Factors Affecting the Distribution of Extreme Values in Synchronized Tree Parity Machines

Mykyta Aleksandrov[1,†], Yevgen Bashkov[1,*,†]

[1] Donetsk National Technical University, Shevchenka Str. 9, 82100 Drohobych, Ukraine

Abstract

Mutual synchronization of tree parity machines (TPM) is a promising direction for building cryptographic key exchange systems. An important characteristic of a synchronized network is the distribution of weight coefficients, since it directly affects the cryptographic stability of the generated key and the overall stability of the system to statistical attacks. The paper studies the influence of neural network architecture on the number of extreme values after the completion of the TPM mutual synchronization process. Architectures with a total number of weight coefficients from 25 to 100 and weight value ranges L=1, L=2 and L=3 were experimentally investigated. 1000 iterations of mutual synchronization were performed for each configuration. The results obtained showed that with an increase in the parameter L, the number of weight coefficients equal to the limiting value ±L decreases significantly. At the same time, the experiments demonstrate that the total number of neurons has almost no effect on this indicator. The results obtained can be used to improve the cryptographic stability of future TPM-based systems.

Keywords

neurocryptography, tree parity machine, neural network, synchronization, cryptographic key.

1. Introduction

Modern information systems require reliable mechanisms for data protection and secure exchange of cryptographic keys. Traditional asymmetric cryptography algorithms are based on the complexity of mathematical problems and require significant computing resources [1-3]. In this regard, alternative approaches are actively developing, such as the use of the phenomenon of mutual synchronization of artificial neural networks. Tree parity machines allow two parties to form the same set of weight coefficients without their direct transmission over the communication channel [4-6].

Previous studies investigated synchronization verification, key generation based on synchronized weights, and methods for accelerating TPM synchronization. Recently, attention has also been paid to the influence of weight distribution and the use of nonbinary input vectors on the cryptographic properties of Tree Parity Machines [7–12]. However, the statistical distribution of extreme weight values after mutual synchronization remains insufficiently studied.

2. Relevance of the research

The number of extreme values of the weight coefficients after synchronization is completed directly affects the cryptographic stability of systems using mutually synchronized TPMs. Additionally, extreme values can be used as another criterion for confirming the completion of synchronization. The distribution of weights also affects the entropy of the generated secret key, which in turn can affect stability. Statistical data on the distribution of weight coefficients can be used when assessing the stability of the system to various attacks, in particular statistical analysis.

[1]RS-2026: Resilient Systems: Secure Digital Technologies and Critical Infrastructure, June 30, 2026, Drohobych, Ukraine
* Corresponding author.
† These authors contributed equally.
mykyta.aleksandrov@donntu.edu.ua (M. Aleksandrov); eab23may@gmail.com (Y. Bashkov)
0000-0002-2754-2139 (M. Aleksandrov); 0000-0001-6974-4882 (Y. Bashkov)

3. Statement of the Problem

The aim of the work is to study the influence of the weight range parameter and the architecture of the tree parity machine on the number of extreme values after mutual synchronization is completed. To achieve the set goal, the following tasks were defined:

1. To conduct a series of experiments for TPMs of different architectures.
2. To synchronize networks for different values of the parameter L.
3. To determine the proportion of weight coefficients reaching extreme values ±L.
4. To analyze the influence of the network architecture and the parameter L on the obtained results.
5. To assess the statistical stability of the obtained dependencies.

4. Research Results

4.1. Tree Parity Machine Model

The experiments used the classical Tree Parity Machine model, consisting of K hidden neurons and N inputs for each hidden neuron. The state of a hidden neuron is defined by the expression:

$$\sigma_i = sgn(\sum_{j=1}^{N} w_{ij} x_{ij}), \text{(1)}$$

where:

- x_{ij} - input signal;
- w_{ij} - weight coefficient.

The output of the network is defined as:

$$\tau = \prod_{i=1}^{K} \sigma_i, \text{(2)}$$

Training was performed using the Hebbian learning rule [5].

4.2. Experimental methodology

The following TPM architectures were used for the study (INPUT x HIDDEN neurons): 5×5, 5×10, 5×15, 5×20, 10×5, 15×5, 20×5.

