UDC 004.056.5:004.89:004.738.5 DOI: 10.20535/2411-2976.22025.36-47

THE ROLE OF CYBERSECURITY IN FACILITATING DIGITAL ECONOMY: A TREE PARITY MACHINE-BASED APPROACH

[1]Lela Mirtskhulava, [2]Larysa S. Globa, [3]Nana Gulua, [4]Mariam Gugunashvili, [2]Svitlana V. Sulima

[1] Department of Computer Science, Ivane Javakhishvili Tbilisi State University, Georgia

[2] Educational and Research Institute of Telecommunication Systems Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

[3] Department of Informatics, Faculty of Mathematics and Computer Science, Sokhumi State University, Tbilisi, Georgia

[4] Department of Computer Science, Faculty of Arts and Sciences, American University in Bulgaria, Blagoevgrad, Bulgaria

Background. As the digital economy expands, ensuring secure communication and data integrity becomes increasingly vital. Traditional cryptographic algorithms such as RSA and ECC are vulnerable to quantum computing advances, necessitating post-quantum solutions. Tree Parity Machines (TPMs), inspired by neural synchronisation principles, present a promising alternative for secure key exchange, particularly within Internet of Things (IoT) environments.

Objective. This study aims to evaluate the effectiveness of TPMs as a lightweight, energy-efficient, and quantum-resistant method for secure key generation and exchange in cybersecurity applications, with a focus on IoT networks.

Methods. A hybrid methodology combining theoretical analysis and practical simulations was employed. Theoretical modelling explored TPM synchronisation mechanisms, key generation dynamics, and resilience to cyber-attacks such as man-in-the-middle, replay, brute force, and eavesdropping. Practical simulations were conducted in a controlled network environment to assess TPM performance in terms of synchronisation time, key generation rate, computational overhead, and resistance to attacks, compared with traditional cryptographic methods.

Results. Simulation results demonstrated that TPMs outperform RSA/ECC across multiple parameters. TPMs achieved a synchronisation time of 15.2 ms versus 45.6 ms for RSA/ECC, a key generation rate of 500 keys/s compared to 120 keys/s, and reduced energy consumption (1.2 mJ vs. 3.8 mJ). They also exhibited superior resistance to man-in-the-middle attacks (99.9% vs. 90.4%) and required less computational overhead. These findings confirm TPMs' robustness, scalability, and suitability for resource-constrained IoT environments.

Conclusions. Tree Parity Machines provide an efficient, post-quantum-secure alternative to conventional cryptography, offering enhanced protection against emerging cyber threats. Their lightweight architecture, rapid synchronisation, and minimal energy consumption position them as a key enabler of secure digital infrastructure. Future research should explore TPM integration with blockchain, federated learning, and edge computing to further strengthen cybersecurity frameworks.

Keywords**:** *Tree Parity Machine (TPM); post-quantum cryptography; secure key exchange; IoT security; neural synchronisation; cyber-attack prevention.*

Introduction

In the domain of cybersecurity, ensuring Secure key exchange in secure communication is paramount for protecting sensitive information from unauthorised access. In the digital age, safeguarding sensitive information against unauthorised access and cyber-attacks has become increasingly critical. Traditional cryptographic methods, while foundational to modern security protocols, are facing growing challenges due to the sophistication of contemporary attack vectors and advancements in computational power. In this context, innovative approaches to secure communication are essential to enhance the robustness of cybersecurity frameworks. Tree Parity Machines (TPMs) offer a novel solution to the challenge of secure key exchange, leveraging the principles of neural networks to achieve synchronisation between parties without directly transmitting secret keys. The TPM model is distinguished

by its ability to facilitate secure key exchange through an iterative synchronisation process, making it a compelling candidate for enhancing security protocols. Stypinski and Niemiec (2022) explored the synchronisation of Tree Parity Machines (TPMs) using nonbinary input vectors, demonstrating enhanced robustness and versatility in neural key exchange mechanisms. In their 2023 work, they applied TPM-based neural networks to secure key agreement protocols for smart grids, emphasising their potential for reliable and energy-efficient cryptographic applications.

TPMs are a type of artificial neural network (ANN) designed for specific applications in cryptography and machine learning. Inspired by biological neural networks, TPMs are known for their ability to synchronise through mutual learning processes, making them particularly useful in secure key exchange protocols. Their design is structured hierarchically, where multiple hidden neurons feed into a single output neuron, forming a "tree-like" architecture that enables efficient computation.

The concept of synchronisation in TPMs is pivotal to their application in cryptography. By starting with different initial states, two communicating entities can achieve identical internal states after a series of training steps without transmitting the actual state information. This property provides a robust mechanism for generating shared secret keys over an insecure communication channel, making TPMs a candidate for post-quantum cryptographic schemes (Kanter et al., 2002; Rosen-Zvi et al., 2002). Moreover, TPMs have found applications in machine learning tasks that require high-dimensional data processing. Their hierarchical structure and non-linear activation functions allow them to model complex relationships, like other deep learning architectures, albeit with a specific focus on security-oriented tasks (Kinzel & Kanter, 2002).

