessaro, S. Password Hashing and Preprocessing. In: Canteaut, A., Standaert, FX. (eds) Advances in Cryptology – EUROCRYPT 2021. Lecture Notes in Computer Science. 2021. 12697. Springer, Cham. https://doi.org/10.1007/978-3-030-77886-6_3

[4] Herrera J., Ali M. L. Concerns and Security for Hashing Passwords. 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2018. 861-865. doi: 10.1109/UEMCON.2018.8796720.

[5] Brogada M. D., Sison A. M., Medina R. P. Head and Tail Technique for Hashing Passwords. IEEE 11th International Conference on Communication Software and Networks (ICCSN), 2019. 805-810. doi: 10.1109/ICCSN.2019.8905384.

[6] Fomichev V., Bobrovskiy, D., Koreneva, A. et al. Data integrity algorithm based on additive generators and hash function. J Comput Virol Hack Tech. 2022. 18. 31–41. https://doi.org/10.1007/s11416-021-00405-y

[7] Wang J., Luo W., Hu Y., Jiang H. PN-HASH: An Immune-Inspired Scheme for Data Integrity Check. 12th International Conference on Advanced Computational Intelligence (ICACI), 2020. 340-348. doi: 10.1109/ICACI49185.2020.9177796.

[8] Thomas Espitau. Mitaka: Faster, Simpler, Parallelizable and Maskable Hash-and-Sign Signatures on NTRU Lattices. In Proceedings of the 8th ACM on ASIA Public-Key Cryptography Workshop (APKC '21). Association for Computing Machinery, New York, NY, USA, 1. https://doi.org/10.1145/3457338.3458293

[9] Belej, O., Staniec, K., Więckowski, T. The Need to Use a Hash Function to Build a Crypto Algorithm for Blockchain. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Theory and Applications of Dependable Computer Systems. DepCoS-RELCOMEX 2020. Advances in Intelligent Systems and Computing. 2020. 1173. Springer, Cham. https://doi.org/10.1007/978-3-030-48256-5_6

[10] N, Y., P, M. Radial kernelized regressive merkle–damgård cryptographic hash blockchain for secure data transmission with IoT sensor node. Peer-to-Peer Netw. Appl. 2021. 14. 1998–2010. https://doi.org/10.1007/s12083-021-01135-0

[11] Chilambarasan, N.R., Kangaiammal, A. Matyas–Meyer–Oseas Skein Cryptographic Hash Blockchain-Based Secure Access Control for E-Learning in Cloud. In: Suma, V., Chen, J.IZ., Baig, Z., Wang, H. (eds) Inventive Systems and Control. Lecture Notes in Networks and Systems. 2021. 204. Springer, Singapore. https://doi.org/10.1007/978-981-16-1395-1_65

[12] Patil, Harsha Kundan. Blockchain Technology-Security Booster. Blockchain Applications in IoT Security, edited by Harshita Patel and Ghanshyam Singh Thakur, IGI Global, 2021. 128-139. https://doi.org/10.4018/978-1-7998-2414-5.ch008

[13] Sakan K., Nyssanbayeva S., Kapalova N., Algazy K., Khompysh A., Dyusenbayev D. Development and analysis of the new hashing algorithm based on block cipher. Eastern-European Journal of Enterprise Technologies. Ukraine. 2022. 2/9(116). 60–73. https://doi.org/10.15587/1729-4061.2022.252060.

[14] Biham, E., Shamir, A. Differential cryptanalysis of the full 16-round DES. Advances in cryptology, proceedings of CRYPTO'92. 1992. 487-496.

[15] EliBiham, AdiShamir Differential Cryptanalysis of Hash Functions. Differential Cryptanalysis

of The Data Encryption Standard, Springer, 1993, ISBN 978-1-4613-0314-6. 133 – 148.

[16] Eli Biham, Orr Dunkelman, Differential Cryptanalysis in Stream Ciphers. Cryptology ePrint Archive, Report. 2007.218. http://eprint.iacr.org/

STUDY OF CRITICAL POINTS IN THE DIFFERENTIAL CRYPTOANALYSIS OF S-BLOCKS IN HASHING ALGORITHM "HBC-256"

S.Nyssanbaeva[1], K.S .Sakan[1,2]
[1]Institute of Information and Computational Technologies SC MES RK, Almaty, Kazakhstan,
[2]Kazakh National University named after al-Farabi, Almaty, Kazakhstan
E-mail: kairat_sks@mail.ru
[1]ORCID ID: https://orcid.org/0000-0002-5835-4958
[2]ORCID ID: https://orcid.org/0000-0002-6812-6000

Abstract. In this work described a differential cryptanalysis of the "HBC-256" algorithm one of the hashing algorithms developed at the Institute of Information and Computing Technologies of the RK MES CS, is provided. The HBC-256 algorithm is based on the block cipher of the CF (Compression Functions) and generates a 256-bit hash value. Like any new cryptographic structure, the HBC-256 algorithm requires careful research in order to confirm its cryptographic properties, namely: irreversibility and resistance to collisions of the first and second kind. As a result of the work, a software implementation of a new hashing algorithm using the C++ programming language was obtained. Differential properties of nonlinear hashing nodes (S-blocks) are considered for the HBC-256 hashing algorithm. Various options for constructing round characteristics are considered. Taking into account the main properties of differential cryptanalysis and based on the conclusions of other scientific works, the situation of pairs of open and corresponding closed texts at critical points is studied. In the conclusion of the article, it is concluded that the S-boxes of the hashing algorithm are resistant to situations where it is possible to cause a collision through critical points in the table of differences.

