International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 3, pp 111-114, March-2023

https://doi.org/10.47001/IRJIET/2023.703016

Review "Improving the Cryptanalysis of Block Cipher Using Artificial Intelligence Algorithms"

[1]Raghad Layth Malallah, [2]Auday Hashem Al Wattar

[1]Computer Science Department, College of Computer and Mathematics & Mosul University, Iraq
[2]Second Professor, Cyber Security Department, College of Computer and Mathematics &, Mosul University, Iraq

***Abstract* - Nowadays, it is important to deliver information in a safe and confidential manner to specific individuals or entities. As the best way for the defense is to attack, therefore, cryptanalysis study is important to highlight any weakness of any security algorithm. Usually, attackers or any third-party tries to intercept to do any malicious actions that might cause problems. Bluefish encryption is one of the main methods of protection, which is a 64-bit Feistel network process. The objective of this review paper is to find out in the literature the possible cryptanalysis methods that applied to bluefish encryption. Where, the analyst tries to analyze the ciphers of a particular encryption algorithm by using many traditional methods. Thus, in this paper, review will be dedicated for try to analyze the ciphers using artificial intelligence on symmetric encryption algorithms, such as Blowfish. This approach to cryptanalysis may be more efficient than traditional methods in terms of accuracy, speed, and memory usage.**

Keywords: Bluefish, Cryptanalysis, Information Security, Artificial Intelligent, Deep Learning.

I. INTRODUCTION

Cryptology is divided into two parts: cryptography and cryptanalysis [1]. Since what is meant by encryption is scrambling and destroying the original data in order to not to be known of foreseen and predicted. In fact, it focuses on creating secure encryption methods and algorithms. While cryptanalysis focuses on the study of methods for cracking or reforming ciphers to its original plaint-text, which is an ideal system for problem identification [1]. The traditional algorithm-based cryptanalysis can classify algebraic structures with block ciphers into several types, including: Differential cryptanalysis is the first general cryptanalysis technique introduced specifically for block ciphers [2]. The main idea is to exploit cryptographic properties, where correlations between input-output differences of a non-optimal block cipher are used to recover the key, usually through a chosen plaintext attack. Normally, each of cryptanalysis method may require some amount of time and memory or may have generalizability limitations or impractical. Therefore, the combination of artificial intelligence and especially machine learning (ML) with cryptanalysis takes a different trend. For instance, it speeds up the cryptanalysis process with minimal cost. It is also could be found differential properties with high probability paths [3] in domain classification and regression. Therefore, this paper is dedicated to listing the works which are describing the cryptanalysis operations based on artificial intelligence. We will specialize in regression because it is possible to propose a model that predicts plaintext using known plaintext attack or it is possible to predict the key. Building a model for cryptographic analysis of a particular cipher algorithm may be the Blowfish algorithm (as a case study) which is one of the symmetric encryption algorithms as it is a 64-bit block cipher (Feistel network) with a variable key length of 32-448 bits [4].

The organization of the paper is as following, in section Two, related work of this review paper will be listed, then in Section 3 the possible result and discussion will be presented and then finally, a conclusion will be reported.

II. RELATED WORK

The idea of a relationship between cryptography and machine learning emerged at 1990s[5]. It is noticed from the literature that machine learning and cryptanalysis as "sister fields" and could be hybrid, because they share many concepts and interests. In typical cryptanalysis, the analyst likes to break one of the cipher systems. This means that he wants to know the secret key, which is the same one used by the users of the cipher system. The cipher system is already known (as in the public existing) and thus the concept of decoding comes from a well-known family[6]. While the cryptanalyst tries to identify the unknown function (this means the decryption function) [7]. Machine learning has proven successful in many applications and in a wide range of field [6]. Among these extensive works is cryptanalysis, as researchers and developers have proven this. Where Alani worked crypt analysis As in 2012 in [8], a cryptanalysis attempt has been implement as an attack by using the known plaintext type. Here the method was used is a neural network on the encryption algorithm DES and 3DES, and he obtained the other plaintexts from the trained neural network without knowing the secret key used in the encryption operation. Also, in2013 [9], it has been proposed a model for cryptanalysis based on neural networks and used the cipher text as input to the network and the plaintext as the output, where the output is compared to the actual plaintext. The network has been trained to obtain a model and performance error indicators have been established. Also, in this work [10], a known plaintext attack was implemented on the a DES algorithm, which managed to prepare with a rudder of more than 40% and half of the entire bytes with accuracy more than 63%.The following Table 1 shows some research papers that are discussing the same or similar cryptanalysis work.