Despite their advantages, TPMs also face challenges, such as susceptibility to synchronisation attacks and limitations in scalability for large datasets. Ongoing research seeks to address these limitations, exploring enhanced training algorithms, hybrid architectures, and novel use cases (Klimov et al., 2002). The integration of TPMs into cybersecurity frameworks represents a promising advancement in secure communication technologies. By addressing contemporary challenges in secure key exchange, TPMs offer a novel approach that complements existing cryptographic techniques and enhances overall security. This research contributes to the field by providing insights into the practical application of TPMs and their potential to address emerging security threats.

TPMs have a variety of applications based on their unique properties that include synchronisation and establishing secure communication channels. TPMs are used for generating symmetric cryptographic keys over public channels without prior exchange of secret information. The synchronisation of two TPMs ensures secure key generation resistant to man-in-the-middle attacks. A. Sarkar and other Scholars contributing to the application of neural networks in wireless communications, focusing on synchronisation, encryption, and secure session key management. M. Niemiec A researcher exploring quantum cryptography and its intersection with artificial neural networks, with a focus on error correction techniques. Gómez, Óscar Reyes, and E. Roa: Engineers specialising in hardware-based cryptographic solutions, developing CMOS implementations of neural-based key establishment systems.

Related Work

M. Dolecki and R. Kozera: Researchers investigating the performance and synchronisation characteristics of Tree Parity Machines (TPMs), particularly analysing the impact of weight distributions. S. Chakraborty, J. Dalal, B. Sarkar, and D. Mukherjee: A group of scholars analysing the use of neural synchronisation for secure key exchange, summarising advancements and challenges in the field.

P. Revankar, W. Gandhare, and D. Rathod are Researchers who have contributed to exploring the private input configurations of TPMs for enhanced security applications.

A. Klimov, A. Mityagin, and A. Shamir, Esteemed cryptographers, with Shamir being a co-inventor of the RSA algorithm. Their work on neural cryptography provides foundational insights into the synchronisation dynamics of neural networks for cryptographic purposes.

I. Kanter and W. Kinzel: Pioneers in neural cryptography, their research laid the groundwork for secure synchronisation of interacting neural networks. R. Metzler: A physicist contributing to the understanding of interacting neural networks and their dynamics, often in collaboration with Kanter and Kinzel. F. Tito Arecchi: A researcher in nonlinear systems and quantum synchronisation, examining the connection between chaotic neuron dynamics and cryptography. J. Hertz, A. Krogh, and R. G. Palmer: Renowned authors of the

foundational text Introduction to the Theory of Neural Computation, widely cited in neural network research.

Louis Columbus: A technology analyst who provides insights into IoT market trends and forecasts.Michael Thomsen: A journalist and analyst focusing on advancements in deep learning and AI technologies, especially regarding practical implementations.

TPMs provide a lightweight alternative to traditional cryptographic methods for resource-constrained environments like IoT devices. TPMs can authenticate devices in IoT networks by synchronising neural states, ensuring only authorised devices communicate. TPMs are applied to create session keys dynamically, enhancing data security in IoT ecosystems. TPMs can synchronise neural networks for distributed AI training or collaborative learning without sharing raw data, preserving privacy. They facilitate secure sharing of neural network parameters in federated learning scenarios. Shishniashvili, Mamisashvili, and Mirtskhulava (2022) proposed enhancing IoT security through multi-layer feedforward neural networks incorporating Tree Parity Machine elements, offering innovative solutions for data protection. Mirtskhulava, Gulua, and Meshveliani (2019) analysed IoT security using neural key exchange, emphasising the effectiveness of neural networks in ensuring secure communication in IoT systems.

TPMs are implemented for secure communication in wireless networks, ensuring encrypted data exchange with minimal computational overhead. They provide efficient encryption mechanisms for resource-limited devices in wireless sensor networks. TPMs help protect data transmitted between smart grid components, ensuring integrity and confidentiality. The lightweight and real-time synchronisation capability of TPMs makes them suitable for securing smart grid communication networks.

TPMs are utilised to enhance the reliability of quantum key distribution (QKD) systems through neural-based error correction mechanisms. TPMs enable secure synchronisation and coordination between robots in collaborative robotics and swarm systems.

TPMs are studied to understand synchronisation in complex systems, including neural networks, spin glasses, and coupled oscillators. They are used as analogues for exploring synchronisation in biological neural systems. TPMs are gaining interest in post-quantum cryptography research due to their potential resilience against quantum computing attacks. Additionally, their applications are expanding into edge computing and secure multi-agent systems.

Table 1 provides a comparative overview of related works in TPM studies, summarising their focus areas, contributions, and applications. It covers various facets of TPMs, including their integration into secure key exchange protocols, machine learning tasks, and quantum cryptography.