Keywords: hash algorithms, requirements for hash algorithms, basic methods of cryptanalysis, differential cryptanalysis.

ИССЛЕДОВАНИЕ КРИТИЧЕСКИХ ТОЧЕК ПРИ ДИФФЕРЕНЦИАЛЬНОМ КРИПТОАНАЛИЗЕ S-БЛОКОВ В АЛГОРИТМЕ ХЕШИРОВАНИЯ "HBC-256"

С.Е. Нысанбаева[1], Қ.С. Сақан[1,2]
[1]Институт информационных и вычислительных технологий МОН РК,Алматы, Казахстан
[2]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан,
E-mail: kairat_sks@mail.ru
[1]ORCID ID: https://orcid.org/0000-0002-5835-4958
[2]ORCID ID: https://orcid.org/0000-0002-6812-6000

Аннотация. В данной работе проводится дифференциальный криптоанализ алгоритма «HBC-256», одного из алгоритмов хеширования, разработанного в Институте информационных и вычислительных технологий МВОН Республики Казахстан. Алгоритм HBC-256 разработан на основе блочного шифра функции сжатия CF (Compression Function) и вырабатывает хэш-значение длиной 256 бит. Как любая новая криптографическая структура алгоритм HBC-256 требуют тщательного исследования с целью подтверждения его криптографических свойств, а именно: необратимости и устойчивости к коллизиям первого и второго рода. В процессе исследования алгоритма была использована программная реализация нового алгоритма хэширования с использованием языка программирования C++. Для алгоритма хэширования HBC-256 рассмотрены дифференциальные свойства нелинейных узлов хеширования (S-блоков). Рассмотрены различные варианты построения раундовых характеристик. С учетом основных свойств дифференциального криптоанализа и на основании выводов других научных работ исследуется ситуаций пар открытых и соответствующих им закрытых текстов в критических точках. В заключении статьи делается вывод о том, что S-блоки алгоритма хеширования устойчивы к дифференциальному криптоанализу и имеющие критические точки после хеширования не порождают коллизию.

Ключевые слова: симметричные алгоритмы шифрования, требования к алгоритмам шифрования, основные методы криптоанализа, атака методом бумеранга.

Авторлар жайында мәлімет:

Қаз: Сақан Қайрат – Әл-Фараби атындағы Қазақ ұлттық университетінің докторанты, kairat_sks@mail.ru

Рус: Сакан Кайрат – докторант Казахского национального университета им. аль-Фараби, kairat_sks@mail.ru

Англ: Sakan Kairat – a doctoral student at Al-Farabi Kazakh National University, kairat_sks@mail.ru

Қаз: Нысанбаева Сауле Екребулановна – Ақпараттық және есептеуіш технологиялар институты, т.ғ.д., профессор

Рус: Нысанбаева Сауле Екребулановна – Институт информационных и вычислительных технологий, д.т.н., профессор

Англ: Nysanbayeva Saule Ekrebulanovna – Institute of Information and Computing Technologies, Doctor of Technical Sciences, Professor

UDC 519.6
IRSTI 27.41.77

A METHOD FOR CALCULATING THE INFORMATION SECURITY RISK

D.K.Mukhayev[1,2], Marat Akhmet[3]

[1]Institute of Information and Computational Technologies
[2]Al-Farabi Kazakh National University
[3]Middle East Technical University, Ankara, Turkey
e-mail:daryn.mukhayev@gmail.com
[1]https://orcid.org/0000-0002-2985-286X
[3]https://orcid.org/0000-0002-3483-1182

Abstract. The article discusses the issues of identifying threats and vulnerabilities of information security violations. To protect information, it is necessary to create computer attack detection systems. Explanations were given on the concept of cyber attacks and their types were affected. No organization is currently sufficiently protected from cyber attacks. All organizations should develop a special plan to combat cybercriminals. A special plan allows you to prepare for emergencies, resist emerging threats and quickly restore the effect of the attack. The need to know the threatening factors and understand their tactics, methods and procedures to protect against cyber attacks is emphasized. The process of information protection should be comprehensive and continuous, carried out at all stages of the creation and use of automated data processing tools. The main methods of information protection are given.

Keywords: Information security, cyber attacks, cybercrime, information protection, threats, vulnerability.

Introduction

Due to the rapid development of science and technology, the influence of world information technologies on all spheres of production is increasing. In this regard, new social groups are being formed in society, the normal way of life of people is changing significantly. Information security issues related to the active informatization currently underway are of paramount importance. Many of them are aimed at creating a unified information space in order to optimize the processing of large amounts of information, including ensuring its reliable storage and accessibility for information exchange.

