https://doi.org/10.31891/2219-9365-2024-80-47
UDC 004.056

ANTONENKO Artem
National University of Life and Environmental Sciences of Ukraine
https://orcid.org/0000-0001-9397-1209
e-mail: artem.v.antonenko@gmail.com
BURACHYNSKYI Andrii
State University of Information and Communication Technologies
https://orcid.org/0009-0003-7913-2152
SOLSKYI Danyil
State University of Information and Communication Technologies
https://orcid.org/0009-0005-0351-5987
TVERDOKHLIB Arsenii
State University of Information and Communication Technologies
https://orcid.org/0000-0002-6591-2866
MISHKUR Yurii
State University of Information and Communication Technologies
https://orcid.org/0009-0004-6807-6914
ZINIAR Denys
State University of Information and Communication Technologies
https://orcid.org/0009-0003-6385-5866

ASPECTS OF APPLICATION OF NEURON NETWORK IN CRYPTOGRAPHY

The article analyzes the possibilities of using neural networks in cryptography to increase the security of encryption keys. The authors focus on growing cyber threats and the importance of implementing modern technologies for information protection. The main goal of the research is to evaluate the effectiveness of the neural network in the exchange of encryption keys, based on the achievements in the field of neural cryptography, as well as the development of new methods of protection against cyber threats. The authors created a neural model that is based on the concept of a parity tree and is used for the exchange of encryption keys. At the preparatory stage, a detailed analysis of existing models of neural networks was performed to assess their compliance with the main goal of the project. Using knowledge from similar studies, the authors developed a special neural model in the Python programming language that implements the theoretical foundations. The next stage included the creation of a test environment that allowed for thorough evaluations, guaranteeing the stability and reliability of the neural network in various conditions. The proposed neural network model can become a secure alternative to the traditional Diffie-Hellman key exchange method. In addition, its expected resistance to quantum decryption takes an important step in strengthening cryptographic protocols against new threats in the age of quantum computing. The model shows high efficiency even in simple configurations. The ability of neural networks to quickly adapt to new threats is especially emphasized, which is critically important for ensuring security in conditions of change. The study also shows that the depth of synaptic connections in a neural network makes it much more difficult for attackers to break the key, reducing the chances of success. The findings highlight the wide range of potential applications of neural networks in areas such as cybersecurity, telecommunications, and financial forecasting. Despite certain difficulties associated with algorithms and high requirements for computing resources, neural networks show significant potential for improving cryptographic systems.

Keywords: neural networks; cryptography; cyber security; encryption; encryption key.

АНТОНЕНКО Артем
Національний університет біоресурсів і природокористування України
БУРАЧИНСЬКИЙ Андрій, СОЛЬСЬКИЙ Даниїл, ТВЕРДОХЛІБ Арсеній,
МІШКУР Юрій, ЗІНЯР Денис
Державний університет інформаційно-комунікаційних технологій

АСПЕКТИ ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ КРИПТОГРАФІЇ

У статті аналізуються можливості застосування нейронних мереж у криптографії для підвищення безпеки шифрувальних ключів. У статті акцентують увагу на зростаючих кіберзагрозах і важливості впровадження сучасних технологій для захисту інформації. Основною метою дослідження є оцінка ефективності нейронної мережі в обміні шифрувальними ключами, ґрунтуючись на досягненнях у сфері нейронної криптографії, а також розробка нових методів захисту від кіберзагроз. Автори створили нейронну модель, яка спирається на концепцію дерева парності та застосовується для обміну шифрувальними ключами. На підготовчому етапі було виконано детальний аналіз наявних моделей нейронних мереж для оцінки їхньої відповідності основній меті проєкту. Використавши знання з подібних досліджень, автори розробили спеціальну нейронну модель на мові програмування Python, що реалізує теоретичні основи. Наступний етап включав створення тестового середовища, яке дозволило провести ретельні оцінки, гарантуючи стійкість і надійність нейронної мережі в різних умовах. Запропонована нейромережева модель може стати безпечною альтернативою традиційному методу обміну ключами Діффі-Хеллмана. Крім того, її очікувана стійкість до квантового дешифрування робить важливий крок у зміцненні криптографічних протоколів перед новими загрозами в епоху квантових обчислень. Модель показує високу ефективність навіть у простих конфігураціях. Особливо підкреслена здатність нейронних мереж швидко адаптуватися до *нових загроз, що є критично важливим для забезпечення безпеки в умовах змін. Дослідження також показує, що глибина синаптичних зв’язків у нейронній мережі значно ускладнює зловмисникам завдання зламу ключа, знижуючи шанси на успіх. У висновках підкреслюється широкий спектр можливостей використання нейронних мереж у таких сферах, як кібербезпека, телекомунікації та фінансове прогнозування. Попри певні труднощі, пов’язані з алгоритмами та високими вимогами до обчислювальних ресурсів, нейронні мережі демонструють значний потенціал для покращення криптографічних систем.*

