УДК 004.9

М.В. Некрасова, канд. техн. наук, доц., НТУ «ХПІ»

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ СТВОРЕННЯ ТА ТЕСТУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

У статті представлено огляд сучасних досліджень у галузі нейрокриптографії, присвячених генераторам псевдовипадкових чисел (ГПВЧ). Розглянуто різні типи ГПВЧ та їх реалізації, а також визначено критерії криптографічної стійкості генераторів. Окреслено причини вибору конкретних типів генераторів залежно від поставлених завдань. Наведено основи теорії нейронних мереж (НМ) та проведено порівняння їх архітектур у контексті створення ГПВЧ та тестування вихідних послідовностей. Оглянуто різні набори статистичних тестів для оцінки якості вихідних послідовностей ГПВЧ. Проаналізовано результати ключових досліджень щодо генерації ГПВЧ на основі НМ, включно з класичними рекурентними мережами (Elman, LSTM) та сучасними генеративно-змагальними мережами (GAN). Окремо розглянуто методи тестування ГПВЧ за допомогою НМ та наголошено на негативних наслідках недооцінки цього етапу в оцінці безпеки генераторів.

Ключові слова: псевдовипадкові числа, генератор псевдовипадеових чисел, нейрокриптографія, нейронні мережі, тестування ГПВЧ, створення ГПВЧ, криптографічна стійкість.

This article presents a review of recent research in the field of neurocryptography focused on pseudorandom number generators (PRNGs). Various types of PRNGs and their implementations are discussed, and the criteria for cryptographic security of generators are outlined. The reasons for selecting specific types of generators depending on the tasks are highlighted. The fundamentals of neural network (NN) theory are presented, and a comparison of their architectures in the context of PRNG design and output sequence testing is provided. Different sets of statistical tests for evaluating the quality of PRNG output sequences are reviewed. Key studies on PRNG generation based on neural networks, including classical recurrent networks (Elman, LSTM) and modern generative adversarial networks (GAN), are analyzed. Methods for testing PRNGs using neural networks are also discussed, emphasizing the potential negative consequences of underestimating this stage in the assessment of generator security.

Keywords: pseudorandom numbers, pseudorandom number generator, neurocryptography, neural networks, PRNG testing, PRNG design, cryptographic security.

Список літератури

1.*Apdullah Y., Yakup K.* Neural Network Based Cryptography. Neural Network World. 2014, no. 24, p. 177–192.

2. *Kannan M.R. Gnanam V.* Neural network based decryption for random encryption algorithms. Proceedings of 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, Hong Kong, 20-22 August 2009, p. 603–605.

3. *Oak R., Rahalkar C., Dhaval G.* Using Generative Adversarial Networks for Secure Pseudorandom Number
Generation. Proceedings of 2019 ACM SIGSAC Conference, London, 11–15 November 2019, p. 2597–2599.

4. *İnce K.* Security Analysis of Java SecureRandom Library. Avrupa Bilim ve Teknoloji Dergisi. 2021, no. 24,
p. 157–160.

5. *Lauria F.E.* On Neurocryptology. Proceedings of the Third Italian Workshop on Parallel Architectures and Neural Networks. Salerno, 15-18 May, 1990. p. 337–343.

6. *Pointcheval D.* Neural networks and their cryptographic applications. Livre des resumes Eurocode Institute for Research in Computer Science and Automation. 1994. p. 1–7.

7. *Schneider B.* Applied Cryptography. Protocols, Algorithms, and Source codes in C. New York, Wiley, 1996. – 758 p.

8. *Luciano D., Prichett G.* Cryptology: From Caesar Ciphers to Public-key Cryptosystems. The College Mathematics Journal. 1987, no. 18(1), p. 2–17.

9. *Godhavari T., Alainelu N.R., Soundararajan R.* Cryptography using neural network. IEEE INDICON 2005 Conf., Chennai, India; 11-13 December 2005, p. 258–261.

10. *Arvandi M., Wu S., Sadeghian A., Melek W.W.,* Woungang I. Symmetric Cipher Design Using Recurrent
Neural Networks. The 2006 IEEE International Joint Conference on Neural Network Proceedings, Vancouver,
BC, Canada, 2006, p. 2039–2046.

11. *Guo D., Cheng L.-M., Cheng L. L.* A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks. Applied Intelligence. 1999, no. 10(1), p. 71–84.

