INTEGRAL CRYPTANALYSIS

Berdimurodov Mansur Alisherovich
Senior Lecturer, Department of Modern Information and Communication Technologies Uzbekistan International Islamic Academy
m.berdimurodov@iiau.uz
Xudoyqulov Kamoljon Toshpo'latovich
Lecturer, Department of Information Technologies
Denov Institute of Entrepreneurship and Pedagogy
kamoljontoshpulatovich@gmail.com

Abstract. This article analyzes the theoretical foundations and practical application of integral cryptanalysis - one of the important cryptanalysis methods used in symmetric cryptography. Integral cryptanalysis is based on the study of the internal structure of block ciphers, which allows determining the statistical properties of the cipher at several encryption stages. The article covers the origin, basic concepts, methodology, and effectiveness of integral cryptanalysis compared to modern block ciphers. Also, the practical aspects of integral cryptanalysis are considered using the example of the AES algorithm.

Keywords: integral cryptanalysis, block cipher, AES, symmetric cryptography, cryptanalysis methods, security.

Аннотация. В данной статье анализируются теоретические основы и практическое применение интегрального криптоанализа - одного из важных методов криптоанализа, используемых в симметричной криптографии. Интегральный криптоанализ основан на изучении внутренней структуры блочных шифров, что позволяет определить статистические свойства шифра на нескольких этапах шифрования. В статье рассматриваются происхождение, основные понятия, методология и эффективность интегрального

криптоанализа по сравнению с современными блочными шифрами. Также рассматриваются практические аспекты интегрального криптоанализа на примере алгоритма AES.

Ключевые слова: интегральный криптоанализ, блочный шифр, AES, симметричная криптография, методы криптоанализа, безопасность.

Introduction. In modern information systems, data protection is one of the important issues. In solving this problem, symmetric cryptographic algorithms, in particular block ciphers, are widely used. However, assessing the security of cryptographic algorithms requires not only their development, but also verification using various cryptanalysis methods[1].

Integral cryptanalysis is one of the relatively powerful statistical methods used in the analysis of block ciphers, based on the aggregate properties of certain bits or bytes at the internal stages of the cipher. The purpose of this article is to reveal the theoretical foundations of integral cryptanalysis and analyze its application to modern block ciphers.

Integral cryptanalysis was first formed in the late 1990s as a result of research aimed at assessing the security of block ciphers. The emergence of this method is mainly associated with the name of the Danish cryptographer Lars Ramkilde Knudsen, who in 1997 proposed an attack called "Square attack" and successfully applied it to the early versions of the Rijndael (later AES) algorithm. Later, this idea was expanded and formed as an independent method of cryptanalysis under the name of integral cryptanalysis. In this direction, leading researchers such as Joan Daemen and Vincent Rijmen (authors of AES), Alex Biryukov, Andrey Bogdanov, Orr Dunkelman, and Nathan Keller deeply analyzed integral properties and effectively applied them to modern block ciphers such as Camellia, PRESENT, and others. As a result, integral cryptanalysis is recognized today as an important scientific tool for assessing the strength of symmetric cryptographic algorithms[2-4].

Literature Review

Integral cryptanalysis was first proposed in 1997 by L. Knudsen under the name "Square attack" and was initially used against the initial versions of the AES algorithm. Later, this method was generalized and became known as "integral cryptanalysis."

In the scientific literature, integral cryptanalysis, along with differential and linear cryptanalysis, is considered one of the main methods of analyzing block ciphers. In a number of studies, AES, Camellia, PRESENT, and other ciphers were analyzed based on integral properties. In these works, it is noted that integral cryptanalysis is often effective for limited stages, but for full-stage ciphers, more complex forms are required[5,6].

Main Part

The main idea of integral cryptanalysis is to change a certain part of the input data by all possible values and leave the remaining part unchanged. As a result, at a certain stage of the encryption process, it is observed that the sum of some output bits or bytes (for example, the sum of XOR) is equal to zero or has a certain pattern.

The following concepts are important in integral cryptanalysis:

- **Active and inactive bytes** - variable and constant values;
- **Balanced state** - the sum of the output values is equal to zero;
- **Integral property** - a statistical property that persists at the internal stages of the cipher.

Results and Analysis

Integral cryptanalysis for the AES block cipher was initially more effective than 3-4-step options. For example, it has been established that when one byte in the input block accepts all 256 values, after a certain step, the XOR sum of the output bytes becomes zero.

Studies show that, although integral cryptanalysis cannot directly disrupt full 10-14 step versions of the NPP algorithm, it provides important analytical results for

shortened stages. This plays an important role in assessing the strength of the algorithm design[7].