The main tasks set for the implementation of this goal are the identification, analysis and classification of information security threats that may lead to unauthorized receipt of information or disruption of the normal functioning of information systems, the definition of the main measures used to counter threats and eliminate vulnerabilities, the development of security criteria and mechanisms, as well as the relevant legislative and regulatory framework.

Analysis of existing threats and vulnerabilities of information security shows that achieving the goals and objectives of information protection, as well as ensuring a high level of security, requires a comprehensive application of available methods and means of protection. For this reason, one of the basic principles based on the development of information security concepts and specific information security tools is complexity.

The process of ensuring the protection of information should be comprehensive and continuous, carried out at all stages of the creation and use of automated data processing tools. The implementation of the information security process in these conditions is based on production conceptual approaches and the production of safety equipment. As a rule, highly qualified information security specialists are involved to create protective mechanisms and ensure their reliable and efficient operation.

Risk assessment as part of the direction of information security (risk management) is an essential tool in building protection. The risk assessment process is designed to identify the risk to an organization's business and determine the security measures taken to reduce the risk.

In the classical view, risk is the probability of the realization of an information security threat.

Risk assessment consists in modeling the picture of the occurrence of adverse conditions by taking into account all possible factors that determine the risk. From a mathematical point of

view, when analyzing risks, such factors can be considered input parameters. At the same time, it is necessary to take into account the many sources of information and the uncertainty of the information itself. At the risk assessment stage, the formulas and input data for calculating the risk value are of the greatest interest.

The article analyzes several different methods of risk calculation and presents its own methodology. The purpose of the work is to derive a formula for calculating the risk of information security, which allows obtaining an array of current risks and assessing losses.

Information security risk in the classical form is defined as a function of three variables:

probability of threat existence;

the probability of vulnerability (insecurity);

Potential impact.

If any of these variables approaches zero, then the total risk tends to zero.

Methods of risk assessment

According to the article «Information Technology. Security methods. Information security management systems. Requirements», the chosen methodology should ensure that risk assessments produce comparable and reproducible results. At the same time, the standard does not provide a specific calculation formula.

The NIST 800-30 «Risk management guide for information technology systems» provides the following classical formula for calculating risk:

$R = P(t) * S$,

Where, R is the risk value;

P(t) is the probability of an information security threat (a mixture is used qualitative and quantitative scales);

S – degree of threat impact on the asset (the asset price on a qualitative and quantitative scale).

As a result, the risk value is calculated in relative units, which can be ranked according to the degree of significance for the information security risk management procedure.

According to the article «Information Technology. Methods and means of ensuring security. Methods of information technology security management», risk calculation in contrast to the NIST 800-30 standard «Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology» occurs according to the following formula:

$R = P(t) * P(v) * S$,

where P(t) is the probability of an information security threat;

P(v) – probability of vulnerability;

S is the value of an asset (resource).

As an example of the values of probabilities P(t) and P(v), a qualitative scale with three levels (low, medium and high) is given. To assess the value of asset S, numerical values are presented in the range from 0 to 4. The comparison of qualitative values should be made by the organization in which information security risks are assessed.

According to the "Information Security Management System Specification", the risk level is calculated taking into account the following indicators: the value of the resource, the threat level and the degree of vulnerability. As the values of these parameters increase, the risk increases. Thus, the formula can be represented as follows:

$R = S * L(t) * L(v)$,

Where, S is the value of the asset (resource);

L(t) – threat level;

L(v) – level (degree of vulnerability).

In practice, information security risks are calculated according to the positioning table of the threat level values, the degree of probability of vulnerability use and the value of the asset. The risk value can vary in the range from 0 to 8, as a result, a list of threats with different risk values is obtained for each asset. The standard offers the following risk ranking scale: low (0-2), medium (3-5) and high (6-8). This allows you to identify the most critical risks.

According to the «Methodology for assessing the risks of information security violations», the assessment of the degree of the possibility of implementing an information security threat is carried out on the following qualitative and quantitative scale: unrealizable threat - 0%, average – from 21% to 50%, etc.

To perform a qualitative assessment of information security risks, a table of compliance with the severity of the consequences and the probability of threat realization is used. If it is necessary to make a quantitative assessment, then the formula can be presented as follows:

$R = P(v) * S,$

Where, S is the severity of the consequences.

Having considered all of the above methods of risk assessment in terms of calculating the value of information security risk, it is worth noting that the risk calculation is performed using the threat value and asset value. A significant disadvantage is the valuation of assets (the amount of damage) in the form of conditional values. Conditional values do not have units of measurement applicable in practice.

As a result, this does not give a real representation of the level of risk that can be transferred to the real assets of the object of protection.

Thus, it is proposed to divide the risk calculation procedure into the following stages:

calculation of the technical risk value;

calculation of potential damage.

Technical risk is understood to mean the importance of information security risk, consisting of the probabilities of the implementation of threats and the use of vulnerabilities of each component of the information infrastructure, taking into account the level of their confidentiality, integrity and availability. For the first stage , the following formulas can be given:

$Rc = Kc * P(T) * P(V);$

$Ri = Ki * P(T) * P(V);$

$Ra = Ka * P(T) * P(V),$

where Rc is the value of privacy risk;

Cc – coefficient of confidentiality of an information asset (resource);

P(T) – probability of threat realization;

P(V) – the probability of using the vulnerability;

Ri – value of integrity risk;

Ki is the integrity coefficient of an information asset (resource);

Ra – availability risk value;

Ka – coefficient of availability of an information asset (resource).