12. *Noughabi A. M. N., Sadeghiyan B.* Design of S-boxes based on neural networks. Proceedings of “International Conference on Electronics and

Information Engineering", Kyoto, 1-3 August 2010, p. 172–178.
13. *Karras D. A. Zorkadis V.* On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators. Neural networks: the official journal of the International Neural Network Society. 2003, no. 16(5-6), p. 899–905.
14. *Ruttor A.* Neural Synchronization and Cryptography. PhD thesis. Bayerischen Julius-Maximilians-Universitat at Wurzburg. 2006.
15. *Sadırodlu S., Ozkaya N.* Neural Solutions for Information Security. Journal of Polytechnic. 2007, vol. 10, no. 1, p. 21–25.
16. *Blum L., Blum M., Shub M.* A simple unpredictable pseudo random number generator. SIAM Journal on Computing. 1986, vol. 15, no. 2, p. 364–383.
17. *Matsumoto M., Nishimura T.* Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Transactions on Modelling and Computer Simulation. 1998, vol. 8, no. 1, p. 3–30.
18. *Abdi H.* A neural network primer. Journal of Biological Systems. 1994, vol. 2, no. 3, p. 247–281.
19. *Eastlake D.E., Jones P.E.* US Secure Hash Algorithm 1 (SHA1). Request for Comments. 2001, no. 3174, p. 1–22.
20. *Fausett V.L.* Fundamentals of neural networks: architectures, algorithms, and applications. Pearson, USA, 1994. – 480 p.
21. *McCulloch W.S., Pitts W.* A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics. 1943, no. 5(4), p.115–133.
22. *Gurney K.* An Introduction to Neural Networks (1st ed.). London: CRC Press, 1997. – 234 p.
23. *Vrahatis M., Magoulas G., Parsopoulos K., Plagianakos V.* Introduction to artificial neural network training and applications. Proceedings of 15th Annual Conference of Hellenic Society for Neuroscience, Greece,
27 – 29 October 2000, p. 1–14.
24. *Kingma D.P., Ba J.* Adam: A method for stochastic optimization. Proceedings of International Conference on
Learning Representations (ICLR), San Diego, 7 – 9 May 2015, p. 1–13.
25. *Abadi M., Barham P., Chen J.* Tensorflow: A system for large-scale machine learning. Proceedings of 12th USENIX Symposium on Operating Systems Design and Implementation is sponsored by USENIX, Savannah, 2 – 4 November 2016, p. 265–283.
26. *Paszke A., Gross S., Massa F.* et al. PyTorch: An Imperative Style, High-Performance Deep Learning Library. Advances in Neural Information Processing Systems, 2019, no. 32, p. 8024–8035.
27. *Chi-Kwong C., Cheng L.M.* The convergence properties of a clipped Hopfield network and its application in the design of key stream generator. IEEE Transactions on Neural Networks. 2001, no. 12, p. 340–348.
28. *Wang, Y., Wang, G., Zhang, H.* (2010). Random Number Generator Based on Hopfield Neural Network and SHA-2 (512). In: Luo, Q. (eds) Advancing Computing, Communication, Control and Management. Lecture Notes in Electrical Engineering, vol. 56. Springer, Berlin, Heidelberg. p. 198–205.
29. *Desai V.V., Deshmukh V.B., Rao D.H.* Pseudo Random Number Generator Using Elman. Proceedings of 2011 IEEE Recent Advances in Intelligent Computational Systems, Trivandrum, 22-24 September 2011, p. 251–254.
30. Sutton, R.; Barto, A. Reinforcement Learning: An Introduction. IEEE Transactions on Neural Networks, vol. 9, no. 5, p. 1054–1054, Sept. 1998.
31. *L'Ecuyer P., Simard R.* TestU01: A C library for empirical testing of random number generators. ACM Transactions on Mathematical Software. 2007, vol. 33, no. 4, p. 22–40.
32. *Rukhin A., Soto J., Nechvatal J.* et. al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22, 2010.
37. *Kadhim M.H., Wijdan R.A.* Binary Sequences Randomness Test Using Neural Networks. International Journal of Computer Science and Mobile Computing. 2015, vol. 4, p. 246–258.
38. *Pol Yee L., De Silva L. C.* Application of MultiLayer Perceptron Network as a one-way hash function. Proceedings of "2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290)", Hawaii, 12 – 17 May 2002, p. 1459–1462.
39. *Anderson J. A., Rosenfeld, E.* Neurocomputing: Foundations of research. Cambridge, USA, The MIT Press, 1988. – 685 p.
40. *Desai V., Patil R., Rao D.* Using Layer Recurrent Neural Network to Generate Pseudo Random Number Sequences. International Journal of

Computational Science Issues. 2012, vol. 9, p. 324–334.
41. *Pasqualini L., Parton M.* Pseudo Random Number Generation: a Reinforcement Learning approach. Procedia
Computer Science. 2020, vol. 170, p. 1122–1127.

