International Journal on Optimization and Applications

IJOA. Vol. 4, Issue No. 2, Year 2024, http://www.ijoa.ma

Cryptanalysis of DES

1[st]Hanaa Hachimi

École Nationale des Sciences Appliquées, Kénitra, Morocoo

hanaa.hachimi@uit.ac.ma

2[nd] Sara Elmasoudy

École Nationale des Sciences Appliquées, Kénitra, Morocoo

sara.elmasoudy@uit.ac.ma

3[rd] Walid Benrqiq

École Nationale des Sciences Appliquées, Kénitra, Morocoo

walid.benrqiq@uit.ac.ma

Abstract—

This survey examines the evolution and current state of cryptanalysis techniques applied to the Data Encryption Standard (DES), providing an in-depth analysis of its enduring relevance in cryptographic research. Since its inception in 1977, DES has undergone extensive scrutiny, exposing several vulnerabilities and influencing the development of new cryptanalytic methodologies. The paper outlines the transition from brute force approaches to more sophisticated techniques such as differential and linear cryptanalysis, which were instrumental in advancing the field. The survey also discusses the impact of increasing computational power on the practicality of breaking DES and the consequent shift towards developing more secure cryptographic solutions. The objective is to provide a comprehensive overview of DES cryptanalysis, its implications for future cryptographic standards, and the continuous evolution of cryptanalysis techniques in addressing modern security challenges.

Keywords— Data Encryption Standard (DES), Differential Cryptanalysis, Linear Cryptanalysis, Cryptographic Research, Cryptanalysis Techniques, Cryptographic Vulnerabilities, Computational Power, Cryptographic Standards, Security Challenges.

I. INTRODUCTION

Cryptanalysis of the Data Encryption Standard (DES) remains a vibrant and crucial area of research in the field of cryptography, despite the algorithm's age and its replacement by more advanced encryption standards. Since its adoption by the U.S. government in 1977 as the official standard for securing sensitive information [1], DES has been the target of numerous cryptanalytic efforts. These efforts have not only exposed the vulnerabilities of DES but have also significantly influenced the development of cryptanalysis techniques and subsequent encryption standards. One straightforward approach to cryptanalysis is the brute force attack, which attempts to break an encryption by systematically trying every possible key until the correct one is found. Although effective, this method is highly resource-intensive and becomes impractical as the key size increases [20].

The seminal work by Biham and Shamir in 1991 introduced differential cryptanalysis, a sophisticated method that proved capable of breaking DES more efficiently than brute force attacks. This method marked a significant breakthrough in cryptanalytic techniques, demonstrating that it was possible to analyse the structure of DES and exploit its weaknesses more subtly and efficiently than by brute force alone [3]. Later, Matsui's introduction of linear cryptanalysis in 1993 provided another powerful tool against DES, demonstrating the algorithm's susceptibility to sophisticated analytical attacks beyond its designers' anticipations [2].

As computational power has increased, the practicality of breaking DES through brute force attacks has also become a reality, exemplified by the Electronic Frontier Foundation's successful crack in 1998 using a specially designed machine [5]. These developments have led to a consensus in the cryptographic community about the inadequacy of DES's 56-bit key size in the face of modern computing capabilities. Consequently, the focus of research has shifted towards enhancing cryptanalytic techniques and exploring new directions in cryptography that can offer secure alternatives to DES.

However, the analysis of DES remains relevant, providing valuable insights into the design and analysis of cryptographic algorithms. Recent advances in cryptanalysis, including advanced forms of differential and linear cryptanalysis, continue to draw lessons from the DES experience.

This survey article delves into the cryptanalysis of DES, exploring the techniques and discoveries that have shaped its journey. We begin by providing generalities and definitions related to cryptography, cryptosystems, cryptanalysis, and block ciphers. Then, we delve into the history, structure, advantages, and disadvantages of DES. Subsequently, we explore linear cryptanalysis, differential cryptanalysis, , and the fusion of both techniques known as differential-linear cryptanalysis, detailing their methodologies, advancements, and future perspectives. Finally, we explore algebraic *cryptanalysis, a field focusing on solving systems of polynomial equations to decrypt encrypted messages, and its relevance to DES.*

By examining these aspects, this paper aims to provide a comprehensive overview of the cryptanalysis of DES, highlighting its importance in the evolution of cryptographic techniques and the ongoing quest for robust, secure encryption standards in an era of advancing computational capabilities and cyber threats.

II. GENERALITIES AND DEFINITIONS

A. Cryptograph

Cryptography, a field merging computer security, and mathematics, focuses on safeguarding exchanges and data. By employing mathematical methods, it encodes and decodes information, ensuring that only authorized parties can access the original content of messages or data. This discipline ensures confidentiality, integrity, authenticity, and sometimes anonymity of data exchanged over potentially vulnerable networks like the Internet.

From [20], Cryptographic systems generally differ along three axes:

The operations used to transform plaintext into ciphertext: All encryption algorithms rely on two fundamental principles, substitution, and transposition. Substitution replaces each element of the plaintext with another element, while transposition reorganizes the elements of the plaintext. Most systems, known as product systems, combine multiple stages of substitutions and transpositions.