Ключові слова: нейронні мережі; криптографія; кібербезпека; шифрування; ключ шифрування.

STATEMENT OF THE PROBLEM IN A GENERAL FORM AND ITS CONNECTION WITH IMPORTANT SCIENTIFIC OR PRACTICAL TASKS

In the course of this work, a neural model based on the parity tree concept was developed and implemented. The main goal was to evaluate the effectiveness of the neural network in the context of encryption key exchange, based on advances in the field of neural cryptography.

The results of the research open the way to the development of innovative cryptographic solutions. Using neural networks, the research contributes to new approaches to encryption, decryption and key management. These innovations have practical implications as they provide information security professionals and cryptographers with a diverse set of tools to address complex security challenges, contributing to a more resilient and adaptive cryptographic infrastructure.

ANALYSIS OF RECENT SOURCES

The ability of neural networks to learn adaptively, revealed in the course of the study, is of practical importance for the implementation of adaptive security measures. The results can be applied to create cryptographic systems that learn and adapt to changing cyber threat patterns. This adaptability ensures that security measures remain effective in the face of dynamic attack strategies, offering a proactive defense mechanism against evolving threats.

FORMULATION OF THE GOALS OF THE ARTICLE

The primary goal is to address today's challenges associated with an ever-changing threat landscape. Cryptographic methods, although they are the basis of information security, face new dimensions of complexity in countering sophisticated cyber threats. By exploiting the adaptability and learning ability of neural networks, this research aims to provide insights into innovative approaches that can harden cryptographic systems to counter new challenges. The research aims to delve into the dynamic nature of neural networks and understand how this adaptability can be exploited for cryptographic purposes. Known for their ability to learn from data and recognize complex patterns, neural networks are a dynamic element that meets the ever-changing demands of cryptographic protocols. The goal is to explore how this dynamic nature can be integrated into cryptographic methodologies to improve their efficiency and responsiveness.

PRESENTING MAIN MATERIAL

The parity tree, a cryptographic construct that has its origins in error-detecting codes, has found practical applications for the secure sharing of cryptographic keys between multiple parties. At its core, TPM is a neural network architecture characterized by interconnected nodes structured in layers. The theoretical basis of TPM involves complex calculations at each node, where input data is multiplied, aggregated and passed through activation functions. These calculations create a unique mathematical landscape that allows TPM to process complex patterns and solve complex problems. Understanding the theoretical underpinnings of TPM is essential to appreciating its computational capabilities and potential applications

