Split-complex numbers in neural cryptography

M. Płonkowski, P. Urbanovich
John Paul II Catholic University of Lublin, Lublin, Poland,
E-mail: marcin.plonkowski@kul.pl

A new field of research on neural networks, which uses neural network methods in cryptographic solutions is known as neural cryptography. One of its most important aspects is the application of the TPM (Tree Parity Machine) architectures in the key exchange protocol [1]. However, unlike the well known Diffie-Hellman key exchange protocol, it does not use the number theory and it is not based on the factoring problem.

Nevertheless, the classic TPM model turned out to be susceptible to the cryptographic attacks (genetic, geometric and probabilistic attacks). The geometric attack considered as the most dangerous one threatened the security of the key exchange protocol based on the TPM architecture. That is why, new solutions have been found in order to guarantee a higher level of security and greater resistance to the known attack patterns [2]. One of these solutions is the application of the complex numbers in the TPCM (Tree Parity Complex Machine) architecture. Thanks to the use of a more advanced, complex transfer function, the key exchange protocol based on the TPCM architecture turned out to be resistant to the geometric attack. Other solutions based on the extension of the real number system have been found (quaternions - TPQM and octonions – TPOM). However, apart from ensuring a higher level of security, these solutions proved to have lower time efficiency [3].

This article describes the TPSCM (Tree Parity Split–Complex Machine) architecture based on the algebraic structure of the split-complex numbers and is founded on the classic TPM model. Nonetheless, the use of the new algebraic structure will require a change to the transfer function and a modification to the training algorithm.

In addition, proposals of other algebraic structures which could be used in the TPM architecture's modification will be presented. One of the chief assets of the solutions proposed herein is greater flexibility in the choice of the TPSCM architecture's parameters (e.g. the choice of the set restricting the weight vector).

The higher level of security of the TPSCM architecture as compared to the classic TPM model are confirmed by mathematical analyses and real simulations. Finally, the proposed solutions' results will be presented in terms of their efficiency and security level as compared to similar TPM architecture's modifications (TPCM, TPQM, TPOM).

References

[1] Kanter I., Kinzel W., Vanstone S.A.: *Secure exchange of information by synchronization of neural networks*, Europhys. Lett. 57, 2002, p. 141-147.

[2] Klimov A., Mityaguine A., Shamir A.: *Analysis of Neural Cryptography*, Advances in Cryptology, ASIACRYPT, 2002, p. 823-828.

[3] Płonkowski M., Urbanowicz P.: *Криптографическое преобразование информации на основе нейросетевых технологии*, Труды БГТУ. Серия VI. Минск: БГТУ, 2005, p. 161-164.