

Improving Methods for Generating Encryption Keys Using Strange Attractors

Volodymyr Shevchenko¹, Igor Sinitsyn², Viktor Shevchenko²

¹ Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street 24, Kyiv, 02000, Ukraine

² Institute of Software Systems of the National Academy of Sciences of Ukraine, Academician Glushkov Avenue 40, Kyiv, 03187, Ukraine

Abstract

The urgency of the work is determined by the need to transfer confidential information through open communication channels. Such information can be of two types: symmetric encryption keys and directly informational messages that are encrypted with encryption keys. The article deals with the problem of improving the transmission of closed information over open channels using the Diffie-Hellman algorithm. The improvement is due to the introduction of a new type of one-way function based on the numerical solution of the system of ordinary differential equations describing the dynamics of the phase coordinate movement of the strange attractor. For this purpose, the classic Diffie-Hellman algorithm based on the one-way function of the discrete logarithm was considered. The required properties of one-way functions in the general case were considered. Next, the peculiarities of algorithm modification in the case of transition to a one-way function based on the use of a strange attractor were considered. It is assumed that at the beginning of the operation of the modified algorithm, through a secret channel, the exchange parties (agents) exchange information regarding the properties of the strange attractor to be used, namely, the definition of the differential equations describing the dynamics of a strange attractor, the values of the parameters of the equations, the initial integration conditions and the integration step (for methods with a constant step of integration). After that, all exchanges are conducted exclusively through open channels. The paper also considers the case of information exchange between more than two agents, in particular, the approach of hiding the number of agents participating in the exchange. Approbation of the method is carried out, and intermediate and final results of the one-way function based on strange attractors are given. Possibilities regarding partial disclosure by agents of certain parameters of the use of one-way functions are discussed. But at the same time, the safety of revealing such information is justified in the general case (both in the classical and in the modified Diffie-Hellman method). It was determined that depending on the needs of users, the complexity of the encryption keys can be increased by changing the initial parameters of the attractor, which will also allow controlling the speed of key generation and encryption in general. The proposed modified algorithm's software is implemented in three programming languages: C#, Python, and MatLab. This made it possible to perform a comparative analysis of the results and consciously choose the programming language of individual parts of the software to optimize the encryption key generation process for specific conditions.

Keywords

information protection, information exchange, Diffie-Hellman algorithm, one-way functions, strange attractors, open channels, encryption keys

13th International Scientific and Practical Conference from Programming UkrPROGP'2022, October 11-12, 2022, Kyiv, Ukraine


EMAIL: vladimir_337@ukr.net (A. 1); ips2014@ukr.net (A. 2); gii2014@ukr.net (A. 3)

ORCID: 0000-0002-2152-6816 (A. 1); 0000-0002-4120-0784 (A. 2); 0000-0002-9457-7454 (A. 3)



© 2022 Copyright for this paper by its authors.

Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

1. Introduction

In current conditions, the exchange of digital information has reached an unprecedented scale and covered all spheres of human activity. The proper activity of any country and its citizens is only possible with the intensive exchange of digital information. Accordingly, the relevance of protecting this information is growing. Today it is not enough just to get useful information. In the face of constant cyber attacks, mostly epidemiological characters [1, 2], it is necessary to reliably protect information at all stages of its collection, processing, storage, and transmission. Information protection requires the expenditure of quite significant resources [3]. One of the areas of information protection is encryption [4]. However, breaking ciphers today is only a matter of available machine time. With the constant increase in the computing power of computers, as well as reducing the cost of their use, it is becoming increasingly difficult to ensure the security of transmission and storage of information on the Internet. Usually, passwords generated by people are not reliable enough, as evidenced by research: an experienced hacker can crack more than a third of passwords in 4 hours, two-thirds in a week, and 9 out of 10 passwords in 5 weeks.

Ensuring secure data transmission over open communication channels is especially acute [5]. Often, information must be transmitted continuously and in large volumes, in particular, transferring data between banks [6, 7, 8] or other large companies. For this purpose, the Diffie-Hellman algorithm [9] is usually used, which allows the creation of common keys for encrypting information. Its classical version uses an arithmetic **one-way function** with commutativity properties, such as based on a discrete logarithm, to generate encryption keys [9]. To decrypt information, the attacker must find the inverse function. In conditions when the one-way function of the algorithm, although complex, remains arithmetic, the selection of the function seems possible. It can be performed relatively quickly (in the presence of significant computing power, the availability of which is increasing every day). Therefore, increasing the cracking strength of ciphers by searching for fundamentally new one-way functions is an urgent task.