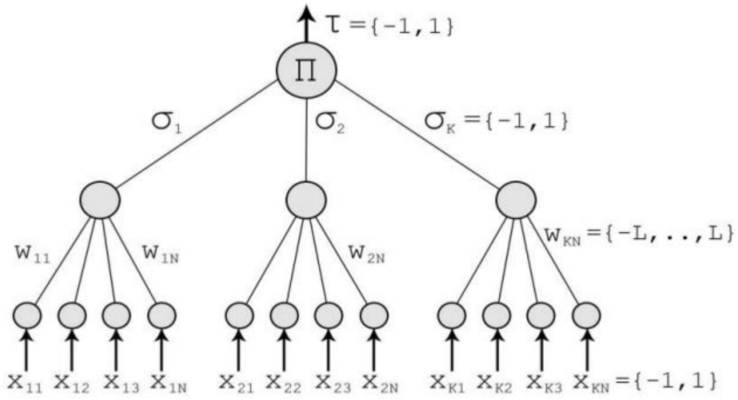

Fig. 1. Graphic structure of TPM

The structural complexity of TPM lies in its multi-level architecture, as depicted in Figure 1. Input nodes, hidden nodes, and output nodes form a complex network in which computations take place. Each level contributes to the transformation of input data, turning it into a meaningful output. Hidden nodes, in particular, serve as the computing power of the neural network, embodying the essence of TPM's problem-solving ability. Unraveling this structural complexity allows us to understand the complex mechanisms that drive TPM's computational capabilities. TPM training includes specialized algorithms designed to tune network parameters, allowing it to learn and adapt. Learning algorithms such as Hebban's learning rule and perceptron learning algorithm play a crucial role in building the intelligence of ANNs. These algorithms contribute to the network's ability to recognize patterns, solve complex tasks, and adapt to a changing environment. Developing intelligence in TPM involves carefully orchestrating these algorithms, fine-tuning the network for optimal performance.

Compared to algorithms based on number theory, the neural algorithm has several advantages. First, it is extremely simple. The learning algorithm essentially acts as a linear filter, which makes it easy to implement at the hardware level. Second, the computational effort required to generate the key is low. Generating a key of length N requires only the order of N computational steps. Third, a new key can be generated for each message or even for each message block. There is no need to store classified information for a long period of time. However, the generated keys must be secure. An attacker E who writes a message between A and B should not be able to compute the secret key. Methods of combating such attackers will be discussed below.

Although TPM is based on theoretical complexities, it finds its true essence in practical application. His ability to recognize patterns and solve complex problems makes him invaluable in a variety of fields. In cybersecurity, TPM is used for anomaly detection by identifying irregular patterns in data flows. In telecommunications, it optimizes signal processing, increasing the efficiency of communication networks. In addition, TPM finds application in optimization tasks, financial forecasting and even in artificial intelligence research, which emphasizes its universality and relevance in the real world. Despite its computing power, TPM is not without its challenges. The complexity of learning algorithms combined with the need for significant computing resources create obstacles to its widespread implementation. However, current research aims to mitigate these challenges, paving the way for improved TPM implementation. The future of TPM promises improved learning methodologies, scalability, and integration with new technologies. Overcoming these challenges, revealing the full potential of MTM and exploring uncharted territories in the field of artificial intelligence and computer science involves solving these problems.

The theoretical working protocol of the Parity Tree is that each side (A and B) uses its own parity machine (TPM) to synchronize the weight matrix. TPM synchronization of machines is achieved by the following steps:

1. Initialization of random weight values.

2. Follow these steps to complete synchronization:

2.1. generating a random input vector X;

2.2. calculation of hidden neuron values;

2.3. calculation of the value of the output neuron;

2.4. compare the values of both tree parity machines: a. the outputs are the same: one of the appropriate learning rules is applied to the weights b. the output data are different: we go to point 2.1.

Once fully synchronized (the wij weights of both TPM machines are the same), A and B can use their weights as keys. Thus, Parity Tree is a practical and universal solution for secure distribution of shared keys in cryptographic applications. Whether it is used for secure multiparty computation, cryptographic key management, or other scenarios requiring shared key generation, Parity Tree integration enhances the security, reliability, and fault tolerance of cryptographic systems. As researchers continue to explore innovative approaches to key distribution and cryptographic protocols, Parity Tree is a significant contribution to the development of secure and collaborative information exchange. In each attack, it is assumed that the attacker E can eavesdrop on the messages between parties A and B, but has no ability to modify them.