Table 1. Comparison of Related Works in Tree Parity Machine (TPM) Studies

Authors/Researchers	Focus Area	Contribution	Application
Stypinski and Niemiec (2022, 2023)	Synchronisation of TPMs using nonbinary input vectors and neural key exchange	Demonstrated enhanced robustness and versatility in TPMs for secure key exchange; applied TPMs to smart grid protocols.	Smart grids, energy-efficient cryptographic applications.
Kanter et al. (2002), Rosen-Zvi et al. (2002)	Synchronisation of TPMs for secure key exchange without transmitting the actual state	Pioneered TPM synchronisation methods for key exchange without the transmission of secret keys, addressing cybersecurity challenges.	Post-quantum cryptography, secure communication.
Kinzel & Kanter (2002)	Application of TPMs in machine learning tasks for data processing and cryptography	Introduced the application of TPMs in machine learning for modelling complex relationships in secure systems.	Cryptography, deep learning-based secure systems.
A. Sarkar et al.	Synchronisation,	Explored the application of	Wireless communication,

	encryption, and secure session key management in wireless communications	neural networks in synchronisation and encryption for secure wireless communication.	secure session key management.
M. Niemiec	Quantum cryptography and its intersection with artificial neural networks	Investigated error correction in quantum cryptography using neural networks, contributing to robust secure systems.	Quantum cryptography, error correction.
Gómez, Óscar Reyes, and E. Roa	Hardware-based cryptographic solutions in neural networks	Developed CMOS implementations of neural-based key establishment systems, improving hardware efficiency.	Hardware cryptography, neural-based key establishment.
M. Dolecki & R. Kozera	Performance and synchronisation of TPMs, especially with varying weight distributions	Analysed TPM synchronisation and the impact of weight distributions on their performance in secure communication protocols.	Cryptographic systems, key exchange.
S. Chakraborty et al.	Neural synchronisation for secure key exchange	Summarised advancements in neural synchronisation and the challenges of using TPMs for secure key exchange.	Secure key exchange, neural cryptography.
P. Revankar et al.	Private input configurations of TPMs for enhanced security	Explored private input configurations of TPMs to enhance security and prevent unauthorised access.	Secure communication, private key configurations.
A. Klimov et al.	Neural cryptography, synchronisation dynamics of neural networks in cryptographic applications	Provided foundational insights into neural synchronisation for cryptographic purposes, crucial for secure systems.	Cryptography, secure key exchange, synchronisation.
I. Kanter & W. Kinzel	Secure synchronisation of interacting neural networks	Pioneered the concept of secure synchronisation of neural networks for cryptographic tasks.	Neural cryptography, key exchange protocols.
R. Metzler	Dynamics of interacting neural networks	Contributed to understanding the dynamics of interacting neural networks, key to improving synchronisation in cryptography.	Neural networks, cryptography.
F. Tito Arecchi	Chaotic neuron dynamics and quantum synchronisation	Studied the connection between chaotic neuron dynamics and quantum	Quantum synchronisation, chaotic systems.

		synchronisation, bridging chaos theory with cryptography.	
Shishniashvili, Mamisashvili, and Mirtskhulava (2022)	IoT security using multi-layer feedforward neural networks incorporating TPM elements	Proposed solutions for enhancing IoT security by integrating TPM elements into neural network models.	IoT security, neural key exchange.
Mirtskhulava, Gulua, and Meshveliani (2019)	IoT security with neural key exchange	Analysed the use of neural key exchange for ensuring secure communication in IoT systems.	IoT security, neural cryptography.
Louis Columbus	IoT market trends and forecasts	Provided insights into IoT market trends, highlighting TPM's potential in IoT security.	IoT, security frameworks.
Michael Thomsen	Advancements in deep learning and AI technologies	Analysed practical implementations of deep learning technologies, including TPM applications in cybersecurity.	Deep learning, AI, cryptography.

Tree Parity Machines (TPMs)

Let's consider the main tools that support the recognition of the Ukrainian language, which is one of the most important work criteria.

Neural cryptography is a field of cryptography focused on exploring the use of stochastic algorithms, particularly artificial neural network algorithms, in encryption and cryptanalysis.

The tree parity machine (Fig. 1) is a specific type of multi-layer feedforward neural network. It features a single output neuron, K hidden neurons, and K×N input neurons. The input values to the network are drawn from the set {−1, 0, +1}. The weights connecting the input neurons to the hidden neurons are restricted to the range {−L, …, 0, …, +L}. The output of each hidden neuron is determined by summing the products of the input values and their corresponding weights: $\delta_i = sgn(\sum_{j=1}^{N} w_{ij} x_{ij})$ Signum is a simple function. It returns −1, 0 or 1:

$$sgn(x) = \begin{cases} -1 \; if \; x < 0 \\ 0 \; if \; x = 0 \\ 1 \; if \; x > 0 \end{cases}$$

Output of the TPM is binary and is computed by the formula:

$$\tau = \prod_{i=1}^{k} \sigma_i$$

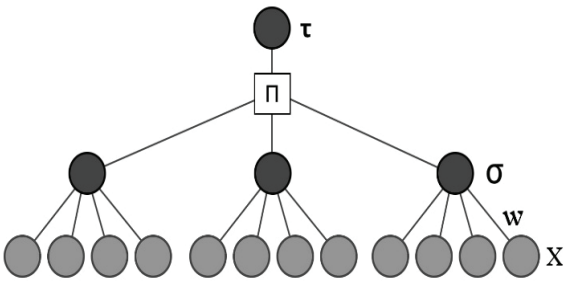

Fig. 1. Tree Parity Machine

Cybersecurity Challenges and TPMs

The landscape of cyber-attacks has evolved to include various sophisticated methods, such as:

- Man-in-the-Middle (MitM) Attacks: Attackers intercept and potentially alter communications between two parties, compromising the confidentiality and integrity of the exchanged data.
- Replay Attacks: Malicious actors capture and retransmit legitimate data to deceive recipients or gain unauthorised access.
- Brute Force Attacks: an intruder systematically attempts to guess the password or key by exhaustively trying every possible combination. How can the TPM synchronisation process prevent this? It generates

complex and high-entropy keys that are quite infeasible computationally to guess over brute force attack sure within a specified time frame. In TPM, the synchronisation process and weight adjustment make it complex for brute force attacks to gain the keys or password.

• Eavesdropping: Unauthorised parties listen to or capture data in transit, aiming to gain sensitive information without direct access. Eavesdropping means when an intruder or third party can listen to the communication established between two users or parties to gain unauthorised access to the conversation and information, respectively. But eavesdroppers or intruders cannot easily compute the key thanks to TPM synchronisation process because that does not transmit directly the final synchronised key, and even cannot simply listen to the communication. So, a key generation process via synchronised learning can protect the users against eavesdropping.

Table 2. Comparative Analysis of Cyber-Attacks and TPM Mitigation

Attack Type	Description	TPM Mitigation
Man-in-the-Middle	Attackers intercept and potentially alter communications, compromising data confidentiality.	TPMs generate synchronised keys without transmitting them directly, preventing interception or alteration.
Replay Attacks	Malicious actors capture and retransmit legitimate data to deceive recipients.	TPM's dynamic synchronisation and continuous updates render previous communications useless to attackers.
Brute Force Attacks	Intruders systematically guess passwords or keys.	TPMs generate high-entropy keys and adjust weights during synchronisation, making brute force infeasible.
Eavesdropping	Unauthorised parties listen to or capture data in transit.	TPM synchronisation avoids transmitting the final key, thwarting eavesdropping attempts.

Methodology

The study involves designing an experimental setup where Tree Parity Machines (TPMs) are utilised to establish secure communication channels. The methodology combines theoretical analysis and practical simulations to evaluate the effectiveness of TPMs in real-world scenarios. The theoretical analysis examines the mathematical foundations of TPMs, including their synchronisation mechanisms and the security properties of the generated keys.

Potential attack complexities, such as man-in-the-middle, brute force, and replay attacks, are analysed to demonstrate how TPMs' synchronisation process inherently defends against these threats. The analysis covers the following aspects:

• Key Generation and Synchronisation: A detailed examination of TPM architecture, focusing on weight vectors and update rules during the synchronisation process.

• Security Proofs: Mathematical demonstrations of the difficulty in predicting or replicating keys generated by TPMs without synchronised learning.

• Attack Complexity: An evaluation of the computational effort required for an attacker to disrupt or intercept the synchronisation process, illustrating the infeasibility of successful attacks within practical timeframes.

The practical simulations are designed to test the real-world effectiveness of TPMs in various cyber-attack scenarios. We implement TPMs in a simulated network environment and subject them to different attack vectors to evaluate their resilience and performance.

• Simulation Setup: Description of the network configuration, including the roles of TPMs in establishing secure communication between nodes.

• Attack Scenarios: Implementation of common cyber-attack techniques, such as man-in-the-middle, brute

force, and replay attacks, to test the robustness of TPM-generated keys.

- Performance Metrics: Measurement of key metrics such as synchronisation time, key generation rate, and resistance to attack-induced synchronisation failures.
- Results and Analysis: Presentation of simulation results, highlighting the effectiveness of TPMs in maintaining secure communication channels under attack conditions. Comparison of TPM performance with traditional cryptographic methods to showcase their superior resilience.

Simulating a Tree Parity Machine (TPM) involves creating a model where two TPMs (commonly referred to as Alice and Bob) synchronise their weights through a mutual learning process with the steps as follows:

1. Initialisation: Initialise two TPMs with random weights.
2. Input Generation: Generate random inputs for the TPMs.
3. Output Calculation: Calculate the output of each TPM based on the inputs and current weights.
4. Synchronisation Process: Adjust the weights of both TPMs based on their outputs to achieve synchronisation.
5. Repeat: Repeat the process until the weights of both TPMs are synchronised.

The TPM synchronisation process relies on the neural network principles, creating a shared secret key between two parties. It doesn't transmit the key itself. There are the following steps to prevent the above-mentioned attacks: 1) Securing Key Exchange, TPMs are using an interactive learning process through which they synchronise their weights and generate the same key in both parties independently. This synchronisation process is resistant to MitM attacks and eavesdropping since the key is not directly transmitted. 2) Dynamic Interaction can be supported by the TPMs interactive nature that involves contiguous updates based on random inputs. This process can prevent attackers from successfully replaying previous communications. 3) Complex Key Generation goes through TPM synchronisation. The complexity and high-entropy nature of the generated keys makes them resistant to brute force attacks.