Steps for Performing Integral Cryptanalysis

Step 1. Definition of the Objective

Integral cryptanalysis does not focus on a single plaintext, but rather on a carefully constructed set of plaintexts, referred to as an *integral*. The main objective is to identify statistical properties that emerge when certain bits or bytes of the input vary over all possible values, while the remaining parts are kept constant. The most commonly observed property is a balanced condition, where the XOR sum of selected output values equals zero.

Step 2. Analysis of the Cipher Structure

At this stage, the internal structure of the target block cipher is examined, including the size of the block, the number of rounds, and the operations performed in each round. Particular attention is given to key addition (XOR with round keys), substitution layers (S-boxes), and diffusion mechanisms, as these components determine how integral properties propagate through the cipher.

S-box:

x	S(x)	x	S(x)
0	E	8	3
1	4	9	A
2	D	A	6
3	1	B	C
4	2	C	5
5	F	D	9
6	B	E	0
7	8	F	7

Step 3. Construction of the Plaintext Set

A plaintext set is generated by varying one or more bytes of the input across all possible values, while fixing the remaining bytes. For example, varying a single byte from 0x00 to 0xFF produces a set of 256 plaintexts, known as a *full integral*. This construction ensures that each possible value appears exactly once in the active byte position.

Step 4. Propagation Through the Initial Rounds

$$X = P \oplus K_1$$

The plaintext set is encrypted through the initial rounds of the cipher. Due to the XOR operation used in key addition, the integral property is preserved after the key-mixing stage. Since S-boxes are typically bijective, the balanced property remains intact after the substitution layer as well. $\oplus_{x=0}^{255} S(x) = 0$.

Step 5. Diffusion and Observation of Integral Properties

As the encryption progresses through subsequent rounds, diffusion mechanisms distribute the influence of active bytes across the state. During this phase, the cryptanalyst observes whether the balanced condition is maintained in specific intermediate bytes or words. The persistence of this property indicates a structural characteristic of the cipher.

Step 6. Detection of the Limiting Round

The encryption is analyzed round by round to determine the maximum number of rounds for which the integral property holds. If the balanced condition is preserved up to a certain round but disappears afterward, the effective range of the integral cryptanalysis is established $\bigoplus_{i=0}^{255} C_i = 0$.

Step 7. Key Recovery Phase

In the final step, partial key information is extracted by working backward from the last round where the integral property is expected to hold. Key guesses are made for selected subkey bits, the inverse S-box is applied, and the XOR sum of the

resulting values is evaluated. If the balanced condition is satisfied, the key guess is considered correct; otherwise, it is discarded $\sum S^{-1}(C \oplus k_{guess}) = 0$.

Integral cryptanalysis is mainly effective in relation to block ciphers with a substitution-permutation structure, which is based on the analysis of the equilibrium properties between active and passive bytes in the input state based on selected plaintext. This method gives especially high results in the case of reduced cipher rounds, since with an increase in the number of rounds, the integral balances are disrupted. In algorithms with bijective S-blocks and linear diffusion mechanisms, the integral properties are preserved for several rounds, which allows for the detection of key bits or partial keys. At the same time, integral cryptanalysis is more effective in the presence of a large volume of selected plaintext, which has important theoretical significance not in relation to full-round variants of modern block ciphers, but in assessing their security limits[8].