The number of keys used: A system is termed symmetric, single-key, secret-key, or conventional encryption when both the sender and receiver use the same encryption key. Conversely, a system is termed asymmetric, two-key, or public-key encryption when the sender and receiver use different encryption keys.

How plaintext is processed: Block encryption processes input in blocks of elements at a time, producing one output block for each input block. In contrast, stream encryption processes input elements continuously, generating output element by element as they are processed.

B. Cryptosystem

The article in [21] defines a cryptosystem as a sophisticated set of methods, techniques, and algorithms used in the field of cryptography to ensure the security of communications and data. It is a comprehensive system that encompasses various layers of protection and procedures aimed at ensuring the confidentiality, integrity, authenticity, and sometimes anonymity of the information exchanged between concerned parties. Within a cryptosystem, several key elements are typically at play. Firstly, encryption algorithms transform data into an unreadable and secure format, rendering its content inaccessible to unauthorized individuals. Subsequently, decryption algorithms reverse this process, allowing legitimate recipients to understand the encrypted data. Alongside encryption and decryption algorithms, cryptosystems often incorporate key management mechanisms, crucial for generating, distributing, and safeguarding the encryption keys utilized to lock and unlock data. Effective key management is paramount in ensuring the overall security of the system by thwarting attacks based on key compromise.

C. Cryptanalysis

Cryptanalysis is the study of techniques aimed at decrypting encrypted messages without having access to the corresponding encryption key. It involves analysing the characteristics of the encryption used and exploiting potential weaknesses to retrieve the plaintext.

According to the article written by William Stallings in [20], an attack is typically categorized based on the type of data it relies on:

Ciphertext-only attack: in this scenario, the cryptanalyst only possesses encrypted versions of messages, allowing them to speculate about the original content without direct access to it. This form of cryptanalysis poses greater difficulty due to the limited information available.

Known-plaintext attack: here, the cryptanalyst possesses both plaintext messages or fragments and their corresponding encrypted versions. Techniques like linear cryptanalysis fall under this category.

Chosen-plaintext attack: in this case, the cryptanalyst has access to plaintext messages and can generate their encrypted counterparts using the algorithm, treating it as a black box.

Chosen-ciphertext attack: in this attack, the cryptanalyst has encrypted messages and seeks the plaintext versions of some of these messages to carry out the attack.

D. Advancements in Cryptanalysis

Recent advancements in the field of cryptanalysis have been significant, underscoring the critical need for comprehensive security assessments of emerging cryptographic technologies. Researchers have been engaged in the complex challenge of breaking the Data Encryption Standard (DES) since its inception in the 1970s [1], a significant project undertaken by the National Institute of Standards and Technology (NIST). In response to the swift pace of technological advancement and heightened security requirements, NIST has introduced new benchmarks, such as the Advanced Encryption Standard (AES)[6].

The establishment of AES has led to the creation of innovative cryptographic systems, which require thorough testing to determine their resilience to advanced cryptanalytic attacks, including linear and differential cryptanalysis. These techniques are now essential tools for verifying the security Critical Vulnerabilities of the Data Encryption Standard [6].

The Data Encryption Standard (DES) encryption algorithm, although groundbreaking at its inception, possesses several vulnerabilities that render it susceptible to various types of attacks. One of its primary weaknesses lies in its small key size, consisting of only 56 bits. This limited key size makes DES vulnerable to brute force attacks, where attackers systematically test all possible keys until finding the correct one [1].

Additionally, weaknesses in DES's key schedule algorithm have been identified, potentially compromising the overall security of the encryption process. DES is susceptible to sophisticated cryptanalytic techniques such as differential and linear cryptanalysis [2][3].

These methods leverage the statistical properties of the algorithm to retrieve the encryption key more efficiently. A limiting characteristic of DES is its fixed block size of 64 bits, which can introduce vulnerabilities when encrypting large volumes of data or in specific modes of operation. These vulnerabilities collectively underscore the need for stronger encryption standards to withstand modern computing capabilities and evolving cyber threats.

E. Block cipher

Block cipher is a cryptographic technique used to secure data by dividing it into fixed-size blocks, and then applying a cipher algorithm to each block individually. In this process, the original data is transformed into encrypted data blocks, known as ciphertexts, which cannot be read without the appropriate decryption key. This method is widely employed to safeguard the confidentiality and integrity of data in various applications, including secure storage, data transmission over networks, and secure communications [20].

F. *Description of DES*

The Data Encryption Standard (DES) is a data encryption standard. It is a symmetric encryption algorithm used to secure electronic data by converting the data into an unreadable format known as ciphertext. This ciphertext can be decrypted to retrieve the original data. Therefore, DES is both a standard and an algorithm used to protect data confidentiality.

The Data Encryption Standard (DES) processes input data consisting of 64 bits and generates an output of the same size. It operates using a 64-bit secret key, although the effective key size is 56 bits. Typically, the key is represented as 64 bits [1], with 8 additional parity bits added to enhance its robustness. However, during encryption and decryption, only 56 of the 64 bits in the key are utilized.