For example, in [8, 10], cellular automata with an extended set of rules regarding the life and death of cells were used to create one-way functions. The reason for this choice of a one-way function was a wide variety of behavioral options for colonies of cellular automata. This ensured, on the one hand, quasi-randomness of the model behavior and, on the other hand, absolute repeatability of the simulation results. A similar effect could be achieved by modeling the dynamics of real-world ecosystems based on systems of ordinary differential equations [11] or deterministic chaos models [12]. However, the numerical solutions of ordinary differential equations are quite predictable, and the models of deterministic chaos require more diversity. As a solution in this paper, it is proposed to use the models of strange attractors.

Consider the possibility of creating one-way functions based on the numerical solution of differential equations describing the dynamics of the behavior of strange attractors. Currently, many strange attractors have been discovered. All of them are chaotic, which makes it possible to use them to generate pseudorandom numbers. At the same time, they also have a sufficiently high level of reproducibility in the numerical calculation of their phase trajectories.

Purpose of the paper. To improve the quality of creating shared encryption keys using open communication channels within the Diffie-Hellman algorithm by creating a one-way function based on modified strange attractors.

2. The classical Diffie-Hellman algorithm

Consider the classic version of the Diffie-Hellman algorithm.

When it is necessary to change passwords or encryption keys constantly, access to closed communication channels is usually either absent or requires too many resources. The Diffie-Hellman algorithm allows using open communication channels to generate encryption keys without any significant risk of compromising the generated keys. More precisely, agents have only one opportunity to use a closed communication channel, but all subsequent communication takes place over open communication channels.

The algorithm is as follows:

1. At the first communication via a closed channel, the agents determine the properties of the one-way function. In the classical version of the algorithm, a discrete logarithm is used as a one-sided function [9, 13]. In our case, it is proposed to use a strange attractor, for which all the necessary properties are determined in this communication session: differential equations describing the dynamics of a particular attractor, the values of the parameters of the equations, the initial conditions of integration and the integration step (for methods with a constant integration step).

2. The first agent forms a secret word x_1 (in our case, the number of integration steps of the attractor). In this case, the parameter y_0 is the initial value of the function (in our case, the initial coordinates of the point in space from which the construction of the attractor begins). The first agent finds the intermediate value of the function

$$y_1 = f(y_0, x_1)$$

and sends the intermediate value of the function to the second agent through the open channel.

3. The second agent receives the intermediate value of the function y_1 from the first agent, generates its secret word x_2 , and uses the same function. Now the second agent knows the new encryption key

$$y_{12} = f(y_1, x_2).$$

4. Then the agents act similarly (steps 2, 3), but now they change places:

$$y_2 = f(y_0, x_2); \quad y_{21} = f(y_2, x_1).$$

Since the function is commutative, then

$$y_{21} = f(y_2, x_1) = f(y_1, x_2) = y_{12}.$$

Thus, both agents have formed a new encryption key y_{21} .

Probable attackers listen to the open channel and know the intermediate values of the function y_1, y_2 , but do not know the new key y_{21} and the initial values of y_0 .

3. The classical one-way functions

As already mentioned, one of the common variants of the one-way function is the discrete logarithm. Consider its use for the above Diffie-Hellman algorithm.

Initially, the agents generate numbers g and p that are not secret and possibly known to the attacker. Then agents separately generate secret words - vast numbers x_1 and x_2 , each using them to generate intermediate values of the one-way function.

$$y_1 = g^{x_1} \bmod p$$

$$y_2 = g^{x_2} \bmod p$$

y_1 and y_2 agents send over the open channel to each other and repeat the same procedure as what they received from their colleague

$$y_1^{x_2} = g^{x_1 x_2} \bmod p = y_3,$$

$$y_2^{x_1} = g^{x_2 x_1} \bmod p = y_3.$$

As in the generalized algorithm discussed above, both agents received information through an open channel that allowed them to form a common secret code y_3 . The inverse function seems to be non-existent, but all the efforts of cryptanalysts today are focused on solving this problem, which is at least well formalized. And this gives cryptanalysts hope that an increase in computing power will allow them to find the discrete inverse logarithm. Therefore, one of the ways to create unbreakable one-way functions is to use algorithmic functions instead of arithmetic (algebraic) functions, which have a mathematical formalization of individual elements, but practically no mathematical formalization for the entire function, for example, algorithmic functions based on strange attractors.