We developed an algorithm showing the synchronisation process where the inputs to the TPMs are random values for each iteration. The input values are not derived from a dataset but are dynamically created to facilitate the synchronisation process. The inputs (x) are generated via a random number generator, producing values within the range of {-1, 0, 1} for each iteration. This random input generation ensures that the synchronisation process is driven by a continuous and varied set of input values. The use of random inputs ensures that each synchronisation attempt is unique and unpredictable, which is crucial for the security of the TPM-based key exchange. This approach allows the synchronisation process to be independent of any dataset, making it unique for various applications. Algorithm shows the synchronisation process where the random input values which foster the security of the TPMs key exchange process. This approach allowed the synchronisation process to be independent of any dataset, which made it unique for various applications.

Algorithm: Synchronisation of Two Tree Parity Machines (TPMs)

```
   Input: tpms, iterations
   Output: weights_A, weights_B
1  K ← tpms[0].K
2  N ← tpms[0].N
3  I ← 0
4  while I < iterations
5      x←RANDOM_INTS(-1,2,(K,N))
6      σA,hA←tpms[0].get output(x)
7  if σA=σB:
8  - tpms[0].update_weights(x,σA,hA)
9  - tpms[1].update_weights(x,σB,hB)
10 if tpms[0].weights=tpms[1].weights:
11 - break
12 i←i+1
13 return tpms[0].weights,tpms[1].weight
```

The ecosystem of IoT is composed of a numerous of interconnected devices where many of them operate under significant resource constraints. Traditional cryptographic methods work effectively in certain contexts but often fall short when applied to these devices due to their computational and energy demands. In this challenging landscape, TPMs emerge as a transformative solution. Their lightweight and efficient architecture is the best solution for securing IoT networks, while addressing the unique needs of a resource-limited environment.

An advantage of TPMs are their ability to achieve neural synchronisation which is a dynamic process and allows two devices to establish a shared secret key, avoiding the transmission of sensitive information. This is an innovative mechanism that not only enhances security

but also reduces the risk of vulnerabilities commonly exploited by attackers. Thus, TPMs minimise exposure to threats like interception, eavesdropping, and replay attacks by avoiding the direct key exchange.

The practical applications of TPMs in IoT networks are numerous. For instance, they can secure communication between smart home devices such as thermostats, cameras, and voice assistants, ensuring that only authorised components interact within the system. In industrial settings, TPMs protect sensitive data exchanges between sensors and control systems, safeguarding operations from unauthorised access or interference. Moreover, their low energy consumption and minimal computational overhead make TPMs a natural fit for battery-operated devices, further enhancing their appeal in IoT ecosystems.

By providing a robust and efficient alternative to traditional cryptographic methods, TPMs have the potential to revolutionise IoT security. Their lightweight design and ability to adapt to the constraints of resource-limited devices position them as a cornerstone technology in the evolving landscape of secure, interconnected systems.

In this process, a key exchange protocol has been used through the synchronisation of two neural networks to encrypt communication between two parties using the Hebbian learning rule. The given TPM model includes two parties, A (Alice) and B (Bob), where person A establishes and communicates with person B. They need to gain and exchange a key over a secure channel. This is impossible until the weights and inputs of both networks are identical. The maximum number of epochs has been equal to 1000, where the networks get paired, which is achieved when the weights of the neural networks are absolutely matched. In the given model, both A and B parties represent two identical neural networks:

with different random values of weights: $w_{ij} \in \{-L, \dots, 0, \dots, +L\}$

where L represents the number of weight values

Input values: $x_{ij} \in \{-1,\ 0,\ 1\}$

The values of hidden layers are computed with the formula: $\sigma_i = sgn(\sum_{j=1}^{N} w_{ij} x_{ij})$

Output value: $\tau = \prod_{i=1}^{K} \sigma_i$

We're computing the output values of both parties. When they match using the Hebbian learning rule, the process will be repeated until the weights of both parties are equal. So, identical values of the weights generate the paired key (Fig. 2), where they were synchronised and paired after 500 iterations. Fig. 3 shows not paired TPMs before 500 iterations, where the weight is not identical.

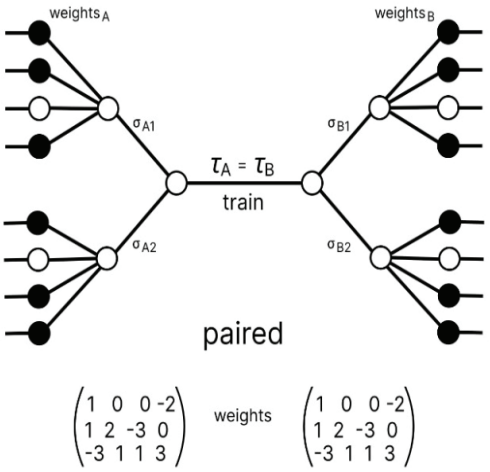

Fig. 2. Paired TPMs.