The algorithm divides the message into blocks of bits, then processes them by subjecting them to substitutions, transpositions, and other mathematical operations to perform encryption. Using the same key, DES can also be used to decrypt the ciphertext and retrieve the original data.

G. *History of DES*

The origins of DES date back to 1972 when a study by the National Bureau of Standards (NBS) highlighted the need for a government standard to encrypt unclassified but sensitive information in the realm of US government computer security [1].

Around the same period, in 1972, engineer Mohamed Atalla established Atalla Corporation and engineered the pioneering hardware security module (HSM) named the "Atalla Box," commercially launched in 1973. This innovation safeguarded offline devices using a robust PIN generation mechanism, culminating in notable commercial success [23]. The banking and credit card sectors harbored concerns over Atalla potentially monopolizing the market, prompting the development of an international encryption standard. Atalla emerged as an early contender to IBM International Business Machines Corporation within the banking domain, and his influence was acknowledged by IBM personnel involved in shaping the DES standard [7]. Subsequently, the IBM 3624 integrated a comparable PIN verification framework akin to the original Atalla system [4].

On May 15, 1973, following consultations with the NSA National Security Agency, the NBS requested proposals for a cipher that would meet stringent design criteria. However, none of the submissions met the requirements. A second call for proposals was issued on August 27, 1974. This time, IBM submitted a candidate that was deemed acceptable a cipher developed between 1973 and 1974 based on Horst Feistel's earlier algorithm, known as the Lucifer cipher. The team at IBM responsible for the design and analysis of the cipher included Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith, and Bryant Tuckerm.

H. *Structure of DES*

The Data Encryption Standard (DES) was developed to provide a uniform and secure method for protecting sensitive commercial and unclassified information. This encryption system relies on the use of a single key for both encrypting and decrypting data

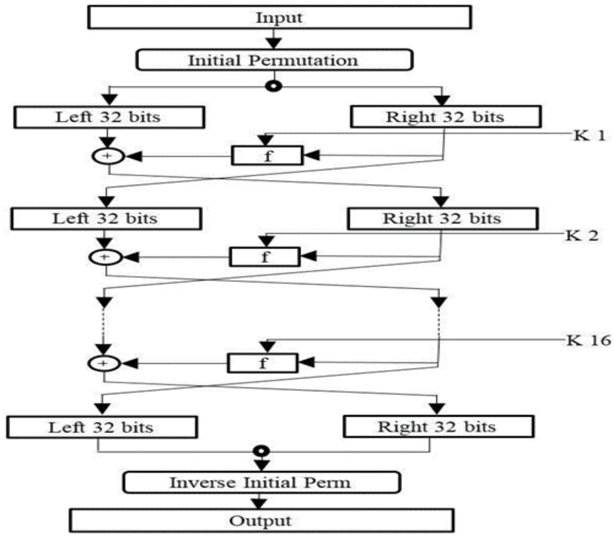

Fig 1 : Structure of DES

The figure (Fig 2) illustrates the encryption process employed by the Data Encryption Standard (DES) algorithm, as presented in the article "A Survey on the Cryptographic

Encryption Algorithm's authored by Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris.

The encryption process consists of several steps [1]:

- **Input and Initial Permutation:**

The encryption begins with a 64-bit plaintext input that is first subjected to an initial permutation. This step reorganizes the bits according to a predefined pattern to prepare the data block for the subsequent steps.

- **Splitting into Left and Right Blocks:**

The permuted data block is then divided into two equal parts: a left half and a right half, each consisting of 32 bits.

- **Encryption Rounds:**

The figure (fig 2) shows several rounds of encryption (16 in total), where each round uses a different key (K1, K2, ..., K16). These keys are derived from the main 56-bit key through a process of permutation and rotation.

Each round includes a complex encryption function (denoted as 'f'), which processes the right half of the data block and the corresponding round key. This function involves expanding the right half to 48 bits, performing an XOR operation with the round key, using substitution boxes (S-boxes) to perform bit substitutions, and applying a final permutation with a permutation box (P-box).

- **Combination and Final Permutation:**

After the final round, the two halves of the data are combined and undergo an inverse initial permutation to produce the final 64-bit encrypted output block.

I. Advantages of DES

Since [22], the following advantages of DES are cited:

Widely Accepted: DES was the first widely adopted encryption standard, leading to its widespread acceptance in industry and government applications.

Performance: It has relatively fast encryption speed and efficient implementation across a variety of hardware platforms.

Stability: Being a well-established algorithm, it has a long history of security and reliability in controlled environments.

J. Disadvantages of DES

According to [22], the drawbacks of DES mentioned are:

Key Size: The main weakness of DES is its small 56-bit key size, making brute-force attacks feasible with modern computing resources.

Vulnerabilities: Advanced attack techniques such as differential cryptanalysis and linear cryptanalysis have revealed vulnerabilities in DES, making its use risky in environments requiring maximum security.