The study was performed for the values

$$L \in \{1,2,3\} \text{ (3)}$$

Where the accuracy was determined by 6 decimal places for the value of L. That is, for L=1 (-1.000000, 1.000000) the number of possible states was 2 000 000. For L=2 and L=3 it was two and three times more, respectively.

For each configuration, 1000 independent runs of the mutual synchronization process were performed. After synchronization was completed, the number of weight coefficients that were in the extreme states was determined:

$$w = \pm L, \text{(4).}$$

The obtained value was normalized relative to the total number of weight coefficients.

4.3. Analysis of the results

Table 1 shows the results of all experiments conducted with different architectures and ranges of weight coefficients L. Also, for greater clarity, a graph (Fig. 1) is additionally formed, which shows the dependence of the number of extreme values on the total number of TPM weight coefficients after the completion of mutual synchronization.

Table 1

Results of experiments

N	K	L	Weights	Min %	Mean %	Median %	Max %
5	5	1	25	4	34.872	36	64
5	10	1	50	14	32.902	34	54
10	5	1	50	14	32.796	32	56
5	15	1	75	16	32.607	32	49.3
15	5	1	75	17.3	32.46	32	49.3
5	20	1	100	19	32.378	32	47
20	5	1	100	18	32.152	32	47
5	5	2	25	4	21.34	20	52
5	10	2	50	6	19.468	20	38
10	5	2	50	2	19.56	20	36
5	15	2	75	6.7	18.792	18.6	34.6
15	5	2	75	5.3	19.065	18.67	32
5	20	2	100	9	18.816	19	31
20	5	2	100	9	18.914	19	32
5	5	3	25	4	16.188	16	36
5	10	3	50	2	14.422	14	32
10	5	3	50	2	14.458	14	38
5	15	3	75	2. 7	13.685	13.3	29.3
15	5	3	75	1.3	13.634	13.3	29.3
5	20	3	100	5	13.381	13	25
20	5	3	100	4	13.378	13	25

The results obtained demonstrate that for a fixed value of the parameter L, the share of extreme values remains practically constant even when the number of weight coefficients increases from 25 to 100. This confirms the absence of influence of the total number of synapses of the system on the share of extreme values. Also, according to the results of the experiments, it can be stated that the ratio of the number of input to the number of hidden neurons does not influence the number of extreme values.

It can also be seen that the largest values of the number of extreme values are observed for L=1 and are about 32–35% of all synapse values, while for L=3 this figure decreases to 13–16%. However, it should be noted that increasing the value of parameter L negatively affects the time of mutual synchronization of networks, as was demonstrated in previous works.[6-7]

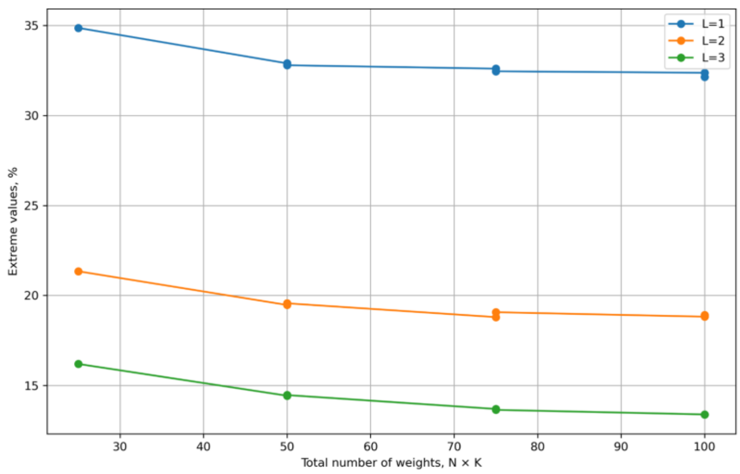

Figure 1: Extreme Values Depending on TPM Size

Fig. 2 shows the influence of the weight range parameter L on the total share of extreme values. The obtained results demonstrate a tendency to decrease the share of extreme values with an increase in the weight range L. A similar pattern is observed for all studied architectures, which indicates a much more significant influence of the parameter L compared to the influence of the total number of synapses in the network.