4. Statement of the problem

General conditions

1. It is required to create a method that generates encryption keys as often as needed using only an open information exchange channel.

2. At the beginning of the algorithm, there is at least one secret exchange of information about the type, properties, and parameters of the one-way function and the algorithm of interaction between agents in determining a new encryption key.

3. The number of agents can be arbitrary, considering the required total number of addresses for the mutual exchange of secret messages.

4. The necessary expedient is to take the Diffie-Hellman algorithm and modify it.

Determining the procedure of the one-way function based on strange attractors.

First, let's decompose the problem into two components:

1. Develop ways to transform the result of a strange attractor into what can be perceived as the result of a one-way function.

2. Modify the properties of strange attractors by choosing the initial conditions, parameters of differential equations, and, in some cases, the integration step size to diversify the function's behavior.

Properties of the function:

- One-way property. That is, the ability to obtain the value of the function based on information about the argument $y = f(x)$

and the simultaneous impossibility of obtaining the value of the argument based on the value of the function, more precisely, the absence of an inverse function that would ensure finding the argument for a given value of the function $x = f^{-1}(y)$.

In the case of strange attractors, the one-way property cannot be obtained without introducing additional modifications since any attractor that can be represented as a system of differential equations (in this paper, we consider just such attractors), which makes it possible to find $x = f^{-1}(y)$ based on the known characteristics of the attractor. For the strange attractor to acquire the one-way property, it is proposed to round the obtained numbers to a particular order at each integration step by the Euler method. For example:

At iteration t_n , the coordinates of point A_n were obtained - (0.641, -1.345, 123.532). In this case, before calculating the coordinates of the next point A_{n+1} , it is necessary to round the value of A_n to the first decimal place; as a result we get: A_n' - (0.6, -1.4, 123.5), which will be used to calculate the next point A_{n+1} .

Although changes in the coordinate values of a point can be considered insignificant numerically, in the case of accumulation of "error," the values for the next point may differ from those that could be without "error." This modification gives the attractor the properties of unilateralism since, during the formation of encryption keys, nothing interferes with the operations of the agents. If the attacker tries to find the inverse function, he will not succeed since the roundings that were made during the calculations will be unknown.

- Commutativity property. If we denote the action of the function by " \times ," then the commutativity property of group operations means $x1 \times x2 = x2 \times x1$.

In the example of the function, it can be

$$f(x1 \times x2) = f(x2 \times x1),$$

$$f(x1 + x2) = f(x2 + x1).$$

$$f(x1, x2) = f(x2, x1)$$

5. Modification of the Diffie-Hellman algorithm for n agents

Suppose it is necessary to generate a single password for n agents. The algorithm, in this case, will look similar, except for some features:

1. In the first communication session over a secret channel, the agents agree on the parameters of the $f(x)$ transformation function and related data, just as in the case of two agents. All other communication takes place through open communication channels.

2. In case of the need to change the encryption key, all agents generate secret words x_i , $i = \overline{1, n}$ and calculate intermediate values of the first level function

$$y_i^{(1)} = f(y_0, x_i), \quad i = \overline{1, n}.$$

The value of $y_i^{(1)}$ is cyclically sent by each agent i to agent $i + 1$ through the open channel. Cyclic means that agent n sends intermediate values 1 of level to agent 1 . Generally speaking, the number of the next agent is equal to the remainder of dividing $i + 1$ modulo n .

$$r = (i + 1) \bmod n.$$

3. Now, each agent r at each new step k processes information from previous agents $y_i^{(k-1)}$. To do this, he uses his secret word xr every time. Only the intermediate value of the function $y_i^{(k-1)}$ changes each time. The new intermediate value is equal to

$$y_r^{(k)} = f(y_i^{(k-1)}, xr), \quad i = \overline{1, n}.$$

4. At step n , each agent receives the intermediate value of the function, which he converts into a new shared encryption key using his secret word.

$$y_r^{(n)} = f(y_i^{(n-1)}, xr), \quad i = \overline{1, n}.$$

When generating encryption keys, agents cooperate with only two agents: the sender of the intermediate function value and the receiver agent. Information about other agents is not available.

