The appearance of conflict by using the chaos function to calculate the hash code

P. Urbanovich[1), 2)], M. Plonkowski[2)], K. Churikau[1)]
[1)] Belarussian State Technological University, Minsk, Belarus,
E-mail: chkv85@gmail.com
[2)] Lublin Catholic University, Lublin, Poland

The use of artificial neural networks (ANN) for modeling cryptographic information transfer systems is a new, promising trend in the field of information security.

There are three basic learning algorithms of ANN: with teacher, without a teacher, with reinforcement.

ANN interaction model of "learning without a teacher" has the following properties: mutual learning, self-learning, stochastic behavior, low sensitivity to noise, inaccuracies (data distortion, weights weighting coefficients, program errors). These properties can be used to solve the crypto-conversion problems in systems with a public key, for key distribution, for hash messages and for generation of pseudorandom numbers.

In [1] a neural network architecture for hashing messages is proposed. In [2] this idea was developed through the use of complex numbers algebra. In this case, the neural network model suggests to use the dependencies known from chaos theory as a transition functions.

They are:

totality of the Julia set - a set of chaotic dynamics:

$$z_{n+1} = z^2_n + c;$$

equation of Duffing oscillator:

$$\begin{cases} x_{n+1} = x_n + y_n, \\ y_{n+1} = y_n - x^3_n + ax_n - by_n; \end{cases}$$

equation of Hanon:

$$\begin{cases} x_{n+1} = y_n + 1 + ax^2, \\ y_{n+1} = bx. \end{cases}$$

An important aspect of these functions is their resistance to conflict, which affects the security of the entire neural network as a hash function. This concerns the question of the existence of two different input vectors, generating a single output value. The analysis showed that the emergence of collisions in the equation describing the Julia set arise 3 times less than in the equation of Duffing oscillator, and they arise 4 times more often in the Hénon equation: if you take the emergence of collisions in the equation of the Duffing oscillator for the average value of 1, then the equation describes the conflicts of the Julia set is equal to 0.33, while in the Henon equation is equal to 4.

References

[1] Kinzel W., Kanter I.: *Interacting neural networks and cryptography*, Advances in Solid State Physics 42 Springer, 2002, p. 383-392.

[2] Plonkowski M.: *Analiza funkcji chaosu w funkcjach skrótu opartych na sieciach neuronowych*, Przegląd Elektrotechniczny 3/2008, 2008, p. 102-104.