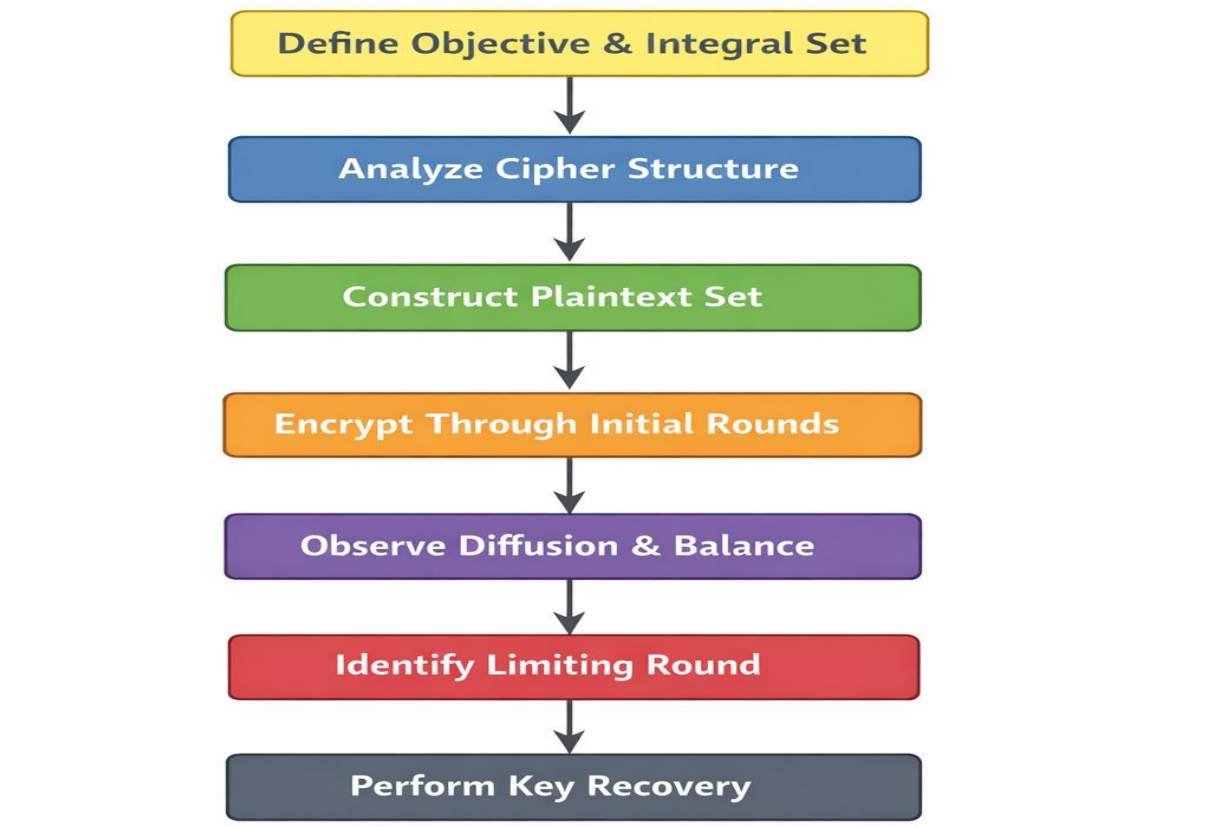

Figure 1. General scheme of integral cryptanalysis

Conclusion

This article thoroughly examines the theoretical foundations of integral cryptanalysis, the history of its formation, and its practical significance in the analysis of block ciphers. The research results showed that integral cryptanalysis allows determining the equilibrium states in the internal structure of the cipher based on the statistical properties of the set of input data. Especially in the case of simplified encryption models and shortened block ciphers, the preservation of integral properties confirms the effectiveness of this method. It is also substantiated that integral cryptanalysis serves as an important tool for identifying weaknesses in the design of algorithms, and in modern full-stage ciphers, it is necessary to use it in combination with other methods, such as differential and linear cryptanalysis. The obtained results show that integral cryptanalysis can be considered as an important scientific direction in assessing the cryptographic strength of symmetric cryptographic algorithms.

List of references

1. Knudsen L. R. *Truncated and Higher Order Differentials*. Fast Software Encryption, 1995.

2. Daemen J., Rijmen V. *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer, 2002.

3. Bogdanov A. et al. *Integral Cryptanalysis*. Advances in Cryptology – CRYPTO, 2011.

4. Urunbaev, E., Baizhumanov, A., and Berdimurodov, M., “Implementation of the algorithm for constructing a corrector of multivalued logic functions,” Proceedings of the 2022 International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2022, pp. 1–5.

5. Rakhimberdiev, K., Bozorov, A., and Berdimurodov, M., “Round Key Generation Algorithm Used in Symmetric Block Encryption Algorithms to Ensure

the Security of Economic Systems," Proceedings of the 7th International Conference on Future Networks and Distributed Systems, 2023, pp. 548–554.

6. Kabulov, A., Baizhumanov, A., Saymanov, I., and Berdimurodov, M., "Effective methods for solving systems of nonlinear equations of the algebra of logic based on disjunctions of complex conjunctions," Proceedings of the 2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA), IEEE, 2022, pp. 95–99.

7. Kabulov, A., Urunbaev, E., and Berdimurodov, M., "A logical method for finding maximum compatible subsystems of systems of Boolean equations," Scientific Journal of Samarkand University, vol. 2020, no. 3, pp. 27–37, 2020.

8. Kabulov, A. V., Berdimurodov, M. A., and Saymanov, I. M., "Logical Boolean function representation of cryptographic algorithm micro-operations (AES, ElGamal)," Scientific Journal, no. 3 (127/1), vol. 127, pp. 5–16, 2023.