Probable attackers, as in the two-agent case, listen to the open channel and know the intermediate values of the function from all agents but do not know either the new encryption key or the secret words from individual agents.

Confusing information about the number of agents

To keep the information about the number of agents secret, it is proposed in this paper that one of the agents "plays" instead of several agents. This will give the impression that there are more agents than there are. However, at the same time, there should not be too many fake agents because, in this case, the attacker gets more information about the intermediate values of the function, with which he can more easily choose the attractor parameters and numerical integration parameters.

6. Modification of the process of forming the initial values of the function

In the modified Diffie-Hellman algorithm, the initial value of the function is a combination of the coefficients of the differential equations of the strange attractor, the initial coordinates of the attractor, and the cryptographic salt utilized for the transmission of intermediate values. The aforementioned data can be transmitted to the agents in an encrypted format during the first covert communication, or through steganographic techniques.

As an example, a collection of ordinary pixel images or photos can be found on certain websites on the Internet. In a covert communication scenario, a particular region of an image from the gallery can be designated as the initial attractor parameters by specifying its sequence number. Alternatively, the initial data for attractor parameters can also be derived from textual information.

In our case, a graphic image is chosen as the primary input. Thereafter, the bits of colors and halftones can be translated into specific binary or numerical properties of individual parameters and coordinates of the attractor.

In certain circumstances, it may not be necessary to conceal the image being used, as determining the inverse function based on intermediate results would be practically infeasible.

7. Modifying the process of exchanging intermediate function values

In many hash functions, for additional reliability, a so-called "cryptographic salt" is added to the function to form a hash [17, 18]. This complicates the process of password selection since the value of the "salt" has to be searched for as well. In the case of strange attractors, the necessary data on the basis of which an attacker can select an encryption key or attractor parameters are intermediate values of the attractor coordinates.

To protect this data, the author proposes to use an analog of "cryptographic salt" - numbers that will be added to the intermediate values of the attractor. As mentioned in the previous section, these values can be generated during the first secret communication. However, it is also possible to change the salt constantly. Depending on the situation, agents can generate new "salt" numbers using the

existing and final attractor values that all agents participating in the encryption key generation will have. In this case, all agents will have exactly the same results, and the attacker will not be able to determine the value of the "salt" because he does not know the final values of the strange attractor obtained at the end of the previous encryption key generation session.

An alternative way to generate salt values is to use a strange attractor. Agents can agree to customize the attractor to generate "salt" and generate values that are unpredictable to an attacker.

The process of using "salt" is as follows:

1. It is necessary to generate or agree on the values of the "salt" that will be the same for all agents. In our case, it will be (1232.6435341, -112.3096545, 132423.58765032).

2. It is necessary to generate intermediate values of the attractor - in our case, there will be two agents.

The generated values of Agent 1 are (0.641, -1.345, 123.532).

Generated values of Agent 2: (1.242, 1.3, 13.5).

3. Now the agents need to apply "salt" to the intermediate values of the attractor, which in turn are different for the agents.

Agent 1 will get the following values: (1233.2845341, -113.6546545, 132547.11965).

Agent 2 will receive the following values: (1233.8855341, -111.0096545, 132437.08765).

4. Agents send the generated values to each other.

5. After receiving the values, the agents must decrypt the values using the same "salt" and get the following values:

The values decrypted by Agent 1 and received from Agent 2: (1.242, 1.3, 13.5).

The values decrypted by Agent 2 and received from Agent 1: (0.641, -1.345, 123.532).

Thus, the agents successfully complicated the process of decrypting the initial parameters of the strange attractor for a potential attacker. It is worth noting that this method can also work when the number of agents generating encryption keys is more than two.

8. Approbation of the modified Diffie-Hellman algorithm

In particular, the Newton-Lepnick attractor was used as a one-way function. In general, any attractor can be used as a one-way function, provided that the initial parameters of the attractor, which were formed during the first contact, are kept secret.

Based on a random graphical image (Fig. 1), agents form the same set of parameters and initial values to solve a system of differential equations of strange attractors.