In the future, it is possible to calculate the damage value. To do this, the average value of the risk of each information asset and the amount of potential losses are used. The damage value (L) is calculated using the following formula:

$L = Ravg * S,$

Where, Ravg is the average risk value;

Conclusion

The use of this algorithm will make it possible to make a more detailed risk assessment, as a result, to obtain a dimensionless value of the probability of the risk of compromising each information asset separately.

Also, the proposed methodology allows you to correctly assess the value of information security risk and assess losses in the event of security incidents.

As part of future research, it is planned to consider ways to improve the quality of the forecast about threats and vulnerabilities of information security.

References

[1] Kirsanov, K.A. Information security: Textbook K. A. Kirsanov, A.V. Malyavina, N. V. Popov; Moscow. acad. Economics and Law. – Moscow: MAEP, 2020

[2] Koneev, I.R. Information security of the enterprise: [Inform. safety. Classification of attacks. Risk management methodology. Cryptographer. tools and mechanisms] Iskander Koneev, Andrey Belyaev. – St. Petersburg: BHV-Petersburg, 2021

[3] Melnikov, V.V. Information protection in computer systems: – M.: Finance and Statistics. Electroinform, 2014

[4] Shakovets, A.N. Fundamentals of computer information protection and information security: Lecture by A.N. Shakovets, N.V. Rymareva; M-in internal. Affairs of Russia, Far East. jurid. in- – Khabarovsk: Far East. jurid. in-t of the Ministry of Internal Affairs of the Russian Federation, 2021

[5] Smagin A.A., Poletaev V.S. Algorithm for forecasting threats to information security. Infocommunication technologies. 2018. 16(2). 192-198.

[6] Yazan Alshboul, Kevin Streff. Analyzing Information Security Model for Small-Medium Sized Businesses: Twenty-first Americas Conference on Information Systems, Puerto Rico. 2015. DOI: https://core.ac.uk/download/pdf/301365935.pdf

[7] Julian Jang-Jaccard, Surya Nepal. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 2014. 80(5). 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

[8] Top cybersecurity threats on enterprise networks: https://www.ptsecurity.com/ww-en/analytics/network-traffic-analysis-2020/

[9] Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri.2018. The Privacy Implications of Cyber Security Systems: A Technological Survey.ACM Comput. Surv.51,2, Article 36 (February 2018), 27 pages. https://doi.org/10.1145/3172869

[10] Obotivere B. A., Nwaezeigwe A. O.. Cyber Security Threats on the Internet and Possible Solutions, IJARCCE 9(9). 2020. 92-97. DOI: 10.17148/IJARCCE.2020.9913

[11] Information technology. Security methods. Information security management systems. Requirements: ISO/IEC 27001. – Introduction. 06.01.2018. – Moscow: Standartinform, 2018. 54.

[12] Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology : NIST 800-30. – Introduction. 06.01.2020. – USA. 2020. 56.

[13] Information technology. Methods and means of ensuring security. Part 3. Methods of information technology security management: GOST R ISO/IEC T13335-3-2017. – Introduction. 01.09.2017. Moscow: Standartinform, 2017. 76.

[14] Specification of the information security management system: BS 7799-2:2005. –Introduction. 01.07.2019. – England. 2019. 86.

[15] Ensuring information security of organizations of the banking system of the Russian Federation. Methodology for assessing the risks of information security violations: RS BR IBBS-2.2-200. – Introduction. 06.01.2019. – Moscow: Standartinform, 2019. 23.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛІН ЕСЕПТЕУ ӘДІСІ

Д.К.Мухаев[1,2], Марат Ахмет[3]
[1]Ақпараттық және есекптеуіш технологиялар институты, Алматы, Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Казақстан
[3]Таяу Шығыс техникалық университеті, Анкара, Түркия
e-mail:daryn.mukhayev@gmail.com
[1]https://orcid.org/0000-0002-2985-286X
[3]https://orcid.org/0000-0002-3483-1182

Аңдатпа. Мақалада ақпараттық қауіпсіздікті бұзудың қатерлері мен осалдықтарын анықтау мәселелері талқыланады, ақпаратты қорғау үшін компьютерлік шабуылдарды анықтау жүйелерін құру қажеттілігі негізделеді. Кибершабуылдар түсінігі бойынша түсіндірмелер беріледі және олардың түрлері әсер етеді. Қазіргі уақытта ешбір ұйым кибершабуылдардан абсолютті қауіпсіздікті қамтамасыз етпейді. Барлық ұйымдар пайда болатын қауіптерге қарсы тұру және тез

қалпына келтіру үшін арнайы киберқылмыстық жоспарларды әзірлейді (осылайша шабуылдың әсерін азайтады). Қауіпті факторларды білу және кибершабуылдардан қорғау тактикасын, әдістері мен процедураларын түсіну қажеттілігі атап өтіледі. Ақпаратты қорғау процесі ақпаратты өңдеудің автоматтандырылған құралдарын жасау мен пайдаланудың барлық кезеңдерінде жүзеге асырылатын жан-жақты және үздіксіз болуы керек. Ақпаратты қорғаудың негізгі әдістері келтірілген.