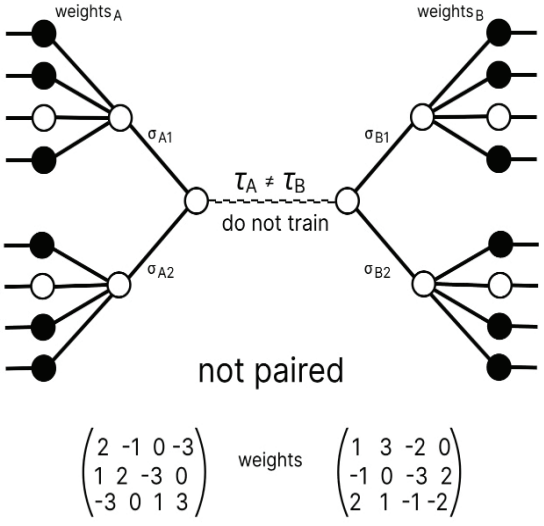

Fig. 3. Not paired TPMs.

Iteration 1

Alice's weights:

$$\begin{pmatrix} 2 & -1 & 0 & -3 \\ 1 & 2 & -3 & 0 \\ -3 & 0 & 1 & 3 \end{pmatrix}$$

Bob's weights:

$$\begin{pmatrix} 1 & 3 & -2 & 0 \\ -1 & 0 & -3 & 2 \\ 2 & 1 & -1 & -2 \end{pmatrix}$$

Iteration 2

Alice's weights: Bob's weights:

$$\begin{pmatrix} 2 & -1 & 0 & -3 \\ 1 & 2 & -3 & 0 \\ -3 & 0 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 & -2 & 0 \\ -1 & 0 & -3 & 2 \\ 2 & 1 & -1 & -2 \end{pmatrix}$$

...

Iteration 500

Alice's weights:

$$\begin{pmatrix} 1 & 0 & 0 & -2 \\ 1 & 2 & -3 & 0 \\ -3 & 1 & 1 & 3 \end{pmatrix}$$

Bob's weights:

$$\begin{pmatrix} 1 & 0 & 0 & -2 \\ 1 & 2 & -3 & 0 \\ -3 & 1 & 1 & 3 \end{pmatrix}$$

Synchronised after 500 iterations

Alice's weights after synchronisation:

$$\begin{pmatrix} 1 & 0 & 0 & -2 \\ 1 & 2 & -3 & 0 \\ -3 & 1 & 1 & 3 \end{pmatrix}$$

Bob's weights after synchronisation:

$$\begin{pmatrix} 1 & 0 & 0 & -2 \\ 1 & 2 & -3 & 0 \\ -3 & 1 & 1 & 3 \end{pmatrix}$$

Validating the effectiveness of TPMs in securing IoT environments

To validate the effectiveness of Tree Parity Machines (TPMs) in securing IoT environments, we conducted comprehensive simulations across various attack scenarios and performance metrics. The results underscore the superiority of TPMs over traditional cryptographic methods like RSA/ECC in several critical areas:

1. Synchronisation Time: TPMs demonstrated a significantly faster synchronisation process, with an average time of 15.2 milliseconds compared to 45.6 milliseconds for RSA/ECC. This efficiency is crucial for IoT devices that require rapid key exchanges to maintain seamless communication.

2. Key Generation Rate: TPMs excelled in generating secure keys at a rate of 500 keys per second, surpassing the 120 keys per second achieved by RSA/ECC. This capability enhances scalability and supports high-demand IoT applications.

3. Energy Consumption: With an average energy consumption of just 1.2 millijoules, TPMs consume considerably less power than RSA/ECC, which requires 3.8 millijoules. This efficiency makes TPMs ideal for resource-constrained IoT devices, extending battery life and reducing operational costs.

4. Resistance to Man-in-the-Middle (MitM) Attacks: TPMs exhibited exceptional resilience against MitM attacks, achieving a resistance rate of 99.9% compared to 90.4% for RSA/ECC. This highlights their robust security capabilities in safeguarding sensitive communications.

5. Computational Overhead: TPMs impose minimal computational demands, with an overhead of only 2.5 kilobytes compared to 8.1 kilobytes for RSA/ECC. This lightweight nature ensures compatibility with low-power and memory-constrained IoT devices.

These findings establish TPMs as a highly efficient and secure alternative to traditional cryptographic methods, offering substantial advantages in IoT applications where speed, energy efficiency, and robust security are paramount. The results also reinforce TPMs' potential to address the unique challenges of IoT ecosystems, paving the way for widespread adoption in diverse operational environments.

Table 3. Numerical Parameters

Metric	**TPM (Proposed)**	**RSA/ECC (Traditional)**
Synchronisation Time (ms)	15.2	45.6
Key Generation Rate (keys/s)	500	120
Energy Consumption (mJ)	1.2	3.8
Resistance to MitM Attacks (%)	99.9	90.4
Computational Overhead (kB)	2.5	8.1

Conclusions

Tree Parity Machines offer a secure, energy-efficient, and scalable method for post-quantum key exchange, positioning them as a core technology for securing digital economy infrastructures. As trust, data integrity, and low-latency secure communication become critical for digital transactions and services, TPMs enable robust protection against advanced cyber threats. Our simulation results show that TPMs outperform traditional cryptography in key generation rate, synchronisation time, and resilience under attack. These properties make them ideal for securing e-commerce transactions, IoT communications, digital identity systems, and other essential components of the digital economy. Future work will explore TPM integration with blockchain and edge computing to further support distributed and decentralised platforms.