To carry out a brute force attack, an attacker must test all possible keys (all possible values of weights wij). With K hidden neurons, K×N input neurons, and a weight limit L, this gives (2L+1) KN possibilities. For example, a configuration of K = 3, L = 3, and N = 100 gives us 3*10253 key possibilities, making the attack impossible with modern computing power. One basic attack can be performed by an attacker who owns the same tree parity machine as parties A and B. He wants to synchronize his tree parity machine with these two parties. Three situations are possible at each step:

Output(A) ≠ Output(B): Neither side updates their weights.

Output(A) = Output(B) = Output(E): All three parties change the weights in their parity machines.

Output(A) = Output(B) ≠ Output(E): Parties A and B update their tree parity machines, but the attacker cannot do so.

Due to this situation, its learning is slower than the synchronization of parties A and B. It is proven that the synchronization of the two parties is faster than the training of the attacker. This can be improved by increasing the synaptic depth L of the neural network. This gives this protocol enough security that an attacker can learn the key with only a small probability. For conventional cryptographic systems, protocol security can be increased by increasing the key length. In the case of neural cryptography, we improve it by increasing the synaptic depth L of neural networks. Changing this parameter increases the cost of a successful attack exponentially, while user effort increases polynomially. Therefore, breaking the security of neural key exchange belongs to the NP complexity class.

The resilience of the parity tree to various attacks, as mentioned in the previous sections, positions it as a secure key exchange method, especially in scenarios where eavesdropping is a priority. One of the main advantages is its resistance to brute force attacks. Given the huge key space generated by the combination of hidden neurons (K), input neurons (N), and weight constraints (L), the number of possibilities becomes astronomically large. For example, even with a relatively modest configuration such as K = 3, L = 3, and N = 100, the number of potential keys reaches a value that modern computing power considers insurmountable. An intriguing scenario arises when an attacker owns the same tree parity machine as parties A and B and seeks to synchronize with them. In this case, the attacker faces problems in maintaining the synchronization rate of parties A and B. Three possible situations at each step dictate the dynamics of updating the weights. In particular, when Output(A) ≠ Output(B), neither party updates its weights. If Output(A) = Output(B) = Output(E), all three parties change their weights. However, when Output(A) = Output(B) ≠ Output(E), parties A and B are in sync and the attacker cannot. This internal limitation slows down the learning process of the attacker compared to the synchronization of the legitimate parties.

To increase security, the synaptic depth (L) of the neural network can be increased. This strategic setting introduces a level of complexity that greatly complicates an attacker's ability to learn the key effectively. Thus, the security of the protocol is strengthened, and the probability of successful learning of the key by an attacker is minimized. In conventional cryptographic systems, increasing security is often associated with increasing key length. In the field of neural cryptography, the equivalent parameter is the synaptic depth (L). It is noteworthy that changing this parameter leads to an exponential increase in the cost of a successful attack, while the effort required by legitimate users grows polynomially. This characteristic places the security of neural key exchange in the class of NP-hardness, indicating the level of computational complexity that corresponds to hard-to-solve problems. In conclusion, the analysis highlights the resilience of the parity tree to potential attacks, providing a secure framework for key exchange in scenarios where eavesdropping and malicious synchronization attempts are a concern. Strategically adjusting the depth of synaptic connections adds an additional layer of security, making neural key exchange a robust and computationally intensive approach to secure communication.

The testing phase was carefully performed and included several iterations with different matrix sizes and different maximum number values. A careful repetition of each test six times was applied to check the consistency of the results. To facilitate this comprehensive testing, the Randas library was used. Pandas, a robust open source data manipulation and analysis library for Python, has proven to be a valuable tool. Her capabilities in creating high-performance, user-friendly data structures combined with effective data analysis tools have made the process of working with structured data seamless and efficient. The assessment of differences in settings and synchronization was expressed on a scale where 100.0 means no network at all. This quantitative metric provided a clear and standardized measure of performance, allowing for a detailed understanding of network behavior under various conditions. Complex testing, supported by the versatility of the Randas library, facilitated thorough analysis of neural network response and synchronization in various scenarios.