Түйінді сөздер. Ақпараттық қауіпсіздік, кибершабуыл, киберқылмыскер, ақпаратты қорғау, қауіптер, осалдықтар.

МЕТОД РАСЧЕТА РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.К.Мухаев[1,2], Марат Ахмет[3]
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Казахский национальный университет имени аль-Фараби, Казахстан
[3]Ближневосточный технический университет, Анкара, Турция
e-mail:daryn.mukhayev@gmail.com
[1]https://orcid.org/0000-0002-2985-286X
[3]https://orcid.org/0000-0002-3483-1182

Аннотация. В статье рассматриваются вопросы выявления угроз и уязвимостей нарушения информационной безопасности, обоснована необходимость создания систем обнаружения компьютерных атак для защиты информации. Даны разъяснения по понятию кибератак и затронуты их виды. В настоящее время ни одна организация не обеспечивает абсолютную защищенность от кибератак. Все организации разрабатывают специальные планы по борьбе с киберпреступниками, позволяющие противостоять возникающим угрозам и быстро восстанавливаться (тем самым уменьшая последствия от эффект атаки). Подчеркивается необходимость знания угрожающих факторов и понимания тактики, методов и процедур для защиты от кибератак. Процесс защиты информации должен быть комплексным и непрерывным, осуществляться на всех этапах создания и использования автоматизированных средств обработки данных. Приведены основные методы защиты информации.

Ключевые слова. Информационная безопасность, кибератака, киберпреступность, защита информации, угрозы, уязвимость.

Авторлар жайында мәлімет:
Қаз: Мухаев Дарын – Әл-Фараби атындағы Қазақ ұлттық университетінің докторанты, daryn.mukhayev@gmail.com
Рус: Мухаев Дарын – докторант Казахского национального университета им. аль-Фараби, daryn.mukhayev@gmail.com
Англ: Mukhayev Darin – a doctoral student at Al-Farabi Kazakh National University, daryn.mukhayev@gmail.com

Қаз:Марат Ахмет, профессор, Таяу Шығыс техникалық университеті, Анкара, Түркия
Рус: Марат Ахмет, профессор, Ближневосточный технический университет, Анкара, Турция
Англ:Marat Akhmet, professor, Middle East Technical University, Ankara, Turkey
Орынбай Мажит Темирбекулы – студент Казахского национального университета имени Аль-Фараби, temirbek.majit@gmail.com

МРНТИ 20.15.05

ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Жумашев Н.Ж., Кусепова Л.Т.
Международный университет Астана, Нур-Султан, Казахстан
e-mail: nurik.universal@gmail.com
https://orcid.org/0000-0002-7972-3169

Аннотация. Актуальность данного исследования состоит в том, что облачными системами в сегодняшние дни пользуются не только определенные группы пользователей, а также множество компаний применяют их как хранилище данных и используют для осуществления обмена данными. Облачные вычисления состоят из таких основных компонентов, как ядро платформы, интерфейс, хранилище данных, управление пользователями, функционирование приложений, которым обязательно нужно осуществлять мониторинг системы в целом и обеспечивать их защиту. Соответственно в данной статье было особое внимание уделено облачным вычислениям и их различным подходам обеспечения безопасности, а также методам шифрования данных, осуществляющим шифрование с симметричным и асимметричным ключами. Система облачных вычислений могут быть подвержены к различным угрозам безопасности, а именно угрозам конфиденциальности, целостности, доступности данных и облачной инфраструктуры.

Ключевые слова: облачные вычисления, безопасность, конфиденциальность, Docker, Kubernetes

Введение

Облачные платформы предоставляют свои ресурсы в виде сервисов, поддерживающих различные услуги, в которой обеспечиваются подходящей инфраструктурной поддержкой пользовательские приложения. Благодаря поддержке управления облачными приложениями осуществляется удобный доступ к аппаратно-программным платформам, т.е. вычислительным ресурсам в виде сетей, устройств хранения данных, приложений. В состав облачной платформы входит следующие основные компоненты:

Ядро платформы: осуществляет интеграцию облачных сервисов со средами и наборами утилит.

Интерфейс: пользователь через различные API и веб-интерфейсы взаимодействуют с облаком.

Хранилище данных: хранятся большие объемы данных.

Управление пользователями: оптимизируются и подстраивается под задачи пользователей.

Мониторинг функционирования приложений и их поддержка: осуществляется интеграция приложения с облачными сервисами.

Каждый из этих компонентов уязвим к программным или иным ошибкам, допущенными пользователями и сервисом.

Облачные вычисления имеют ряд преимуществ, которые побудили пользователей и клиентов перенести свои данные в облако, использовав при этом облачные серверы. Любая форма информации и данные клиентов загружаются на облачные сервера и могут быть сохранены на хранилище данных облачного провайдера, который предоставляет множество услуг. Соответственно вся информация и данные пользователей должны быть защищены и обеспечены безопасностью. Иначе это могло привести к утечке данных и получению несанкционированного доступа злоумышленниками.

