A Survey on the Cryptanalysis of the Advanced Encryption Standard

Muhammad Reza Z'aba[1], Mohd Aizaini Maarof[2]

Department of Computer Systems and Communications
Faculty of Computer Science & Information Systems
Universiti Teknologi Malaysia
[1]Tel: 07-5532398, E-mail: mreza2@siswa.utm.my
[2] Tel: 07-5532002, E-mail: maarofma@fsksm.utm.my

Abstract

The Advanced Encryption Standard (AES) is a cipher adopted by the National Institute of Standards and Technology (NIST) to secure classified United States (US) digital government documents. A cipher is an algorithm that converts information (plaintext) to unreadable (ciphertext) form and vice-versa. The AES has also been employed in other areas such as to secure information in smart cards and online transactions. This year marks the fifth year that the AES has been adopted as a standard. During that period, many attacks have been performed on the cipher. However, none have fully broken the complete round cipher. All of the attacks were launched on reduced-round version and the complexity is compared to that of brute force. Brute force is an attack that tries every possible value of the key of the cipher. Therefore, it serves as the upper bound on the attack on block ciphers. In this paper, we will review some existing cryptanalytic attacks on AES.

Keywords: Cryptanalysis, Cryptography, Advanced Encryption Standard

1 Introduction

Cryptology is concerned with the making (cryptography) and breaking (cryptanalysis) of schemes that provide certain security services (confidentiality, integrity, authenticity etc.). The schemes contribute significantly to the practical and intellectual underpinnings for communications security [8].

Cryptography is a science of protecting information by encryption and decryption using a key. Encryption is the process of converting information from readable to unreadable format. The message prior to the encryption process is called the plaintext while the scrambled data after the encryption is called the ciphertext. The plaintext can be recovered from the plaintext with a decryption process using a key. The algorithm that can perform encryption and decryption is called a cipher.

A cipher is categorized into symmetric and asymmetric algorithms. The former uses the same key for encryption and decryption while the latter employs different key for both operations. A symmetric cipher can be further classified into block and stream cipher. A block cipher operates on blocks of data and a stream cipher works on one bit at a time.

Cryptanalysis is the opposite of cryptography. The field deals with the uncovering of encrypted messages without initial knowledge of the key used in the encryption process.

In 1997, NIST spearheaded an effort to replace the Data Encryption Standard (DES) [26], which is to be called the AES [27]. After some evaluation processes, the Rijndael [11] cipher was selected as the AES from fifteen candidates in 2000.

This paper aims to review existing attacks on AES and highlights some potential future works. Section 2.0 gives an introduction to the AES and some basic concepts of cryptanalysis is given in section 3.0. Section 4.0 reviews existing attacks on AES. Further research is suggested in section 5.0 and section 6.0 concludes the paper.

2 Advanced Encryption Standard

The AES [27] is a 128-bit block cipher with key lengths of 128 (denoted AES-128), 192 (AES-192) and 256 bits (AES-256). For AES-128, the cipher uses 10 rounds, 12 rounds for AES-192 and 14 rounds for AES-256. The 128-bit data block can be illustrated as a 4x4 byte matrix as shown in Figure 1. The indices of byte *s* represent the row and column of each byte. Each round except for the last consists of four transformations namely SubBytes, ShiftRows, MixColumns and AddRoundKey. SubBytes simply substitutes one byte to another byte, ShiftRows cyclically shifts the rows of the state over different offsets, MixColumns is a linear transformation of all four bytes in the same column and KeyAddition is an exclusive-OR (XOR) operation of the current data block with the round key. The last round omits the MixColumns

transformation and the first round is preceded with an AddRoundKey.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

Figure 1: A 4x4 data block of the AES

3 Cryptanalysis

This section introduces some basic concepts on the cryptanalysis of a block cipher.

The attacks performed on block ciphers is based on a threat model called Kerckhoff's assumption [18] whereby the attacker knows all the details of the cipher except the secret key. Based on this assumption, attacks are classified according to adversary's capabilities:

- Ciphertext-only: a passive attack whereby an adversary is assumed to possess a set of ciphertext to recover the plaintext of secret key.
- Known plaintext: a passive attack whereby an adversary knows some plaintext-ciphertext pairs to find the unknown portion of the plaintext or secret key.
- Chosen plaintext: an active attack whereby an adversary has the ability to choose plaintexts and obtained the corresponding ciphertexts.
- Chosen ciphertext: an active attack whereby an adversary has the ability to choose ciphertexts and obtained the corresponding plaintexts.
- Related-key: an adversary is assumed to choose some relation between the secret key used in encryption and decryption, but not the value of the key.

A cipher vulnerable to a ciphertext-only attack is considered weak [16] while a cipher which is secure against a chosen ciphertext attack is deemed secure [21].