Analyzing the Hebbian update results with low values in Table 1, it can be seen that the hacker could only successfully connect to the first and second complexity levels. As the level of complexity increased, the system demonstrated a significant increase in resilience, strengthening its defenses against more sophisticated intrusion attempts. The results of the Hebbian update with average values highlight the robust security of the system, as the hacker's attempts to connect to the network were consistently thwarted, resulting in negative synchronization values that indicate complete synchronization reversal, especially for values below −100. This robust defense mechanism emphasizes the resilience of the network to intrusion attempts. When updating the Hebbian with high values. the hacker faced insurmountable barriers, failing to establish a connection even once. The constant occurrence of sync backs further highlights the network's impenetrability in these tests. These results are the most robust among all iterations, demonstrating the system's strong protection against various attack scenarios.

The comparative analysis presented in Table 2 highlights the significant difference between the Hebbian and Anti-Hebbian learning mechanisms. In particular, the average minimum synchronization values in Anti-Hebbian are lower, indicating a higher level of security. Regardless, the main conclusion is that Anti-Hebbian learning makes it nearly impossible for random guesses or attempts at external synchronization to lead to success. Thus, based on this evaluation, anti-Hebbian learning appears to be the safer option of the two. Its ability to resist random guesses and external synchronization attempts improves the overall security of cryptographic applications. This finding highlights the importance of choosing an appropriate learning mechanism for neural networks in cryptographic contexts where security is paramount.

The distinction between Hebbian and anti-Hebbian update rules is a key aspect in the field of neural network learning mechanisms. These rules define the principles governing synaptic plasticity, highlighting various aspects of the relationship between neuronal activations and the corresponding adjustments in synaptic weights. The Hebbian update rule works on the principle of synaptic enhancement based on correlated activity. It states that when neurons exhibit simultaneous and correlated activation, the strength of their synaptic connection should increase.

This reinforcement, described by the phrase "cells that fire together, bind together," is at the heart of associative learning and memory formation. Hebbian learning promotes the creation of functional neural circuits through the strengthening of connections that are consistent with coherent firing patterns.

Table 1

A test of Hebbian update rules with different values

	Iteration	**Network settings**			
A test of Hebbian update rules with low values		k: 3, n: 4, l: 6	k: 6, n: 8, l: 12	k: 9, n: 12, l: 18	k: 12, n: 16, l: 24
	1	70,36	28,69	-3,80	-17,71
	2	102,30	29,90	10,25	-60,20
	3	102,30	102,30	-1,94	-37,50
	4	46,05	31,81	0,22	-13,19
	5	102,30	20,36	-13,90	-43,88
	6	65,49	42,23	-44,46	-49,39
	Result	3/6 broken	1/6 broken	0/6 broken	0/6 broken
A test of Hebbian update rules with mean values	**Iteration**	**Network settings**			
		k: 15, n: 20, l: 30	k: 18, n: 24, l: 36	k: 21, n: 28, l: 42	k: 24, n: 32, l: 48
	1	84,88	-63,61	-110,95	-171,04
	2	-66,34	-117,67	-167,16	-217,84
	3	-39,51	-107,90	-160,09	-168,26
	4	-41,23	-132,23	-132,14	-118,86
	5	-66,31	-122,62	-127,09	-142,68
	6	-87,70	-101,37	-122,59	-148,23
	Result	0/6 broken	0/6 broken	0/6 broken	0/6 broken
A test of Hebbian update rules with high values	**Iteration**	**Network settings**			
		k: 27, n: 36, l = 54		k: 30, n: 40, l: 60	
	1	-199,60		-231,84	
	2	-193,90		-264,80	
	3	-220,27		-223,40	
	4	-170,40		-246,05	
	5	-171,30		-209,00	
	6	-221,68		-240,98	
	Result	0/6 broken		0/6 broken	

The distinction between Hebbian and anti-Hebbian update rules is a key aspect in the field of neural network learning mechanisms. These rules define the principles governing synaptic plasticity, highlighting various aspects of the relationship between neuronal activations and the corresponding adjustments in synaptic weights. The Hebbian update rule works on the principle of synaptic enhancement based on correlated activity. It states that when neurons exhibit simultaneous and correlated activation, the strength of their synaptic connection should increase. This reinforcement, described by the phrase "cells that fire together, bind together," is at the heart of associative learning and memory formation. Hebbian learning promotes the creation of functional neural circuits through the strengthening of connections that are consistent with coherent firing patterns.