Система облачных вычислений могут быть подвержены к различным угрозам безопасности, а именно угрозам конфиденциальности, целостности, данных и облачной инфраструктуры.

Обзор литературы

Актуальность данного исследования обусловливается тем, что облачные вычисления становятся неотъемлемой частью повседневной жизни каждого гражданина, также компаний, при этом возрастает необходимость обеспечения безопасности каждого компонента в моделях обслуживания и развертывания облачных сервисов. Для развертывания облачных вычислений и предоставления ресурсов пользователям применяются технологии виртуализации, контейнеризации и оркестровки. При виртуализации клиентам предоставляются виртуальные ресурсы, а контейнеризация упрощает виртуализацию за счет специальной конструкции контейнеров в виде пакетов приложений из отдельных образов.

В работе Серикулы О. [1] описываются потенциальные угрозы информационной безопасности в технологии виртуализации, к примеру, пользование общего хранилища данных разными виртуальными машинами. Виртуальные машины могут клонироваться и перемещаться между физическими серверами. Каждая виртуальная машина хранится в виде отдельных файлов и могут быть изменены по необходимости от нужд пользователя, т.е. уменьшение и увеличение размера разделов могут привести к изменению физических секторов и перемещению данных с одной виртуальной машины на другую.

В работе [2] рассматривается использование технологии контейнеризации при разработке программ. Самыми популярными технологиями контейнеризации являются Docker и Kubernetes. Безопасность Kubernetes основана на следующих принципах: облако, кластер, контейнер и код. Основой безопасности Kubernetes является базовая физическая инфраструктура. Защита кластера включает компоненты API и все приложения. При обеспечении безопасности контейнеров производится сканирование контейнеров на наличие уязвимостей во время сборки. Код является поверхностью для атаки любой среды Kubernetes и обеспечение его безопасности является главной необходимостью системы, регулярное тестирование и сканирование могут предотвратить возникновение проблем безопасности в данной среде.

В работе [3] криптография определяется решением множеств проблем, а именно он помогает обеспечивать конфиденциальность, целостность и доступность информации, т.е. преобразовывает данные из простой формы в зашифрованную. При шифровании и дешифровании используются ключи. По количеству ключей криптографию разделяют на криптосистемы с асимметричным ключом и с симметричным ключом [3]. К шифрам с симметричным ключом относятся DES, Triple DES, blowfish, AES, а к асимметричным – RSA, ElGamal, DSA. Они имеют как преимущества, так и недостатки. В зависимости от этого сейчас применяются гибридный криптографический подход.

В статье M. K. Sinchana and R. M. Savithramma [4] представили обзор по безопасности облачных вычислений. В работе были изучены набор гибридных криптографических моделей и их конструкция, описаны преимущества и реализация каждой модели. Тут же рассматривается повышение безопасности и его эффективность осуществляется комбинированием симметричными и асимметричными видами шифрования.

В [5] работе был выполнен сравнительный анализ шести различных работ, использующие схемы дедупликации для эффективного доступа к облачным серверам. В качестве основных параметров, учитывающих при измерении производительности были производительность записи, размеры фрагментов и использование оперативного запоминающего устройства. Дедупликация снижает нагрузки на сервер, обеспечивая при этом, безопасный доступ к данным и помогает избежать избыточности данных. В работах, рассмотренные в данной статье объединяют безопасность и дедупликацию, обеспечивающую высокую производительность с точки зрения использования энергии, скорости доставки пакетов и временной задержки [5].

В работе [6] определяет дедупликацию данных как ограничительного подхода для удаления идентичных документов с повторяющейся информацией в репозитории. Данный метод используется для увеличения репозитория и уменьшения полосы пропускания.

В работе [7] представлен алгоритм конвергентного шифрования для обеспечения безопасности данных в облачных вычислениях. Чтобы найти дубликат документа и провести анализ типа документа и его преобразования в байт используется анализ границ на уровне индекса. Если копия документа была отклонена, то на следующем уровне документ преобразовывается в формат шифрования с использованием конвергентного шифрования.

Управление безопасностью облачной среды постоянно интегрируется и изменяется, т.к. это обусловлено тем, что злоумышленники могут использовать уязвимости, вызванные впоследствии неправильных манипуляции пользователей или конфигурациями системы. Приспособляемость модели безопасности является критически важным требованием при рассмотрении ее для облачных сред [8].

Методы исследования

В данной работе был проведен анализ статей, рассматривающих безопасность облачных вычислений и изучены методы шифрования, AES, DES, 3DES, RSA и определены следующие параметры оценки, включающее время шифрования и дешифрования, пропускную способность и длину зашифрованного текста. Время процесса шифрования зависит от увеличения количества символов. Время процесса дешифрования показывает восстановление исходных данных по истечению какого-то промежутка времени. Вычислить его можно по следующей формуле:

$$Time = Time_{end} - Time_{start} \quad (1),$$

где Time означает потребляемое время, Timeend – время окончания и Timestart – время начала.