Source Number	The year	Method	The Work and Result
[11]	2010	Research on plaintext restoration of EDS base on neural network.	▪ Feed forward BP neural network and the cascade feed forward BP neural network were used to perform cryptanalysis on AES for plaintext recovery . ▪ To restore the cipher texts of the AES- 128 and AES-256 algorithms in ECB and CBC modes. ▪ The results showed that the neural network can recover the entire byte with a probability of more than 40%and the number of bytes in more than half is 89%.
[8]	2012	Neuro-Cryptanalysis of DES and Triple-DES	▪ A neural model was created that retrieves the plaintext without the need to retrieve the key used for encryption. ▪ The analytics attack is applied to DES and Triple-DES. The attack type is known-plaintext attack based on neural networks. ▪ This attack required an average of 211 plaintext-cipher text pairs to perform cryptanalysis of DES in an average duration of 51 minutes. ▪ For the cryptanalysis of Triple-DES, an average of only 212 plaintext-cipher text pairs was required in an average duration of 72 minutes. ▪ The attack was practical and successful compared to other attacks. ▪ This attack is an improvement in terms of the number of known-plaintexts required as well as the time required to perform the full attack.
[9]	2013	Artificial Neural Networks for Cryptanalysis of DES	▪ Develop neural network-based simulators using plaintext methods and known cipher texts, then decrypt cipher texts using the DES encryption algorithm. ▪ The back propagation neural network has been exploited for solving cryptanalysis problem. ▪ Over 90% of fitting rate are compared with the plaintext in the experiment.
[12]	2014	Improved Cryptanalysis Combining Differential and Artificial Neural Network Schemes	▪ Improved security of algorithms for Differential Cryptanalysis (DC) by developing a new S-Box for S-DES. ▪ MLB is used to attack Multilayer Perceptron (MLP). We found that the neural network was still able to find some correlations between key bits. ▪ A correlation between neural cryptanalysis and key-based DC is established here.
[10]	2020	Research on plaintext Restoration Of Blowfish Based on Neural Network	▪ A model was designed that attempts to recover the plaintext of the blowfish algorithm. ▪ The result is that the neural network simulator can fit data with an error rate of less than 0.04 when the data sum size exceeds 2^19 .

[5]	2020	Deep Learning (DL) based of Lightweight Block Cipher.	▪ From a set of plaintext-cipher text pairs, the DL model seeks to identify the key used for block ciphers. ▪ Restricted to 64 ASCII characters, this particular concept has the ability to retrieve the essential components. ▪ With a success probability of 0.9, the S-DES cipher was breached by a DL-based attack, assuming 2^8.08 plaintexts were already known. ▪ The DL-based cryptanalysis can reveal linear approximations relating the plaintext-cipher text pairs to the given key when utilizing block ciphers along with text keys. ▪ Successfully breaking entire rounds of Simon 32/64 and Speck32/64 resulted in the achievement.
[13]	2020	Optimized deep neural network for cryptanalysis of DES	▪ The symmetric encryption algorithm, DES, is subjected to analysis using an innovated neural network model. Utilizing Back propagation technique with activation function and multiple hidden layers yields the desired results. ▪ The problem of vanishing gradient has been tackled in this setting. ▪ Compared to previous techniques, the accuracy attained of 90% was deemed rather impressive.
[14]	2021	Differential-ML Distinguisher: Machine Learning based Generic Extension for Differential Cryptanalysis	▪ Reported is a framework for extending the classical differential discriminator, utilizing a machine learning-based approach. ▪ For distinguishing 9-round and 12-round SIMON SPECKs, the success rate was reported to be 95% and 98% respectively using this method. The technique was tested on SPECK & SIMON lightweight block zeros. ▪ Using an 8-round binary ML discriminant, GIFT64 can achieve an accuracy of up to 99%. ▪ In terms of data complexity and the number of rounds, this approach proved to be superior.
[15]	2022	Output Prediction Attacks on Block Ciphers Using Deep Learning	▪ The method here is predicting output attacks based on deep learning on three zeros with 64-bit block size in a black box. ▪ To look deeper into deep learning specific characteristics that output prediction attacks using deep learning will make it easier to estimate the resistance to differential and linear attacks, even without possessing knowledge about the target cryptographic algorithm or cryptanalysis methods.
[16]	2021	Improve Neural Distinguisher for Cryptanalysis	▪ Improve performance by finding compatible domain knowledge of differentially encoded analysis structures and other differential properties with high probability during deep learning training, taking into account the integrity of the cipher text's information to the training data. ▪ Neural discriminators (NDs) and related key neural discriminators (RKNDs) are built for Simon and Simeck. ▪ For Simeck32/64, ND and RKND are obtained from rounds 11 and 14, achieving 63.32% and 87.06% accuracy, respectively. ▪ In addition, 17-round ND and 21-round RKND were constructed for Simeck64/128 with accuracy rates of 64.24% and 62.96%, respectively.