Obsolescence: Due to its vulnerabilities and limited key size, DES is considered obsolete and not recommended for use in new systems or applications requiring robust security

III. Linear Cryptanalysis

Linear cryptanalysis is a widely used known-plaintext attack against block ciphers, particularly DES (Data Encryption Standard), invented by Mitsuru Matsui [32]. Its principle relies on the high probability of occurrence of linear expressions involving plaintext bits, ciphertext bits, and the key.

The main objective of linear cryptanalysis is to obtain an approximation of the block cipher using a linear expression. This linear expression takes the form:

$$\mathbf{X \oplus Y \oplus K = u \oplus v \oplus w}$$

Where X represents the plaintext bits, Y represents the ciphertext bits, and K represents the key bits. The indices u, v, and w denote fixed bit locations.

The linear probability bias, e, is defined as the difference between the observed probability (p) and the expected probability (1221). The higher this bias, the greater the efficiency of the linear expression.

If a linear expression satisfies the equation with a high probability bias, it means that the encryption used is not random enough [19]. A cipher is considered random if a randomly selected value of its linear expression bits would result in the expression being true with a probability of ½.

Once a linear approximation with the highest bias is obtained, the attack can be launched by recovering a subset of the key bits. This is done using Algorithm as described in [32].

To obtain a linear equation with a high probability bias, the process begins by constructing a statistical linear path between the input and output bits of each S-box. This path is then extended to the entire cipher to achieve a linear expression without any intermediate values [32].

Although S-boxes are generally nonlinear operations in block ciphers, it is possible to construct a linear approximation for them. Techniques for this purpose are described in [33].

Once a linear expression for the entire cipher is obtained, certain key bits can be deduced using Algorithm in [32].

In this field, various studies have been conducted to explore and understand the mechanisms and limitations of linear cryptanalysis. Matsui's work [32] laid the foundation for linear cryptanalysis and was followed by experimental attacks on DES, deepening our understanding of this method. Biham [29] formalized the method by demonstrating significant similarities between linear and differential cryptanalysis, paving the way for further research. Studies by Buttyan and Vajda [27] established a link between identifying relevant characteristics and determining the most significant paths in a directed graph. Daemen et al. [28] proposed using a correlation matrix as a representation tool to better understand the linear cryptanalysis process. Works by Harpes, Kramer, and Massey [30] attempted to generalize linear cryptanalysis concepts and assess their applicability to various encryption algorithms. Kaliski and Robshaw [31] explored the use of multiple linear approximations to enhance cryptanalysis performance in specific scenarios. Junod [38] conducted a practical implementation of linear cryptanalysis on DES, focusing on its efficiency under controlled experimental conditions. Subsequent advancements, such as the zero-correlation attacks introduced by Bogdanov and Rijmen [47, 48], expanded the possibilities of linear cryptanalysis. A further generalization of zero-correlation attacks, called attacks based on key-invariant biases, was presented in [49].

Regarding future perspectives, the article by [39] provides specific methods for evaluating mutual information in linear cryptanalysis, while [36] explores statistical cryptanalysis techniques to complement traditional linear approaches. Utilizing Reed-Muller techniques to identify linear approximations with lower biases, as discussed in [38], also opens avenues for more subtle cryptanalysis methods. Finally, a comprehensive analysis of the complexity of the Valembois algorithm, as outlined in [37], would enable a critical assessment of its strengths and weakness.

IV. Differential cryptanalysis,

Differential cryptanalysis, an advanced analytical technique, focuses on studying the impact of specific differences between pairs of plaintexts on the observed variations in the corresponding pairs of ciphertexts. This method proves particularly effective in estimating the probabilities associated with potential keys and determining the most likely key. It relies on the analysis of numerous pairs of plaintexts sharing a specific difference while limiting itself to the use of resulting pairs of ciphertexts. In the context of cryptosystems like the Data Encryption Standard (DES), this difference is typically defined as a fixed XOR value between two plaintexts [8]. To conduct effective differential cryptanalysis on DES, it is crucial to understand the non-linearity of this encryption system. Recognizing that DES is not a linear cipher, meaning that the difference between ciphertexts does not necessarily correspond to the difference between plaintexts. The analysis should begin with a thorough examination of the S-boxes, which are the non-linear components of DES and play a crucial role in creating confusion and diffusion within the encryption process [19]. By leveraging the understanding of DES's non-linearity, it is possible to identify specific differences between pairs of plaintexts that significantly influence the differences between pairs of ciphertexts [16]. These identified differential characteristics can then be extended to form complete sets of characteristics, a process that may require multiple iterations of analysis and extension [19]. The final step involves launching a differential attack using these extended sets of characteristics, aiming to reveal information about the encryption key by exploiting the differences between pairs of plaintexts and ciphertexts [19].