Эффективность алгоритмов обеспечения безопасности в облачных вычислениях можно проанализировать с помощью его пропускной способности. Пропускная способность алгоритма прямо пропорциональна производительности, т.е. чем выше производительность, тем выше пропускная способность [8]. Формула, которая рассчитывает пропускную способность методов шифрования, выглядит следующим образом:

$$Th = Size_{Plain\_text} / Time_{enc} \quad (2)$$

где Th означает пропускную способность, $Size_{Plain\_text}$ – размер обычного текста и $Time_{enc}$ – время кодирования.

При шифровании на стороне клиента данные шифруются перед загрузкой на сервер, а объем загруженных данных напрямую влияет на время передачи [9].

Защита сервисов облачных систем не ограничиваются шифрованием, также для этого необходим комплексный подход, предусматривающий весь жизненный цикл процессов облачных систем, зависимостей, межсервисных взаимодействий, вызовов внешних библиотек, уязвимости.

При рассмотрении безопасности облачных сервисов как SaaS, определяются характеристики поведения приложения и уязвимости системы. Приложения можно классифицировать по характеру поведения следующим образом: безопасный, вредоносный и уязвимый. Состояние приложения диагностируются с точки зрения потенциального риска, проверки поведения и угроз безопасности. Риск безопасности можно подразделить на критическую, высокую, среднюю и низкую. Для каждого

обнаруженного небезопасного потока уровень риска равен максимальному уровню безопасности его источника [10].

Результаты и обсуждение

В данной работе были исследованы вопросы организации и обеспечения безопасности в облачных вычислениях и нацелена на определение эффективности алгоритмов защиты облачных систем в целом. При диагностике безопасности нужно рассматривать его в соответствии с основными моделями облачных вычислений: в плане инфраструктуры как сервис (IaaS), платформы как сервис (PaaS) и программное обеспечение как сервис (SaaS). Защита сервисов облачных систем применяется комплексный подход, предусматривающий весь жизненный цикл процессов облачных систем, зависимостей, межсервисных взаимодействий, вызовов внешних библиотек и уязвимости.

Выводы

Рассмотрев вопросы организации и обеспечении безопасности в облачных вычислениях можно сделать вывод о нижеследующем:

- не рекомендуется разрешать реестрам и сомнительным службам работать в облаке;
- нужно следить за тем, чтобы никто не получил доступ к информации о кредитных картах и транзакциях;
- учетные данные для входа в облачную систему должны быть надежно защищены, механизмы обмена учетными данными должны быть установлены должным образом;
- соединения API между моделями обслуживания должны быть правильно установлены;
- критерии сетевой безопасности должны соответствовать уровню безопасности IaaS;
- нужно периодически выполнять сканирование уязвимостей и проверку настроек;
- шифровать данные, находящиеся на облачном сервисе;
- необходимо использовать двухфакторную аутентификацию для доступа в систему;
- необходимы комплексные процедуры безопасности и управления данными, т.е. выполнять дедупликацию данных.

Список литературы

[1] Серикулы О. Информационная безопасность при облачных вычислениях. Вестник магистратуры. 2019. 6-5(93).

[2] Мельникова А.Е., Рычков В.А. Использование технологии контейнеризации при безопасной разработке программного обеспечения. Материалы второго международного научно-практического форума по экономической безопасности «VII ВСКЭБ». – Москва, 2021.

[3] Murad Sh.H., Rahouma K.H. Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. Procedia Computer Science. 2021. 194. 165–172.

[4] Sinchana M. K., Savithramma R. M. Survey on Cloud Computing Security. In Innovations in Computer Science and Engineering. Springer, Singapore, 2020. 1-6.

[5] Pragash K., Jayabharathy J. A survey on DE – Duplication schemes in cloud servers for secured data analysis in various applications. Measurement: Sensors. 2022.

[6] Geeta C.M., Shreyas R.Ga. Raju, Raghavendra S., Rajkumar B., Venugopal K.R., Iyengard S.S., Patnaik L.M. SDVADC: Secure Deduplication and Virtual Auditing of Data in Cloud. Procedia Computer Science. 2020. 2225–2234.

[7] Krishnasamy V., Venkatachalam S. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. Materials Today: Proceedings. 2021.

[8] Irsheida A., Murada A., AlNajdawia M., Qusef A. Information security risk management models for cloud hosted systems: A comparative study. Procedia Computer Science. 2022. 205–217.

[9] Thabit F., Alhomdy Sh., Jagtap S. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. International Journal of Intelligent Networks. 2021. 18-33.

[10] Elsayed M., Zulkernine M. Offering security diagnosis as a service for cloud SaaS applications. Journal of Information Security and Applications. 2019. 32-48.

References

[1] Serikuly O. Informatsionnaya bezopasnost' pri oblachnykh vychisleniyakh. Vestnik magistratury. 2019. 6-5(93).

[2] Mel'nikova A.Ye., Rychkov V.A. Ispol'zovaniye tekhnologii konteynerizatsii pri bezopasnoy razrabotke programmnogo obespecheniya. Materialy vtorogo mezhdunarodnogo nauchno-prakticheskogo foruma po ekonomicheskoy bezopasnosti «VII VSKEB». – Moskva, 2021.