The distinction between Hebbian and anti-Hebbian update rules is a key aspect in the field of neural network learning mechanisms. These rules define the principles governing synaptic plasticity, highlighting various aspects of the relationship between neuronal activations and the corresponding adjustments in synaptic weights. The Hebbian update rule works on the principle of synaptic enhancement based on correlated activity. It states that when neurons exhibit simultaneous and correlated activation, the strength of their synaptic connection should increase. This reinforcement, described by the phrase "cells that fire together, bind together," is at the heart of associative learning and memory formation. Hebbian learning promotes the creation of functional neural circuits through the strengthening of connections that are consistent with coherent firing patterns.

In contrast, the anti-Hebbian update rule embodies the concept of weakening synaptic connections in response to uncorrelated or time-dispersed neuronal activity. The essence of anti-Hebbian learning is that "cells that work out of sync lose their communication". This rule introduces an element of competition by selectively weakening connections between neurons that do not exhibit correlated firing patterns. Anti-Hebbian learning serves as a mechanism for network stability, preventing overexcitation and contributing to the accuracy of memory networks. The fundamental difference lies in the influence of these rules on the dynamics of learning in neural networks. Hebbian learning facilitates associative learning, memory formation, and the creation of coherent neural representations. Conversely, anti-Hebbian learning complements this process by facilitating the selective pruning of less relevant or temporally disconnected connections, promoting network stability and preventing the occurrence of unpredictable excitation. The interplay between Hebbian and anti-Hebbian learning is integral to network plasticity and homeostasis. While Hebbian learning adapts synaptic connections to recurrent patterns of activation, anti-Hebbian learning acts as a regulatory mechanism, maintaining balance in the network by eliminating less relevant connections. This delicate interplay contributes to the structural and functional dynamics of neural networks, shaping their ability to adapt to changing conditions while maintaining stability.

Table 2

Test of Anti-Hebbian update rules with different values

A test of anti-Hebbian update rules with low values	**Iteration**	**Network settings**			
		k: 3, n: 4, l: 6	k: 6, n: 8, l: 12	k: 9, n: 12, l: 18	k: 12, n: 16, l: 24
	1	94,66	25,39	17,42	-12,85
	2	77,30	47,09	5,70	-11,37
	3	69,66	45,36	6,85	-5,95
	4	80,77	57,68	21,28	-1,35
	5	64,11	49,52	27,76	-39,84
	6	66,88	45,53	31,47	9,37
	Result	0/6 broken	0/6 broken	0/6 broken	0/6 broken
A test of Anti-Hebbian update rules with mean values	**Iteration**	**Network settings**			
		k: 15, n: 20, l: 30	k: 18, n: 24, l: 36	k: 21, n: 28, l: 42	k: 24, n: 32, l: 48
	1	-48,84	-51,06	-111,55	-141,65
	2	-40,45	-38,19	-134,87	-160,69
	3	-17,42	-36,97	-121,69	-149,89
	4	-50,87	-42,51	-125,62	-154,71
	5	-22,67	-100,11	-139,64	-108,13
	6	-42,64	-55,92	-124,02	-79,74
	Result	0/6 broken	0/6 broken	0/6 broken	0/6 broken
Anti-Hebbian update rule test with high values	**Iteration**	**Network settings**			
		k: 27, n: 36, l = 54		k: 30, n: 40, l: 60	
	1	-123,61		-261,66	
	2	-154,59		-169,85	
	3	-163,17		-220,87	
	4	-156,77		-209,05	
	5	-133,70		-157,19	
	6	-206,08		-120,30	
	Result	0/6 broken		0/6 broken	