In the development of the Feistel cipher, C. Adams proposed a design method that ensures effective resistance to differential cryptanalysis with the implementation of at least five rounds [11]. Dawson and Tavares strengthened this resistance by designing S-boxes producing equiprobable XOR outputs, using bent functions to enhance security [12]. The groundbreaking work of Eli Biham and Adi Shamir in 1990 highlighted the effectiveness of differential cryptanalysis against a simplified version of DES [8]. Their subsequent research in 1991 revealed the vulnerability of various ciphers, including the two-pass Snefru, to this form of cryptanalysis. In 1992, their method was extended to analyse the complete 16 rounds of DES [9]. The concept of Markov ciphers, introduced by James Massey and Xuejia Lai, played a key role in defending iterated block ciphers against attacks of differential cryptanalysis [16]. The work of K. Nyberg confirmed the resilience of certain DES-like iterated ciphers against differential cryptanalysis [15]. Sean Murphy and M.J.B. Robshaw raised concerns about the potential vulnerability of the Twofish cipher in eight rounds, particularly due to the influence of key-dependent S-boxes [14]. In a similar approach, Youssef, and Tavares in 1995 proposed increasing input variables and balancing S-boxes to enhance resistance against both differential and linear cryptanalysis [13] [11].

Researchers can explore new methods and techniques to enhance the effectiveness and sophistication of differential attacks, particularly by advancing the modelling of differences and propagation trajectories in cryptographic algorithms. In a novel approach, a method has been developed to address the

Researchers are exploring new methods and techniques to enhance the efficiency and sophistication of differential attacks by advancing the modelling of differences and propagation trajectories in cryptographic algorithms. An innovative approach has been developed to address the fundamental problem of differential cryptanalysis, which aims to identify the highest entries in the Difference Distribution Table (DDT) of a given application [25]. Additionally, differential attacks can be combined with other advanced attacks in what are known as hybrid attacks. This integration enables the introduction of new attack strategies, such as integrating differential attacks with algebraic attacks [26].

By integrating machine learning with these traditional cryptanalysis techniques [24], it is hoped that the precision and speed of finding solutions to break cryptographic systems can be improved. This combined approach could be crucial in the context of data security and privacy protection, allowing for better understanding and defines against potential attacks.

V. Linear Differential Cryptanalysis

In differential-linear cryptanalysis applied to DES, the method involves dividing the encryption process into two distinct parts. In the first part, significant differential characteristics are sought, indicating that differences in the plaintext input result in significant variations in the ciphertext output. In the second part, biased linear approximations are identified, exploiting a linear relationship between the input and output bits. By combining these two aspects, a differential-linear distinguisher is developed to attack DES and recover part of the secret key.

Differential-linear cryptanalysis combines both differential and linear attacks to decrypt a cipher by segmenting the process into two distinct parts. In the first part, a significant difference is identified, while in the second part, a biased linear approximation is pinpointed. This method was introduced by Langford and Hellman [40], and later expanded by Biham et al. [41, 55] by introducing a probabilistic truncated difference in the early rounds of the process. Recently, Lu [54, 53] examined the validity of the Biham et al. model, aiming to reduce the assumptions required for the attack. Wagner [53] proposed ideas for a unified perspective on statistical block cipher cryptanalysis, albeit with reservations regarding the assumptions underlying differential-linear attacks. Although the theoretical link between linear and differential attacks has not been fully exploited in previous work, recent studies [51, 50] have extended the application of this cryptanalytic technique to ciphers such as Ascon and Chaskey

Recently, a differential-linear attack [56] was presented against the authenticated cipher ICEPOLE [43]. The authors employed classical methods to identify potentially significant input differences and output masks. However, the bias of the differential-linear characteristics was so substantial that the authors were able to estimate it experimentally, indicating that no assumptions about the differential-linear hull were made in this estimation. The block cipher CTC2 [57] has been demonstrated to be weak against differential-linear attacks. In previous attacks [58, 59, 60], the space V was one-dimensional, but using the differential-linear hull, the authors of [61] enhanced the best attack on this cipher. The estimation of the differential-linear bias is based and developed in [62].

The study [63] on differential-linear cryptanalysis opens several exciting perspectives in the field of cryptography and computer security. Firstly, innovative techniques such as the Differential Algebraic Transitional Form (DATF) offer new ways to understand and analyse the underlying mechanisms of encryption algorithms. This approach can be extended to other cryptosystems and could even reveal vulnerabilities previously unknown in widely used cryptographic systems.

Furthermore, improving estimates of the differential-linear bias represents a major challenge for researchers. By refining these techniques, it would be possible to better assess the potential risks posed by differential-linear attacks on a variety of cryptosystems, thus enhancing their security.

Moreover, the application of the methods developed in this study to specific encryption algorithms such as Ascon, Serpent, and Grain v1 opens new possibilities for analysing the security of these systems. Further research could be conducted to extend these analyses to other commonly used algorithms and protocols, which could contribute to a better understanding of their resistance to differential-linear attacks.

VI. Algebraic Cryptanalysis

Algebraic cryptanalysis, pioneered by Jacques Patarin in 1995[64], is a cryptographic discipline focused on deciphering encrypted messages by solving systems of polynomial equations. It gained significant traction particularly when applied to the Matsumoto-Imai multivariate cryptography scheme. This method leverages mathematical tools like finite field theory and linear algebra to scrutinize the algebraic characteristics of encryption algorithms, identifying vulnerabilities that can be exploited to break the encryption [65].