III. CONCLUSION

In this paper, recent publications including pre-recent ones have been reviewed. It is noticed form the literature that neural networks are highly used to perform cryptanalysis on block ciphers for more than one type of attack, as well as focused mostly on the known script attack. It turns out, it might be gotten some advantages, facilities, and accurate results from this method compared to traditional cryptanalysis. The use of neural networks is much better. It is also shown that difficult obtaining a complete encryption crack. However, certain relationship between the cipher text and the plaintext using artificial intelligence could be predicted. In which this relationship helps researchers or other attackers to reduce the possible ways to analyze the codes and reach the target.

REFERENCES

[1] Ali, F.H., M.G. Al-Safi, and A.A.J.A.-N.J.o.S. Yousif, Analyzing Cryptosystems by Using Artificial Intelligence. 2018(1): p. 100-108.

[2] Avanzi, R.J.I., Lyon, France, A Salad of Block Ciphers The State of the Art in Block Ciphers and their Analysis. 2017.

[3] Fu, K., et al. MILP-based automatic search algorithms for differential and linear trails for speck. in Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers 23. 2016. Springer.

[4] Asassfeh, M.R., et al., Performance evaluation of blowfish algorithm on supercomputer iman1. 2018. 10(2).

[5] So, J.J.S. and C. Networks, Deep learning-based cryptanalysis of lightweight block ciphers. 2020. 2020: p. 1-11.

[6] LeCun, Y., Y. Bengio, and G.J.n. Hinton, Deep learning. 2015. 521(7553): p. 436-444.

[7] Rivest, R.L. Cryptography and machine learning. in ASIACRYPT. 1991.

[8] Alani, M.M. Neuro-cryptanalysis of DES and triple-DES. in Neural Information Processing: 19th International Conference, ICONIP 2012, Doha, Qatar, November 12-15, 2012, Proceedings, Part V 19. 2012. Springer.

[9] Akiwate, B., V.J.I.J.o.I.i.E. Desai, and Technology, Artificial neural networks for cryptanalysis of DES. 2013. 2(4): p. 11-17.

[10] Zhang, W. and Y. Zhao. Research on Plaintext Restoration of Blowfish Based on Neural Network. in 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT). 2020. IEEE.

[11] Hu, X., Y.J.S. Zhao, and C. Networks, Research on plaintext restoration of AES based on neural network. 2018. 2018: p. 1-9.

[12] Danziger, M. and M.A.A. Henriques. Improved cryptanalysis combining differential and artificial neural network schemes. in 2014 International Telecommunications Symposium (ITS). 2014. IEEE.

[13] Mundra, A., et al., Optimized deep neural network for cryptanalysis of DES. 2020. 38(5): p. 5921-5931.

[14] Yadav, T. and M. Kumar. Differential-ml distinguisher: Machine learning based generic extension for differential cryptanalysis. in Progress in Cryptology–LATINCRYPT 2021: 7th International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, October 6–8, 2021, Proceedings. 2021. Springer.

[15] Kimura, H., et al. Output Prediction Attacks on Block Ciphers Using Deep Learning. in Applied Cryptography and Network Security Workshops: ACNS 2022 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Rome, Italy, June 20–23, 2022, Proceedings. 2022. Springer.

[16] Hou, Z., J. Ren, and S.J.C.e.A. Chen, Improve neural distinguisher for cryptanalysis. 2021.

Citation of this Article:

Raghad Layth Malallah, Auday Hashem Al Wattar, “Review "Improving the Cryptanalysis of Block Cipher Using Artificial Intelligence Algorithms"” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 3, pp 111-114, March 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.703016

****