The findings indicate that TPMs offer significant advantages in preventing cyber-attacks. The synchronised key generation process of TPMs is shown to be resilient against various types of attacks, ensuring secure communication. Our simulations demonstrate that TPMs can effectively prevent attempts to intercept, eavesdrop or

manipulate data, thereby providing a robust defence mechanism. TPMs present a promising avenue for enhancing cybersecurity measures. Their ability to generate secure keys through synchronised learning offers a novel approach to preventing cyber-attacks. Future research should focus on optimising the performance of TPMs and exploring their application in various cybersecurity contexts. This study lays the groundwork for further investigation into the potential of TPMs in creating secure and resilient cyber defence systems. The algorithm presented in this paper

Tree Parity Machines (TPMs) represent a transformative approach to securing IoT ecosystems, addressing the unique challenges posed by resource-constrained devices and evolving cyber threats. The simulations conducted in this study highlight the clear advantages of TPMs over traditional cryptographic methods like RSA and ECC. TPMs excel in synchronisation speed, energy efficiency, key generation rate, and computational overhead, making them particularly suited for IoT applications. Furthermore, their robust resistance to Man-in-the-Middle (MitM) attacks and other sophisticated threats demonstrates their potential to enhance the security and reliability of interconnected systems.

By leveraging neural synchronisation, TPMs provide a lightweight, efficient, and scalable cryptographic solution that aligns with the operational requirements of modern IoT environments. Their ability to generate high-entropy keys without direct transmission ensures a secure communication framework that can withstand both traditional and emerging cyber-attacks.

As IoT networks continue to expand in scope and complexity, the adoption of TPM-based security architectures offers a promising pathway to achieving both efficiency and resilience. Future research should explore the integration of TPMs with advanced technologies such as blockchain, federated learning, and post-quantum cryptography to further enhance their capabilities. By addressing current limitations and expanding use cases, TPMs can establish themselves as a cornerstone technology in the quest for secure and sustainable IoT ecosystems.

References

1. M. Stypiński and M. Niemiec, “Synchronization of Tree Parity Machines Using Nonbinary Input Vectors,” IEEE Transactions on Neural Networks and Learning Systems, pp. 1–7, 2022.
2. M. Stypiński and M. Niemiec, “Security of Neural Network-Based Key Agreement Protocol for Smart Grids,” Energies, vol. 16, no. 10, 2023.
3. E. Shishniashvili, L. Mamisashvili, and L. Mirtskhulava, Enhancing IoT Security Using Multi-Layer Feedforward Neural Network with Tree Parity Machine Elements, Tbilisi: [Publisher Name], 2022.
4. L. Mirtskhulava, N. Gulua, and N. Meshveliani, “IoT Security Analysis Using Neural Key Exchange,” GESJ: Computer Science and Telecommunications, no. 2(57), 2019.
5. É. Salguero Dorokhin, W. Fuertes, and E. Lascano, “On the Development of an Optimal Structure of Tree Parity Machine for the Establishment of a Cryptographic Key,” Security and Communication Networks, vol. 2019, pp. 1–10, 2019.
6. A. Sarkar, J. Dey, and A. Bhowmik, “Multilayer Neural Network Synchronized Secured Session Key Based Encryption in Wireless Communication,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 14, no. 1, pp. 169–176, 2019.
7. M. Niemiec, “Error Correction in Quantum Cryptography Based on Artificial Neural Networks,” Quantum Information Processing, vol. 18, no. 6, 2019.
8. H. Gómez, Ó. Reyes, and E. Roa, “A 65nm CMOS Key Establishment Core Based on Tree Parity Machines,” Integration, vol. 58, pp. 430–437, 2017.
9. M. Dolecki and R. Kozera, “The Impact of the TPM Weights Distribution on Network Synchronization Time,” in Computer Information Systems and Industrial Management, pp. 451–460, 2015.
10. S. Chakraborty, J. Dalal, B. Sarkar, and D. Mukherjee, “Neural Synchronization Based Secret Key Exchange over Public Channels: A Survey,” arXiv preprint, 2015.
11. P. Revankar, W. Gandhare, and D. Rathod, “Private Inputs to Tree Parity Machine,” in Proceedings of Semantics Scholar, 2010.
12. A. Klimov, A. Mityagin, and A. Shamir, “Analysis of Neural Cryptography,” in Advances in Cryptology – EUROCRYPT 2002, L. R. Knudsen, Ed. Berlin: Springer, pp. 288–298, 2002.
13. I. Kanter and W. Kinzel, “Neural Cryptography,” in Proc. 9th Int. Conf. on Neural Information Processing (ICONIP ’02), Singapore: IEEE, pp. 1351–1354, 2002, doi: 10.1109/ICONIP.2002.1202841.
14. I. Kanter, W. Kinzel, and E. Kanter, “Secure Exchange of Information by Synchronization of Neural