The difference between Hebbian and anti-Hebbian renewal rules lies in their respective approaches to synaptic plasticity. Hebbian learning enhances correlated activity, promoting associative learning and memory formation, while anti-Hebbian learning weakens uncorrelated connections, promoting network stability and homeostasis. This subtle relationship between reinforcement and weakening mechanisms is key to understanding the fundamental principles of neural network learning. In addition to the robust protection provided by Anti-Hebbian and Random-Walk under various conditions, it is worth emphasizing the adaptability of these rules to dynamic cybersecurity landscapes. Anti-Hebbian's inherent ability to keep security at a minimal level makes it a reliable defense mechanism against potential threats, even in scenarios where the hacking machine exhibits advanced capabilities. Moreover, the Random-Walk rule is the most optimal choice due to its ability to provide reliable protection not only at low but also at high settings. This dual capability provides resilient protection by adapting to potential fluctuating network conditions and cyber threats. The adaptability of Random-Walk becomes especially important when faced with sophisticated attacks or unpredictable vulnerabilities, as it maintains a secure connection even in the face of a changing threat landscape. Additionally, Hebbian's performance at higher settings, especially in achieving excellent backward synchronization, highlights its suitability for scenarios where advanced security measures are paramount. By using Hebbian in such environments, organizations can improve their overall cybersecurity posture and reduce the risk of sophisticated attacks that may attempt to exploit vulnerabilities at elevated settings.

In conclusion, a comprehensive analysis of Hebbian, Anti-Hebbian, and Random-Walk rules offers a nuanced approach to cybersecurity. While Hebbian excels in specific high-tuning scenarios, Anti-Hebbian and Random-Walk are versatile options capable of providing robust protection in a variety of environments. A strategic combination of these rules can create a robust defense system that guarantees the integrity and confidentiality of connections in the face of evolving cyber threats and potential adversary advances. The random walk rule is a special mechanism in the field of neural network learning that introduces a stochastic element into the tuning of synaptic weights. Unlike deterministic rules driven by correlation patterns, the Random Walk rule embraces unpredictability and randomness in exploring the space of synaptic weights. This scientific review aims to highlight the fundamental principles and implications of the application of the random walk rule in neural networks. In essence, the Random-Walk update rule introduces a certain level of uncertainty into the adjustment of the synaptic weights. Rather than relying on an explicit correlation or anticorrelation between neuronal activations, the Random-Walk rule allows for probabilistic changes. This stochasticity allows the network to pass through a range of states, potentially facilitating the discovery of new configurations that might not be immediately obvious using deterministic rules.

The philosophy behind the Random-Walk rule is similar to a random search strategy in the synaptic weight space. This study is consistent with the notion that the network, through probabilistic settings, can avoid local optima and explore regions that may lead to more optimal configurations. This element of randomness introduces inherent adaptability and flexibility, allowing the neural network to respond to a variety of environmental stimuli. From a practical point of view, the Random-Walk update rule can be applied in scenarios where a certain degree of exploration and unpredictability is an advantage. It can help overcome local minima in the learning process, allowing the network to explore alternative solutions and potentially converge to more globally optimal configurations. Such adaptability is especially valuable in dynamic environments where deterministic rules may fail to cope with changing patterns or unpredictable challenges.

Introducing randomness into synaptic weight adjustments, facilitated by the random walk rule, is consistent with the broader concept of stochastic optimization in neural networks. This concept recognizes that incorporating randomness into learning processes can be a powerful strategy for avoiding local optima and achieving more robust and adaptive solutions. The random walk rule in neural networks is a departure from deterministic learning mechanisms, taking into account stochasticity and unpredictability. This rule introduces a degree of randomness to synaptic weight adjustments, facilitating the exploration of weight space and potentially leading to the discovery of more optimal configurations. The Random-Walk update rule illustrates the adaptability and flexibility that stochastic elements bring to the complex learning dynamics of neural networks.