[3] Murad Sh.H., Rahouma K.H. Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. Procedia Computer Science. 2021. 194. 165–172.

[4] Sinchana M. K., Savithramma R. M. Survey on Cloud Computing Security. In Innovations in Computer Science and Engineering. Springer, Singapore, 2020. 1-6.

[5] Pragash K., Jayabharathy J. A survey on DE – Duplication schemes in cloud servers for secured data analysis in various applications. Measurement: Sensors. 2022.

[6] Geeta C.M., Shreyas R.Ga. Raju, Raghavendra S., Rajkumar B., Venugopal K.R., Iyengard S.S., Patnaik L.M. SDVADC: Secure Deduplication and Virtual Auditing of Data in Cloud. Procedia Computer Science. 2020. 2225–2234.

[7] Krishnasamy V., Venkatachalam S. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. Materials Today: Proceedings. 2021.

[8] Irsheida A., Murada A., AlNajdawia M., Qusef A. Information security risk management models for cloud hosted systems: A comparative study. Procedia Computer Science. 2022. 205–217.

[9] Thabit F., Alhomdy Sh., Jagtap S. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. International Journal of Intelligent Networks. 2021. 18-33.

[10] Elsayed M., Zulkernine M. Offering security diagnosis as a service for cloud SaaS applications. Journal of Information Security and Applications. 2019. 32-48.

БҰЛТТЫ ЕСЕПТЕУЛЕРДІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ЖӘНЕ ҰЙЫМДАСТЫРУ

Жумашев Н.Ж., Кусепова Л.Т.
Астана Халықаралық университеті, Нұр-Сұлтан, Қазақстан
e-mail: nurik.universal@gmail.com
https://orcid.org/0000-0002-7972-3169

Аңдатпа. Бұл зерттеудің өзектілігі, бүгінгі таңда, бұлтты жүйелерді қолданушылардың белгілі бір топтары ғана емес, сонымен қатар көптеген компаниялар оларды деректер қоймасы ретінде және деректермен алмасу үшін пайдаланады. Бұлтты есептеулер платформа ядросы, интерфейс, деректер қоймасы, қолданушыларды басқару, қосымшалардың жұмыс жасауынан құралатын негізгі компоненттерден тұрады, сондықтан жүйені тұтастай мониторинг жүргізіп, олардың қорғалуын қамтамасыз ету керек. Тиісінше, осы мақалада бұлтты есептеулерге және оның әр түрлі қауіпсіздік тәсілдеріне, сондай-ақ симметриялық және асимметриялық кілттермен шифрлауды жүзеге асыратын деректерді шифрлеу әдістеріне ерекше назар аударылды. Бұлтты есептеу жүйесі әр түрлі қауіпсіздік қатерлеріне, атап айтқанда, құпиялылық, тұтастық, деректердің қолжетімділігі және бұлтты инфрақұрылым қауіптеріне ұшырауы мүмкін.

Кілттік сөздер: бұлтты есептеулер, қауіпсіздік, құпиялылық, Docker, Kubernetes

ORGANIZATION AND SECURITY OF CLOUD COMPUTING

Zhumashev N. Zh. , Kusepova L. T.
Astana International University, Nur-Sultan, Kazakhstan

e-mail: nurik.universal@gmail.com
https://orcid.org/0000-0002-7972-3169

Abstract. The relevance of this study lies in the fact that today not only certain groups of users use cloud systems, but also many companies use them as a data warehouse and use them to exchange data. Cloud computing consists of such basic components as the platform core, interface, data storage, user management, application operation, which must monitor the system as a whole and ensure their protection. Accordingly, in this article, special attention has been paid to cloud computing and its various security approaches, as well as data encryption methods that perform encryption with symmetric and asymmetric keys. A cloud computing system can be exposed to various security threats, namely confidentiality, integrity, data availability and cloud infrastructure threats.

Keywords: cloud computing, security, privacy, Docker, Kubernetes

Авторлар жайында мәлімет:

Қаз.: Жумашев Нурдаулет Жанибекулы - Астана халықаралық университетінің студенті, nurik.universal@gmail.com

Рус.: Жумашев Нурдаулет Жанибекулы - студент Международного университета Астана, nurik.universal@gmail.com

Англ. Zhumashev Nurdaulet Zhanibekuly - student of Astana International University, nurik.universal@gmail.com

Қаз.: Кусепова Лаззат Тұңғышбайқызы - Астана халықаралық университетінің аға оқытушысы, lazzatk@mail.ru

Рус.: Кусепова Лаззат Тұңғышбайқызы - старший преподаватель Международного университета Астана, lazzatk@mail.ru

Англ.: Kusepova Lazzat Tungyshbaikyzy - senior lecturer at Astana International University, lazzatk@mail.ru

Responsible for the release: PhD, Shayakhmetova A.S.
Merkebaev A.

Deputy chief editor: PhD, Mamyrbayev O.Zh

Signed in print 03.03.2020
Edition of 50 copies. Format 60x84 1/16. Paper type.
Order No. 4.

Publication of the Institute of Information and Computational Technologies

28 Shevchenko str., Almaty, Republic of Kazakhstan
7 (727) 272-37-11
atcs@iict.kz