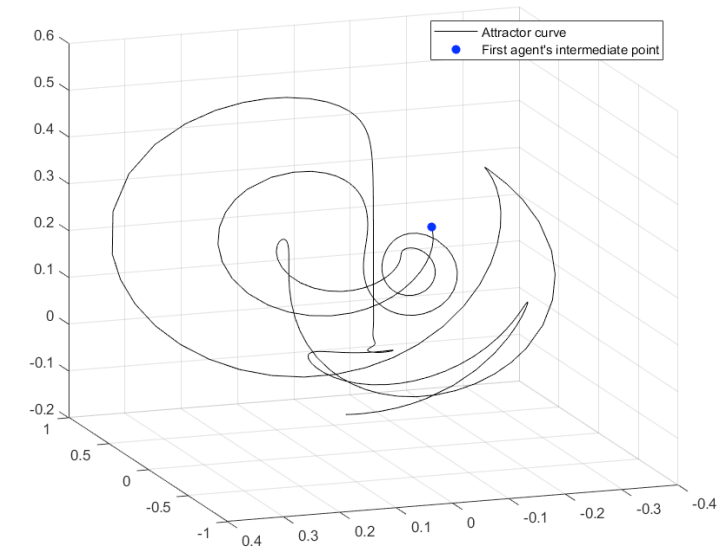


Figure 1: Image for generating the initial coordinates of the attractor

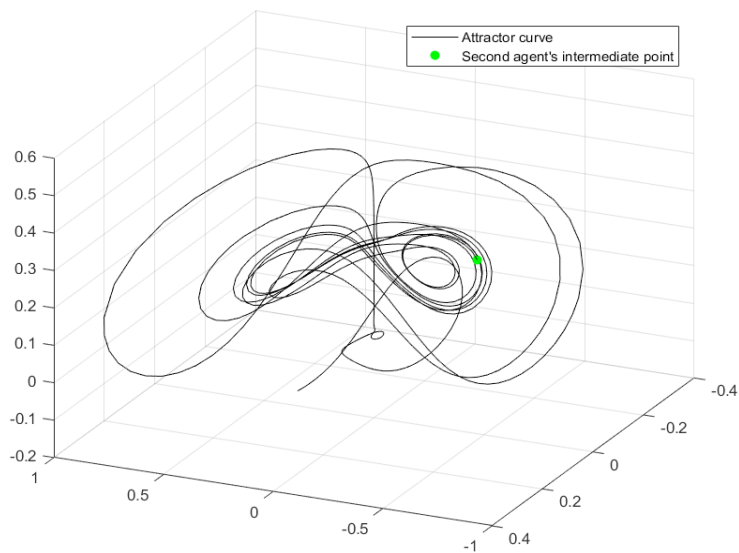
Then each agent comes up with its secret word (for example, 50 for the first and 100 for the second), which corresponds to the number of iterations of the attractor integration, finds the

intermediate coordinates of the attractor, and sends them to the other agent. After that, the obtained intermediate coordinates (Fig. 2 a, b) should be used to pass a known number of integration iterations (50 for the first and 100 for the second, respectively). For the first agent, it is $100+50=150$ steps. The second agent has $50+100=150$ steps. So both agents get the exact final coordinates in different ways (Fig. 3). The attractor curve with intermediate and final points together is shown in Fig. 4.

Critically evaluating the one-way functions of both the classical discrete logarithm and the numerical integration of the strange attractor, it should be noted that in fact both agents can calculate by simulation exactly how many steps the other agent used as a secret word. To do this, it is enough to simulate the dynamics of the attractor, not the full number of steps (in our case 150). At each step, compare the result with the other agent's intermediate coordinates of the attractor. However, this does not give anything additional because other step sizes will be used next time. This time, the final result (at step 150) is already known to both agents belonging to a particular trust group.



a)



b)

Figure 2: Attractor iterations with selected intermediate points. a) with the intermediate point of agent 1; b) the intermediate point of agent 2