In the realm of the Data Encryption Standard (DES), algebraic cryptanalysis is pivotal in resolving systems of polynomial equations that define the relationship between plaintext, ciphertext, and the secret key. By solving these equations, the secret key can be deduced, facilitating the decryption of encrypted messages. Techniques such as Gröbner bases are instrumental in simplifying and solving these polynomial equations efficiently, thereby aiding in the quest for the secret key [65].

Automated solvers, within the domain of algebraic cryptanalysis, refer to computer programs designed to solve complex systems of polynomial equations effectively and systematically. These software tools are utilized to handle equations generated during algebraic cryptanalysis, enabling cryptanalysts to unearth solutions to encryption algorithm challenges. Gröbner bases, on the other hand, are a fundamental concept in commutative algebra. They are employed to resolve and streamline systems of polynomial equations, providing a theoretical framework for manipulating and comprehending these equations. Gröbner bases facilitate the determination of solutions to polynomial equation systems by algorithmically transforming them into simplified and more manageable forms, thereby easing their resolution. In cryptanalysis, Gröbner bases are used to scrutinize the relationships among variables associated with encryption, enabling the discovery of key information such as encryption keys or potential weaknesses in encryption algorithms.

Looking forward, the future of algebraic cryptanalysis in DES encryption involves the utilization of SAT solvers, which have shown effectiveness in solving problems with multiple solutions. Recent research on hash function cryptanalysis has demonstrated the efficacy of SAT solvers, indicating the possibility of breaking certain hash functions and MACs using algebraic and logical attacks like those developed previously, or by combining them with other methods. Additionally, addressing complex questions, such as identifying subsets of key bits in block cipher schemes to achieve specific differentials, is conceivable. In some cases, existing computer packages designed to efficiently solve SAT instances or systems of multivariate equations may be used with minimal human intervention. SAT solvers are specialized tools for solving the Boolean satisfiability problem (SAT), a fundamental challenge in theoretical computer science. Their role is to determine whether a logical formula can be satisfied by assigning truth values to variables [66].

VII. Conclusion

The exploration of DES through various cryptanalytic techniques has significantly contributed to the field of cryptography, particularly in understanding the complexities of cryptographic security and the development of more robust encryption methods. Although DES is now largely obsolete, the methodologies derived from its analysis continue to influence cryptographic research and practice. This paper has highlighted the progression from simple brute force attacks to sophisticated methods like differential and linear cryptanalysis, reflecting major advancements in the field. As the landscape of computing continues to evolve, so too will the techniques used to analyze and secure cryptographic systems. Future research will likely focus on adapting these techniques to newer encryption standards and exploring innovative cryptanalytic approaches to meet the escalating security demands of modern technology. Insights from the long-standing analysis of DES will remain crucial in guiding the design and evaluation of secure cryptographic systems.

References

[1] "Data Encryption Standard," Federal Information Processing Standards Publication No. 46, National Bureau of Standards, January 15, 1977.

[2] Matsui, M. (1993). "Linear Cryptanalysis Method for DES Cipher." In Advances in Cryptology — EUROCRYPT '93, Lecture Notes in Computer Science.

[3] Eli Biham and Adi Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, Vol. 4, No. 1, 1991

[4] Konheim, Alan G. (1 April 2016). "Automated teller machines: their history and authentication protocols". Journal of Cryptographic Engineering. 6 (1):1–29. doi:10.1007/s13389-015-0104-3. ISSN 2190-8516. S2CID 1706990. Archived from the original on 22 July 2019. Retrieved 28 August 2019.

[5] Electronic Frontier Foundation. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. Electronic Frontier Foundation

[6] Announcing the ADVANCED ENCRYPTION STANDARD (AES)." Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Archived from the original on March 12, 2017. Retrieved October 2, 201

[7] "The Economic Impacts of NIST's Data Encryption Standard (DES) Program" . National Institute of Standards and Technology. United States Department of Commerce. October 2001. Archived from the original (PDF) on 30 August 2017. Retrieved 21 August 2019.

[8] Eli Biham and Adi Shamir (1990), Differential Cryptanalysis of DES-like Cryptosystems. Advances in Cryptology -- CRYPTO '90. Springer-Verlag. 2-21.

[9] Eli Biham and Adi Shamir (1992), Differential Cryptanalysis of the Full 16-round DES. Advances in Cryptology -- CRYPTO '92. Springer-Verlag. 487-496.

[10] Eli Biham and Adi Shamir (1991). Differential Cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Advances in Cryptology -- CRYPTO '91. Springer-Verlag. 156-171.

[11] Adams, C. (1992), On immunity against Biham and Shamir's differential cryptanalysis. Information Processing Letters. 41: 77-80.

[12] Dawson, M. and S. Tavares (1991), An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential-Like Attacks. Advances in Cryptology -- EUROCRYPT '91. 353-367.