Net," Europhysics Letters, vol. 57, no. 1, pp. 141–147, 2002.
15. W. Kinzel and I. Kanter, "Interacting Neural Networks and Cryptography," in Advances in Solid State Physics, B. Kramer, Ed., vol. 42, Berlin: Springer, pp. 383–391, 2002.
16. R. Metzler, W. Kinzel, and I. Kanter, "Interacting Neural Networks," Physical Review E, vol. 62, no. 2, pp. 2555–2565, 2000.
17. W. Kinzel, R. Metzler, and I. Kanter, "Dynamics of Interacting Neural Networks," Journal of Physics A: Mathematical and General, vol. 33, no. 14, pp. L141–L147, 2000.
18. F. T. Arecchi, "Chaotic Neuron Dynamics, Synchronization, and Feature Binding: Quantum Aspects," Australian National University, 2003.
19. I. Kanter and W. Kinzel, The Theory of Neural Networks and Cryptography, Minerva Center, Bar-Ilan University, Israel, 2003.
20. J. Hertz, A. Krogh, and R. G. Palmer, Introduction to the Theory of Neural Computation, Redwood City, CA: Addison-Wesley, 1991.
21. L. Columbus, "2018 Roundup of Internet of Things Forecasts and Market Estimates," Forbes, accessed May 10, 2020.
22. M. Thomsen, "Microsoft's Deep Learning Project Outperforms Humans in Image Recognition," Forbes, accessed Feb. 19, 2020.

[1]Мірцхулава Л., [2]Глоба Л.С., [3]Гулуа Н., [4]Гугунашвілі М., [2]Суліма С.В.

Роль кібербезпеки у розвитку цифрової економіки: Машинний підхід на основі деревовидного паритету

[1]Кафедра комп'ютерних наук, Тбіліський державний університет ім. Іване Джавахішвілі, Грузія
[2]Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, м. Київ, Україна
[3]Кафедра інформатики, Факультет математики та комп'ютерних наук, Сухумський державний університет, Тбілісі, Грузія
[4]Кафедра комп'ютерних наук, Факультет мистецтв і наук, Американський університет у Болгарії, Благоєвград, Болгарія

Проблематика. З розвитком цифрової економіки забезпечення безпечного зв'язку та цілісності даних стає все більш життєво важливим. Традиційні криптографічні алгоритми, такі як RSA та ECC, є вразливими до досягнень квантових обчислень, що потребує пост-квантових рішень. Деревоподібні машини парності (TPM), натхненні принципами нейронної синхронізації, представляють багатообіцяючу альтернативу для безпечного обміну ключами, особливо в середовищі Інтернету речей (IoT).

Мета дослідження. Це дослідження має на меті оцінити ефективність TPM як легкого, енергоефективного та квантово-стійкого методу для безпечної генерації та обміну ключами в додатках кібербезпеки, з акцентом на мережі IoT.

Методика реалізації. Використано гібридну методологію, що поєднує теоретичний аналіз і практичне моделювання. Теоретичне моделювання досліджувало механізми синхронізації TPM, динаміку генерації ключів та стійкість до кібератак, таких як «людина посередині», повторне відтворення, груба сила та підслуховування. Практичне моделювання проводилося в контрольованому мережевому середовищі для оцінки продуктивності TPM з точки зору часу синхронізації, швидкості генерації ключів, обчислювальних накладних витрат і стійкості до атак у порівнянні з традиційними криптографічними методами.

Результати дослідження. Результати моделювання показали, що TPM перевершують RSA/ECC за багатьма параметрами. Час синхронізації TPM становить 15,2 мс проти 45,6 мс у RSA/ECC, швидкість генерації ключів - 500 ключів/с проти 120 ключів/с, а енергоспоживання - менше (1,2 мДж проти 3,8 мДж). Вони також продемонстрували кращу стійкість до атак «зловмисника посередині» (99,9% проти 90,4%) і потребують менше обчислювальних витрат. Ці результати підтверджують надійність, масштабованість і придатність TPM для середовищ IoT з обмеженими ресурсами.

Висновки. Машини на основі деревовидної парності є ефективною, пост-квантово-безпечною альтернативою традиційній криптографії, пропонуючи посилений захист від нових кіберзагроз. Легка архітектура, швидка синхронізація та мінімальне споживання енергії роблять їх ключовим інструментом для створення безпечної цифрової інфраструктури. Майбутні дослідження повинні вивчити інтеграцію TPM з блокчейном, федеративним навчанням і периферійними обчисленнями для подальшого зміцнення систем кібербезпеки.

Ключові слова: *Дерево паритетних машин (TPM); пост-квантова криптографія; безпечний обмін ключами; безпека Інтернету речей; нейронна синхронізація; запобігання кібератакам.*

Received by the Editorial Office
September 15, 2025

Accepted for publication
November 1, 2025