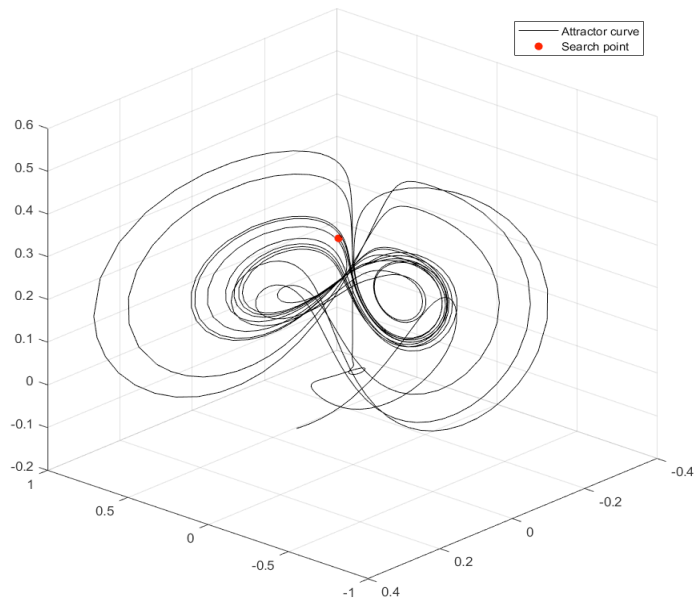


Figure 3: Iterations of the attractor with the selected intermediate point

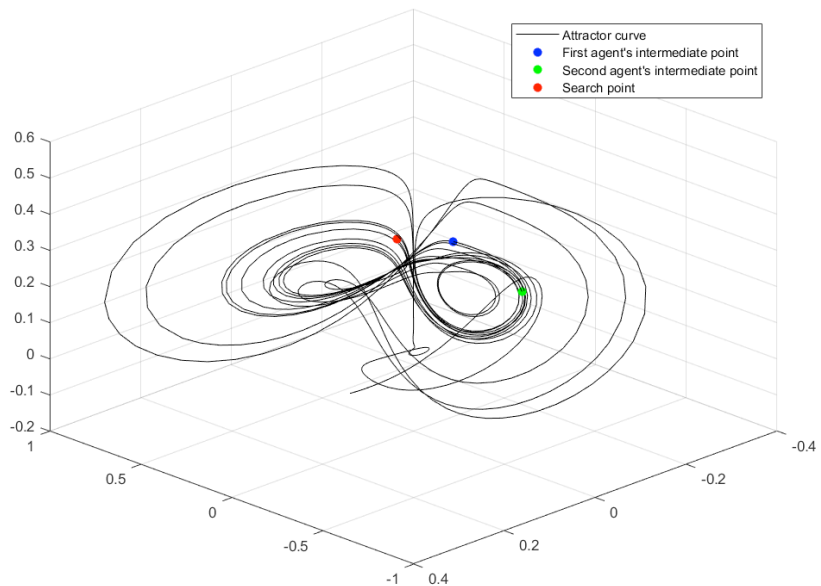


Figure 4: The graph shows the intermediate and end points of the attractor curve

Further, the obtained final coordinates can be used depending on the established protection requirements: in binary form, in hexadecimal, or in the form of a hash (Fig. 5).

```

3226332823302120272716282118292323192823292220282223193025232618272
4153014232225282522172221262628263124242824272121262223202425213020
332227292229382235193435282133392630272613172420173024252430352532
  
```

Figure 5: Shared encryption key based on endpoint coordinates.

9. Conclusions

1. Based on the obtained scientific and applied results, it can be argued that the goal of the work "to improve the quality of the process of creating shared encryption keys using open communication

channels within the framework of the Diffie-Hellman algorithm by creating a one-way function based on strange attractors" has been achieved.

2. In this work, the Diffie-Hellman algorithm is improved by creating a one-way function based on strange attractors.

3. The created algorithm with a modified one-way function based on a strange attractor can be used to create encryption keys and passwords for the secure transmission of information.

4. Depending on users' needs, the complexity of encryption keys can be increased by changing the initial parameters of the attractor, which will also allow controlling the speed of key generation and encryption in general.

5. The software is implemented in three programming languages: C#, Python, and MatLab, which allows one to perform a comparative analysis of the results and consciously choose the programming language of individual parts of the software to optimize the process of generating encryption keys.

6. It is advisable to direct further research toward the systematization of models of strange attractors with the definition of features that affect the cracking strength of the Diffie-Hellman algorithm.