[13] Youssef, A., S. Tavares. (1995). Resistance of Balanced S-boxes to Linear and Differential Cryptanalysis. Information Processing Letters. 56: 249-252

[14] Sean Murphy,M.J.B. Robshaw (2000),Differential Cryptanalysis, Key-dependant,S-boxes, and Twofish

[15] Nyberg, K. 1991. Perfect nonlinear S-boxes. Advances in Cryptology -- EUROCRYPT '91. 378- 386.

[16] Xuejia Lai, Massey J.L (1991). Markov Ciphers and Differential Cryptanalysis. Swiss Federal Institude of Technology, Royal Holloway University of London

[17] Eli Biham and Adi Shamir (1993), Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag,Berlin,Germany

[18] Fauza Mirzan (2000),Block Ciphers and Cryptanalysis, Department of Mathematics, Royal Holloway University of London

[19] Howard M. Heys (2000), A Tutorial on Linear and Differential Cryptanalysis, Memorial University of Newfoundland, Canada

[20] William Stallings, "Cryptography and Netwrk Security: Principles and Practice", 7th Edition, Pearson Education Limited, 2017.

[21] Menezes, A.; Oorschot, P. van; Vanstone, S. (1997). Handbook of Applied Cryptography (5th ed.). CRC Press. ISBN 0-8493-8523-7.

[22] Tameem Hameed Obaida, Abeer Salim Jamil, Nidaa Flaih Hassan. "A Review: Video Encryption Techniques, Advantages And

Disadvantages." Webology, ISSN: 1735-188X, Volume 19, Number 1, 2022.

[23] Bátiz-Lazo, Bernardo (2018). Cash and Dash: How ATMs and Computers Changed Banking. Oxford University Press. pp. 284 & 311. ISBN 9780191085574.

[24] Mohammed M. Alani. 2019. Applications of Machine Learning in Cryptography: A Survey. 1, 1 (February 2019), 8 pages. https://doi.org/10.1145/3309074.3309092

[25] Dinur, I., Dunkelman, O., Gutman, M., & Shamir, A. (2015). Improved Top-Down Techniques in Differential Cryptanalysis. Conference paper presented at Progress in Cryptology -- LATINCRYPT 2015. Lecture Notes in Computer Science (Vol. 9230).

[26] Albrecht, M.R., & Cid, C. (2010). Algebraic Techniques in Differential Cryptanalysis. Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom. {M.R.Albrecht, carlos.cid}@rhul.ac.uk.

[27] Buttyan, L. and I Vajda (1995), Searching for the best linear approximation of DES-like cryptosystems. Electronics Letters. 31(11): 873-874.

[28] Daemen, J., R. Govaerts and J. Vandewalle (1995), Correlation Matrices. Fast Software Encryption. Lecture Notes in Computer Science (LNCS) 1008. Springer-Verlag. 275-285

[29] Eli Biham (1994), On Matsui's Linear Cryptanalysis. Technion, Israel Institute of Technology, Israel

[30] Harpes, C., G. Kramer and J. Massey (1995), A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma, Advances in Cryptology -- EUROCRYPT '95. 24-38.

[31] Kaliski, B. and M. Robshaw (1994) Linear Cryptanalysis Using Multiple Approximations. Advances in Cryptology -- CRYPTO '94. 26-39.

[32] Mitsuru Matsui (1994), Linear cryptanalysis method for DES cipher, EUROCRYPT 1994, no.765, pg. 386-397,

[33] Rainier A. Rueppel (1986), "Analysis and Design of Stream Ciphers," Spreinger Verlag.

[34] Kaliski Jr., B.S., & Robshaw, M.J.B. (2001). Linear Cryptanalysis Using Multiple Approximations. RSA Laboratories, 100 Marine Parkway, Redwood City, CA 94065, USA.

[35] Courtois, N. T., & Pieprzyk, J. (n.d.). Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. CP8 Crypto Lab, SchlumbergerSema, 36-38 rue de la Princesse, BP 45, 78430 Louveciennes Cedex, France. Retrieved from http://www.nicolascourtois.net (Courtois: courtois@minrank.org) and ICS, Macquarie University, NSW 2109, Australia (Pieprzyk: josef@comp.mq.edu.au).

[36] Junod, P. (2005). Statistical Cryptanalysis of Block Ciphers (Thesis No. 3179). École Polytechnique Fédérale de Lausanne, Institute of Communication Systems, Communication Systems Section, Lausanne, EPFL.

[37] A. Valembois. Detection, Decoding, and Recognition of Binary Linear Codes. PhD thesis, Université de Limoges, October 2000.

[38] Pascal A. Junod (1998), Linear Cryptanalysis of DES, Eidgenssische Tenhcische

[39] Linear Cryptanalysis Using Multiple Approximations and Its Applications to DES

[40] Langford, S.K., Hellman, M.E.: Differential-Linear Cryptanalysis. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 17–25. Springer, Heidelberg (1994)

[41] Biham, E., Dunkelman, O., Keller, N.: Enhancing Differential-Linear Cryptanalysis. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 254–266. Springer, Heidelberg (2002)

[42] A.A. Selçuk, On Probability of Success in Linear and Differential Cryptanalysis. J. Cryptol., 21(1), 131–147 (2008)

[43] J. Daemen, V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard. Springer, 2002.