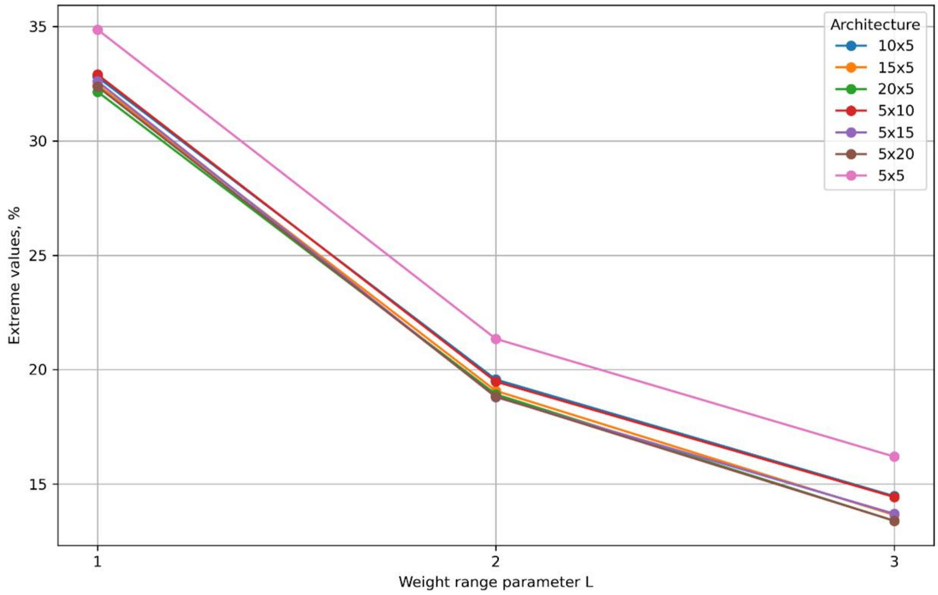

Figure 2: Extreme Values Depending on Weight Range L

Fig. 3 shows the results taking into account the standard deviation. The relatively small values of the standard deviation indicate the stability of the obtained results and their reproducibility when performing the experiments repeatedly. As the number of permissible states increases, the probability of finding the weight coefficient in extreme positions decreases.