10. References

- [1] W. Xin, T. Ahonen, and J. Nurmi. "Applying CDMA technique to network-on-chip." *IEEE transactions on very large scale integration (VLSI) systems* 15.10 (2007): 1091-1100.
- [2] V.L. Shevchenko, O.V. Nesterenko, I.E. Netesin, A.V. Shevchenko, V.B. Polishchuk. *Prognostic modeling of computer virus epidemics*. - K.: UkrSC IND, 2019. - 152 p.
- [3] V. Shevchenko, A. Shevchenko. *The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems*. - 2017 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Polyana, April 20-23, 2017. - p.174-177. doi.org/10.1109/MEMSTECH.2017.7937561.
- [4] V. Shevchenko, A. Shevchenko, R. Fedorenko, Y. Shmorhun, A. Hrebennikov. *Designing of Functionally Stable Information Systems Optimal for a Minimum of Losses*. - CADSM 2019, 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), February 26 – March 2, 2019, Polyana-Svalyava (Zakarpattya), UKRAINE, IEEE Ukraine Section, IEEE Ukraine Section (West), MTT/ED/AP/EP/SSC Societies Joint Chapter Part Number: CFP19508-USB ISBN: 978-1-7281-0053-1 pp.36-40.
- [5] R. Mitsuru Matsui - *Selected Areas in Cryptography / Zuccherato Henri Gilbert, Helena Handschuh // Security Analysis of SHA-256 and Sisters* – August 14 – August 15, 2003, Ottawa, Canada, pp. 175 – 193. doi.org/10.1007/978-3-540-24654-1_13
- [6] P. MacKenzie, T. Shrimpton, M. Jakobsson. *Threshold Password-Authenticated Key Exchange*. // *Journal of Cryptology*, Vol. 19, Issue 1, January 2006, pp. 27-66. doi.org/10.1007/s00145-005-0232-5
- [7] P. Petrov, G. Dimitrov, S. Ivanov "A Comparative Study on WebSecurity Technologies Used in Irish and Finnish Banks." 18 International Multidisciplinary Scientific Geoconference SGEM 2018: Conference Proceedings, 2 - 8 July 2018, Albena, Bulgaria : Vol. 18. Informatics, Geoinformatics a. Remote Sensing. Iss. 2.1. Informatics, Sofia : STEF92 Technology Ltd., Vol. 18, 2018, Iss. 2.1, pp. 3 - 10.
- [8] P. Petrov, S. Krumovich, N. Nikolov, G. Dimitrov, and V. Sulov. 2018. "Web Technologies Used in the Commercial Banks in Finland." In *Proceedings of the 19th International Conference on Computer Systems and Technologies (CompSysTech'18)*, Boris Rachev and Angel Smrikarov (Eds.). ACM, New York, NY, USA, pp. 94-98. DOI: <https://doi.org/10.1145/3274005.3274018>. ISBN: 978-1-4503-6425-6
- [9] V. Shevchenko; G. Dimitrov; D. Berestov; P. Petrova; I. Sinitcyn; E. Kovatcheva; I. Garvanov; I. Kostadinova *One-way Function Based on Modified Cellular Automata in the Diffie-Hellman Algorithm for Big Data Exchange Tasks through Open Space*. – DIGILIENCE 2020: Cyber Protection of Critical Infrastructures, Big Data and Artificial Intelligence. – Varna, September 30 – October 2, 2020. – pp.233-246. <http://isij.eu/isij-47-digilience-2020-cyber-protection-critical-infrastructures-big-data-and-artificial>

- [10] W. Diffie and M. E. Hellman. IEEE Transaction on Information Theory. Vol. IT-22, No.6, November 1976, pp.644-654
- [11] V.V. Shevchenko, D. Berestov, I. Sinitcyn, V.L. Shevchenko Built-In Processor for Sharing Passwords Through the Open Information Space. - 2020 16-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. - Lviv, April 22-26, 2020. - pp.40-44. doi.org/10.1109/MEMSTECH49584.2020.9109523
- [12] A. Lysenko, A. Bychkov, S. Chumachenko, G. Panajotova, E. Kovacheva, V. Shevchenko, A. Turejchuk. Mathematical models and information technology for assessing and predicting environmental conditions at landfills. Publisher: Pro Langs, Kyiv-Sofia 2017, ISBN: 978-954-2995-29-6 pp.1-218.
- [13] V.L. Shevchenko Optimization Modeling in Strategic Planning. - K.: CVSD NUOU, 2011. – 283p.
- [14] S. Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301. DOI: 10.4018/978-1-5225-2773-2
- [15] P. MacKenzie, T. Shrimpton, M. Jakobsson. Threshold Password-Authenticated Key Exchange. // Journal of Cryptology, Vol. 19, Issue 1, January 2006, pp. 27-66. doi.org/10.1007/s00145-005-0232-5
- [16] J. Hong, S. Moon. A Comparison of Cryptanalytic Tradeoff Algorithms. // Journal of Cryptology, Vol. 26, Issue 4, October 2013, pp. 559-637. doi.org/10.1007/s00145-012-9128-3