CONCLUSIONS FROM THIS STUDY AND PROSPECTS FOR FURTHER RESEARCH IN THIS DIRECTION

The parity tree machine, as a neural network architecture, has promising characteristics for cryptographic applications. The use of TPM in key exchange protocols introduces a dynamic element to the process, increasing resistance to potential threats and vulnerabilities. The research aims to understand the intricacies of TPMs, their ability to adapt to changing data models, and their potential to enhance the security of cryptographic key exchanges. The main focus of the research is on solving modern problems faced by traditional key exchange mechanisms. By incorporating TPM, the research aims to offer innovative solutions that go beyond traditional paradigms. This involves not only protecting the key exchange process from malicious attacks, but also optimizing the computational efficiency of cryptographic operations.

Further research suggests possible developments beyond the parity tree machine for cryptographic key exchange. One important perspective is the investigation of real neural encryption/decryption methods. This development aims to create a symbiosis between existing key exchange machines and true neural encryption/decryption methods. The trajectory of cryptographic research is dynamic, marked by continuous development aimed at solving new challenges and using new technologies. If we imagine the future of the implemented prototype, we can highlight several potential upgrades, the main one being the integration of advanced architectures, such as the tree parity machine with vector estimation (VV-TPM). In addition, improvements in key management strategies, diversification of cryptographic algorithms, and scalability considerations are promising directions for enhancing the cryptographic capabilities of the prototype.

The evolution from the traditional tree parity machine (TPM) to the vector-valued tree parity machine (VV-TPM) represents a profound leap in the development of neural network architecture. While conventional TPM excels at reproducing complex patterns using hierarchical structures, VV-TPM extends these capabilities by introducing vector values of the outputs. Such an addition allows for a more detailed representation of information, increasing the potential for handling multidimensional data and complex relationships in cryptographic contexts. The implementation of VV-TPM can improve resistance to modern cryptographic attacks, as the output vector values provide richer pattern encoding. In addition, the potential of parallelization of calculations in vector operations can increase the computational efficiency of cryptographic processes. However, the integration of VV-TPM requires a thorough re-evaluation of learning rules, weight update mechanisms, and synchronization strategies to adapt to the increased dimensionality of vector outputs.

References

1. Nikolayevsky, O. Yu., Skliarenko, O. V., & Sydorchuk, A. (2019). Analysis and comparison of face detection Apis. Telecommunications and information technologies, 4(65), 121–133

2. Kolodinska, Y. (2024). The use of artificial intelligence to manage the processes of creation and development of IT projects. Artificial intelligence in science and education (AISE 2024), 101–102.

3. Troyan, K. M., & Skliarenko, O. V. (2023). Practical cases and prospects for the development of artificial intelligence technologies. Digital transformation in the economy, management and business. Problems of science, practice and education: Collection of materials of the XXVIII International Scientific and Practical Conference. European University Press, 66–68.

4. Skliarenko, O. V., & Nikolayevsky, O. Y. (2021). Biometric security systems: face recognition. Topical issues of cybersecurity and information protection. Proceedings of the VII International Scientific and Practical Conference, European University Press, 85–87

6. Tverdokhlib A.O., Korotin D.S. Efektyvnist funktsionuvannia kompiuternykh system pry vykorystanni tekhnolohii blokchein i baz dannykh. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, 2022, (6)

7. Tsvyk O.S. Analiz i osoblyvosti prohramnoho zabezpechennia dlia kontroliu trafiku. Visnyk Khmelnytskoho natsionalnoho universytetu. Ceriia: Tekhnichni nauky, 2023, (1)

8. Novichenko Ye.O. Aktualni zasady stvorennia alhorytmiv obrobky informatsii dlia lohistychnykh tsentriv. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, 2023 (1)

9. Zaitsev Ye.O. Smart zasoby vyznachennia avariinykh staniv u rozpodilnykh elektrychnykh merezhakh mist. Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky, 2022, (5)