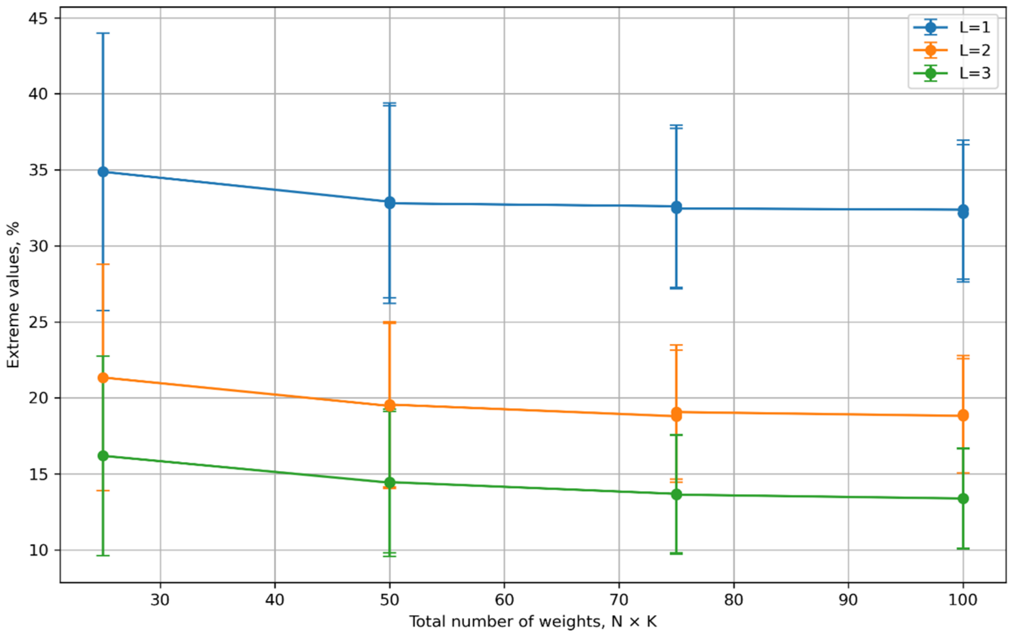

Figure 3: Extreme Values Depending on Weight Range L

At the same time, the obtained results show that after synchronization the distribution of weights is not uniform. Even for the largest studied values of the parameter L, extreme states occur much more often than one would expect. This indicates the existence of non-obvious regularities in the process of mutual synchronization of TPMs, which require further theoretical study.

5. Conclusions

As part of the study, a statistical experimental verification of the distribution of extreme values of weight coefficients in mutually synchronized tree parity machines was carried out. It was found that the greatest influence on the number of extreme values is exerted by the value of the range of weight coefficients L. With an increase in the parameter L from 1 to 3, the proportion of extreme values decreases approximately by half. At the same time, it was proved that the influence of the TPM architecture on the proportion of extreme values is insignificant and can be disregarded when trying to predict the total proportion of extreme values. Also, the ratio of the number of input neurons to hidden neurons does not affect the number of extreme values of synchronized synapses.

The results obtained can be used when evaluating the entropy of the formed keys and developing more cryptographically stable cryptographic systems using tree parity machines. Further research should be directed at building a mathematical model of the distribution of weight coefficients after the completion of mutual synchronization of TPM and at finding additional compensation mechanisms that will reduce the number of extreme values without the need to increase the range of weight coefficients L.

Acknowledgements

The authors received no external funding for this research.

Declaration on Generative AI

During the preparation of this work, the author(s) used GPT-5.5 in order to: Grammar and spelling check. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, New York, NY, USA, 2nd ed., 2007.

[2] C. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal 28 (4) (1949) 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x

[3] N. Ferguson, B. Schneier, Practical Cryptography, John Wiley & Sons, Indianapolis, IN, USA, 2003.

[4] W. Diffie, M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory 22 (6) (1976) 644–654. doi:10.1109/TIT.1976.1055638

[5] M. Volkmer, S. Wallner, Tree Parity Machine Rekeying Architectures, IEEE Transactions on Computers 54 (4) (2005) 421–427. doi:10.1109/TC.2005.70

[6] W. Kinzel, I. Kanter, Neural Cryptography, in: Proceedings of the 9th International Conference on Neural Information Processing (ICONIP 2002), Vol. 3, Singapore, 2002, pp. 1351–1354.

[7] M. Aleksandrov, Use of Interacting Neural Networks in Cryptography, Computer Science, Cybernetics and Computer Engineering, Donetsk National Technical University, 1 (30)

(2020) 19–24. doi:10.31474/1996-1588-2020-1-30-19-24

[8] M. Aleksandrov, Y. Bashkov, Factors Affecting Synchronization Time of Tree Parity Machines in Cryptography, in: Proceedings of the 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2020, pp. 108-112, doi: 10.1109/ATIT50783.2020.9349327.

[9] M. Aleksandrov, Confirmation of Mutual Synchronization of the TPMs Using Hash Functions, in: Proceedings of the 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2021, pp. 80–83. doi:10.1109/ATIT54053.2021.9678779

[10] M. Aleksandrov, Y. Bashkov, Method Using Partial Data to Confirm Completion of the Tree Parity Machines Synchronization, in: Proceedings of the 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 177-180, doi: 10.1109/ATIT58178.2022.10024234.

[11] M. Stypiński, M. Niemiec, Synchronization of Tree Parity Machines Using Nonbinary Input Vectors, IEEE Transactions on Neural Networks and Learning Systems, 35 (1) (2024) 1423–1429. doi:10.1109/TNNLS.2022.3180197

[12] M. Stypiński, M. Niemiec, Weight Equalization Algorithm for Tree Parity Machines, Computer Networks 252 (2025) 110988. doi:10.1016/j.comnet.2024.110988