References (transliterated)

1.*Apdullah Y., Yakup K.* Neural Network Based Cryptography. Neural Network World. 2014, no. 24, p. 177–192.
2. *Kannan M.R. Gnanam V.* Neural network based decryption for random encryption algorithms. Proceedings of 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, Hong Kong, 20-22 August 2009, p. 603–605.
3. *Oak R., Rahalkar C., Dhaval G.* Using Generative Adversarial Networks for Secure Pseudorandom Number
Generation. Proceedings of 2019 ACM SIGSAC Conference, London, 11–15 November 2019, p. 2597–2599.
4. *İnce K.* Security Analysis of Java SecureRandom Library. Avrupa Bilim ve Teknoloji Dergisi. 2021, no. 24,
p. 157–160.
5. *Lauria F.E.* On Neurocryptology. Proceedings of the Third Italian Workshop on Parallel Architectures and Neural Networks. Salerno, 15-18 May, 1990. p. 337–343.
6. *Pointcheval D.* Neural networks and their cryptographic applications. Livre des resumes Eurocode Institute for Research in Computer Science and Automation. 1994. p. 1–7.
7. *Schneider B.* Applied Cryptography. Protocols, Algorithms, and Source codes in C. New York, Wiley, 1996. – 758 p.
8. *Luciano D., Prichett G.* Cryptology: From Caesar Ciphers to Public-key Cryptosystems. The College Mathematics Journal. 1987, no. 18(1), p. 2–17.
9. *Godhavari T., Alainelu N.R., Soundararajan R.* Cryptography using neural network. IEEE INDICON 2005 Conf., Chennai, India; 11-13 December 2005, p. 258–261.
10. *Arvandi M., Wu S., Sadeghian A., Melek W.W., Woungang I.* Symmetric Cipher Design Using Recurrent
Neural Networks. The 2006 IEEE International Joint Conference on Neural Network Proceedings, Vancouver,
BC, Canada, 2006, p. 2039–2046.
11. *Guo D., Cheng L.-M., Cheng L. L.* A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks. Applied Intelligence. 1999, no. 10(1), p. 71–84.
12. *Noughabi A. M. N., Sadeghiyan B.* Design of S-boxes based on neural networks. Proceedings of "International Conference on Electronics and Information Engineering", Kyoto, 1-3 August 2010, p. 172–178.
13. *Karras D. A. Zorkadis V.* On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators. Neural networks: the official journal of the International Neural Network Society. 2003, no. 16(5-6), p. 899–905.
14. *Ruttor A*. Neural Synchronization and Cryptography. PhD thesis. Bayerischen Julius-Maximilians-Universitat at Wurzburg. 2006.
15. *Sadırodlu S., Ozkaya N.* Neural Solutions for Information Security. Journal of Polytechnic. 2007, vol. 10, no. 1, p. 21–25.
16. *Blum L., Blum M., Shub M.* A simple unpredictable pseudo random number generator. SIAM Journal on Computing. 1986, vol. 15, no. 2, p. 364–383.
17. *Matsumoto M., Nishimura T.* Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Transactions on Modelling and Computer Simulation. 1998, vol. 8, no. 1, p. 3–30.
18. *Abdi H.* A neural network primer. Journal of Biological Systems. 1994, vol. 2, no. 3, p. 247–281.
19. *Eastlake D.E., Jones P.E.* US Secure Hash Algorithm 1 (SHA1). Request for Comments. 2001, no. 3174, p. 1–22.
20. *Fausett V.L.* Fundamentals of neural networks: architectures, algorithms, and applications. Pearson, USA, 1994. – 480 p.
21. *McCulloch W.S., Pitts W.* A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics. 2003, no. 5(4), p.115–133.
22. *Gurney K.* An Introduction to Neural Networks (1st ed.). London: CRC Press, 1997. – 234 p.
23. *Vrahatis M., Magoulas G., Parsopoulos K., Plagianakos V.* Introduction to artificial neural network training and applications. Proceedings of 15th Annual Conference of Hellenic Society for Neuroscience, Greece,
27 – 29 October 2000, p. 1–14.

24. *Kingma D.P., Ba J.* Adam: A method for stochastic optimization. Proceedings of International Conference on
Learning Representations (ICLR), San Diego, 7 – 9 May 2015, p. 1–13.
25. *Abadi M., Barham P., Chen J.* Tensorflow: A system for large-scale machine learning. Proceedings of 12th USENIX Symposium on Operating Systems Design and Implementation is sponsored by USENIX, Savannah, 2 – 4 November 2016, p. 265–283.
26. *Paszke A., Gross S., Massa F.* et al. PyTorch: An Imperative Style, High-Performance Deep Learning Library. Advances in Neural Information Processing Systems, 2019, no. 32, p. 8024–8035.
27. *Chi-Kwong C., Cheng L.M.* The convergence properties of a clipped Hopfield network and its application in the design of key stream generator. IEEE Transactions on Neural Networks. 2001, no. 12, p. 340–348.
28. *Wang, Y., Wang, G., Zhang, H.* (2010). Random Number Generator Based on Hopfield Neural Network and SHA-2 (512). In: Luo, Q. (eds) Advancing Computing, Communication, Control and Management. Lecture Notes in Electrical Engineering, vol. 56. Springer, Berlin, Heidelberg. p. 198–205.
29. *Desai V.V., Deshmukh V.B., Rao D.H.* Pseudo Random Number Generator Using Elman.
Proceedings of 2011