APPLICATION OF NEURAL NETWORKS IN ENCRYPTION

Davlatov Mirzo-Ulugbek
mirzoulugbekdavlatov@gmail.com ,
TUIT named after Muhammad al-Khwarizmi

Abstract. *Cryptography plays a key role in ensuring authentication, integrity, confidentiality and secure storage of personal data transmitted over open networks. With the development of computing technologies and their increase in speed, outdated ciphers are replaced by more modern and adaptive solutions. This article discusses the use of new neural network methods for data encryption.*

Key words *: neural networks, encryption, information security; engineering and technical information protection.*

With the development of encryption methods [1], the role of mathematics in cryptography has increased significantly. It is the mathematical principles that have allowed cryptography to reach a level where the number of computational operations in modern ciphers has become astronomically large. This has led to the fact that modern cryptographic algorithms have high resistance to cryptanalysis, unlike outdated methods that could be cracked with a pen and paper. Classical cryptanalysis is no longer able to effectively cope with the cracking of modern ciphers.

In this regard, attack methods based on data interception, the use of spy devices, side-channel attacks, the use of quantum computers and bandit cryptanalysis are becoming increasingly important.

A side-channel attack *is* a class of attacks that target vulnerabilities in the practical implementation of cryptosystems. They exploit the shortcomings of the physical implementation of algorithms. Since even the most complex cryptographic algorithm is ultimately implemented by software code and executed by a processor with a specific architecture, it inevitably has characteristic features that can be exploited by attackers.

"Classical" cryptanalysis looks at encryption algorithms purely from a mathematical point of view, based on their algebraic properties, which may depend on key parameters.

In contrast, side-channel cryptanalysis takes into account parameters such as execution time, power consumption, electromagnetic radiation, acoustic signals, and other factors. Although such attacks are less universal, since they depend on the specific hardware device on which the encryption is performed, they are significantly more effective. In practice, most successful attacks are associated with vulnerabilities in the implementation of cryptographic primitives.

Known types of attacks:

1. **A probing attack** is a simple, invasive attack in which the device is opened and then probes are placed on the processor contacts or the memory cells are examined using a microscope.
2. **Error-based computation attacks** – are based on deliberately influencing the device to cause errors. By analyzing distortions at different stages of the system's operation, it is possible to obtain information that allows one to determine the secret key.
3. **Power consumption attacks** are a passive attack that measures the power consumed by a device. Based on changes in power consumption, information about the operations performed and their parameters can be extracted. This is done by installing a resistor in the power supply circuit and measuring the current passing through it.
4. **Electromagnetic radiation attacks** – electronic devices emit electromagnetic waves during operation. Spectral analysis of the radiation allows us to determine the correspondence of certain signals to specific operations, which can reveal information about the operation of the algorithm.

Research shows that the DES and AES algorithms are particularly vulnerable to side-channel attacks, with some requiring as little as 1.5 seconds or 15 measurements to successfully complete.

Neural networks, as their name suggests, are systems made up of interconnected neurons. Each neuron performs calculations on input data and passes the results to the next layer of the network.

One of the key features of neural networks is their ability to approximate any function, including cryptographic algorithms. By modeling existing algorithms such as DES or AES using neural networks, their resistance to side-channel attacks can be significantly increased.

The general view of the neural network is shown in Fig. 1.

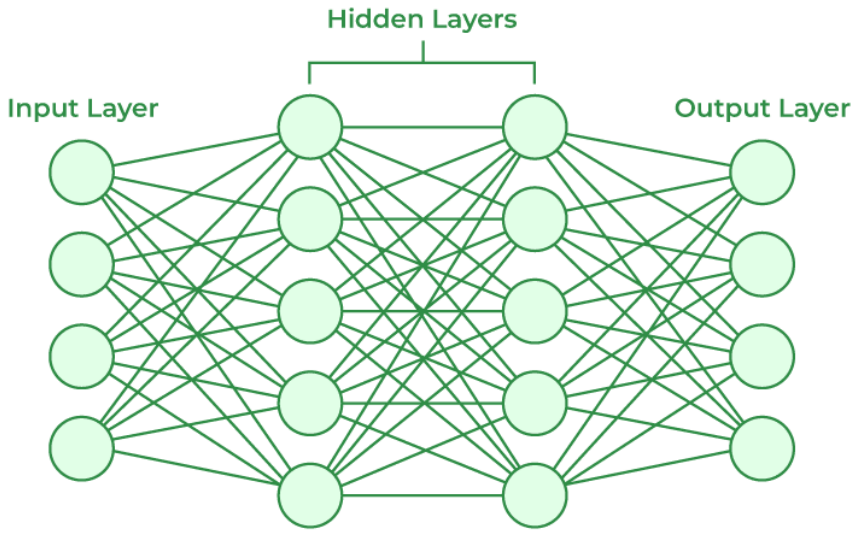

Fig. 1. General view of the neural network

This structure significantly increases security against side-channel attacks because:

1. **Distribution of information** – each neuron contains only a small part of the data necessary for the algorithm to work correctly. This forces the cryptanalyst to analyze all possible memory cells, which significantly complicates the attack.
2. **Independence of computations** - operations in each neuron are performed independently of the input data, so the running time of the neural network depends only on its architecture, and not on the specific encrypted message.
3. **Hiding the key and algorithm** – the weights of the neural network do not allow the secret key to be directly recovered, and in some cases even the encryption algorithm itself remains inaccessible for analysis.

All these properties make neural networks a reliable tool for protecting against side-channel attacks, making it much more difficult for attackers to extract key information.

REFERENCES:

1. Elements of large orders in linear groups and modification of the El-Gamal system. URL: http://www.info-secur.ru/is_15/Zulyarkina.htm
2. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020.
3. Koblitz N. A Course in Number Theory and Cryptography. – Springer, 1994.
4. Menezes AJ, van Oorschot PC, Vanstone SA Handbook of Applied Cryptography. – CRC Press, 1996.
5. Katz J., Lindell Y. Introduction to Modern Cryptography. – CRC Press, 2020.
6. Bishop M. Computer Security: Art and Science. – Addison-Wesley, 2018.