[44] K. Nyberg, Linear Approximation of Block Ciphers. In A. De Santis, editor, EUROCRYPT. LNCS, vol. 950 (Springer, 1994), pp. 439–444

[45] M. Hermelin, J.Y. Cho, K. Nyberg, Multidimensional Extension of Matsui's Algorithm 2, in O. Dunkelman, editor, FSE. LNCS, vol. 5665 (Springer, 2009), pp. 209–227

[46] J.Y. Cho, Linear Cryptanalysis of Reduced-Round PRESENT, in J. Pieprzyk, editor, CT-RSA. LNCS, vol 5985 (Springer, 2010), pp. 302–317

[47] A. Bogdanov, V. Rijmen, Zero-Correlation Linear Cryptanalysis of Block Ciphers. IACR Cryptol. ePrint Arch. 2011, 123 (2011)

[48] A. Bogdanov, V. Rijmen, Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des. Codes Cryptogr. 70(3), 369–383 (2014)

[49] A. Bogdanov, C. Boura, V. Rijmen, M. Wang, L. Wen, J. Zhao, Key difference invariant bias in block ciphers, in K. Sako, P. Sarkar, editors, ASIACRYPT (1). LNCS, vol. 8269 (Springer, 2013), pp. 357–376

[50] G. Leurent, Improved Differential-Linear Cryptanalysis of 7-round Chaskey with Partitioning, in M. Fischlin, J.-S. Coron, editors, EUROCRYPT 2016. LNCS, vol. 9665 (Springer, 2016), pp. 344–371

[51] C. Dobraunig, M. Eichlseder, F. Mendel, M. Schläffer, Cryptanalysis of Ascon, in K. Nyberg, editor, CT-RSA 2015. LNCS, vol. 9048 (Springer, 2015), pp. 371–387

[52] F. Chabaud, S. Vaudenay, Links Between Differential and Linear Cryptanalysis, in A. De Santis, editor, EUROCRYPT. LNCS, vol. 950 (Springer, 1994), pp. 356–365

[53] D. Wagner, Towards a Unifying View of Block Cipher Cryptanalysis, in B.K. Roy, W. Meier, editors, FSE. LNCS, vol. 3017 (Springer, 2004), pp. 16–33

[54] J. Lu, A Methodology for Differential-Linear Cryptanalysis and Its Applications - (Extended Abstract), in A. Canteaut, editor, FSE. LNCS, vol. 7549 (Springer, 2012), pp. 69–89

[55] S.K. Langford, Differential-Linear Cryptanalysis and Threshold Signatures. Ph.D. Thesis, 1995.

[56] C. Guo, H. Zhang, D. Lin, Estimating Differential-Linear Distinguishers and Applications to CTC2, in J. Lopez, Y. Wu, editors, ISPEC 2015. LNCS, vol. 9065 (Springer, 2015), pp. 220–234

[57] J. Lu, A methodology for differential-linear cryptanalysis and its applications. Des. Codes Cryptogr., 77(1), 11–48 (2015)

[58] j. Lu, A Methodology for Differential-Linear Cryptanalysis and Its Applications - (Extended Abstract), in A. Canteaut, editor, FSE. fLNCS, vol. 7549 (Springer, 2012), pp. 69–89

[59] O. Dunkelman, N. Keller, Cryptanalysis of CTC2, in M. Fischlin, editor, CT-RSA 2009. LNCS, vol. 5473 (Springer, 2009), pp. 226–239

[60] N. Courtois, CTC2 and fast algebraic attacks on block ciphers revisited. IACR Cryptol. ePrint Arch. 2007, 152 (2007)

[61] P. Morawiecki, K. Gaj, E. Homsirikamol, K. Matusiewicz, J. Pieprzyk, M. Rogawski, M. Srebrny, M. Wojcik, Icepole: High-speed, hardware-oriented authenticated encryption. Cryptology ePrint Archive, Report 2014/266, 2014. http://eprint.iacr.org/

[62] T. Huang, I. Tjuawinata, H. Wu, Differential-Linear Cryptanalysis of ICEPOLE, in G. Leander, editor, FSE 2015. LNCS, vol. 9054 (Springer, 2015), pp. 243–263

[63] Meicheng Liu, Xiaojuan Lu, Dongdai Lin, "Differential-Linear Cryptanalysis from an Algebraic Perspective," in Advances in Cryptology – CRYPTO 2021, pp. 247–277, 11 August 2021.

[64] Patarin, J. (1995). "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88." EUROCRYPT 95. Springer, Berlin, Heidelberg.

[65] Courtois, N.T., & Bard, G.V. (2007). Algebraic Cryptanalysis of the Data Encryption Standard. In S.D. Galbraith (Ed.), Cryptography and Coding 2007 (pp. 152–169). Springer, Berlin, Heidelberg

[66] Ilya Mironov and Lintao Zhang Applications of SAT Solvers to Cryptanalysis of Hash Functions, In Proc. Theory and Applications of Satisfiability Testing, SAT 2006, pp. 102-115, 2006. Also available at http://eprint.iacr.org/2006/254