Attacks can also be classified based on the required effort that the adversary needs to solve:

- Brute-force: in this attack, every possible value of the key is tried until the plaintext is recognized. The attack is also called an exhaustive key search.
- Shortcut attacks: an attack that has the complexity less than that of brute-force.
- Side channel attacks: an attack based on information obtained from physical implementation of a cipher.
- Fault analysis: an attack based on systematically inducing faults in particular hardware components used to protect or to store keys or algorithms.

This paper focuses on shortcut attacks.

Attacking a cipher does not necessarily mean to find the secret key. Based on recovered information, Knudsen [19] described a hierarchical classification of the outcomes of an attack:

- Total break: an adversary recovers the secret key.
- Global deduction: an adversary discovers an algorithm which is functionally equivalent to the encryption and decryption process without knowledge of the key.
- Instance (local) deduction: an adversary recovers the plaintext (or ciphertext) from an intercepted ciphertext (or plaintext) which was not acquired from the legitimate sender.
- Information deduction: an adversary obtains information about the secret key, plaintexts or ciphertexts which was not directly came from the legitimate sender and which was not known before the attack.
- Distinguishing algorithm: an attacker is able to tell whether the attacked cipher is a randomly chosen permutation or one of the 2k permutations indicated by the secret key.

The success of an attack can be measured by its complexity as follows:

- Data complexity: the amount of data (plaintexts or ciphertexts) required to execute the attack under a certain threat model.
- Time complexity: the number of encryption / decryption needed to perform the attack.
- Memory complexity: the amount of memory needed to hold all data during the attack.
- Success probability: measures the frequency of a successful attack when repeated in a number of times.

3.1 Differential and Linear Cryptanalysis

Two most prominent attacks [29] on block ciphers are linear [24] and differential cryptanalysis [3]. This section briefly explains the gist of the attacks.

Differential cryptanalysis was discovered by Israeli researchers Eli Biham and Adi Shamir [3]. It is a chosen-plaintext attack that relies on the idea that a fixed input difference may, with high probability, generate a particular output difference. By encrypting pairs of plaintexts with prescribed bitwise difference, and seeing which key bits are suggested by the output difference, key bits are determined. As we will see in the following sections, the majority of attacks are based on the concept of differential cryptanalysis.

A few years later, Mitsuru Matsui introduced the concept of linear cryptanalysis [24]. The attack works by finding linear relationship between plaintext, ciphertext and key bits that reveal information about the key. Later, Matsui improved

the attack and performed the cryptanalysis on DES [25]. It is a known-plaintext attack and seeks to find a linear approximate expression of a given cryptographic algorithm.

4 Attacks on AES

This section gives brief reviews on existing attacks on AES. The general idea of the attack is presented along with the complexities of the attacks. The interested reader is advised to read the referred paper for a more detail treatment of the attacks.

4.1 Square Attack

The square attack is originally a dedicated attack on a block cipher with the same name [10]. Because AES inherits some of the properties of the square cipher, therefore the attack also applies to AES. The attack has also been called the saturation [23], integral [20] and structural / multiset [6] attacks.

The attack works by observing the propagation of the XOR for a set of plaintext called a Λ-set. A Λ-set is a set of 256 plaintexts that are all different in some of the bytes and equal in all other bytes. The basic attack can be applied to AES reduced to four rounds. The attack can be extended by adding a round at the end and at the beginning of the cipher for a total of six rounds. Some key values for the initial round, fifth and sixth round are then guessed until the required criterion is met.

The six-round attack requires 2^{32} chosen plaintext or 2^{72} cipher executions while the memory complexity is 2^{32}. In [13], Ferguson et al. reduce the work factor of the six-round attack to 2^{44} cipher executions and the number of chosen plaintext needed is 2^{35}. The authors use a technique called partial sum to improve the complexity of the attack. A further extension of the attack is also described by the authors. For a seven-round attack, $2^{128} - 2^{119}$ chosen plaintexts are required which is comparable to 2^{120} encryptions.

Lucks [22] extended the square attack to cover seven rounds of AES. For AES-192, the nature of its key schedule allows the author to attack AES reduced to seven rounds using 2^{32} chosen plaintexts which is equivalent to 2^{184} of time complexity. The attack on AES-256 requires the same amount of chosen plaintext but the time complexity increases to 2^{200}.

Therefore, the best attack on AES based on the square attack is using the partial sum technique. The attack successfully penetrates seven out of ten rounds of AES-128, up to eight (out of 12) rounds of AES-192 and nine (out of 14) rounds of AES-256. These numbers make up 70% of the AES-128, 68% of AES-192 and 64% AES-256.

4.2 Collision Attack

The square attack is based on the fact that three rounds of AES can be distinguished from a random permutation. Gilbert and Minier [14] devised an attack which could distinguish a four-round AES from a random permutation. They exploit the existence of collisions between some partial functions induced by the cipher. The distinguisher allows them to attack AES reduced to seven rounds which requires 2^{32} chosen plaintexts and a complexity of about 2^{140}. A variant of the attack on AES-128 results in a much lower complexity and faster than brute force.

4.3 Impossible Differential

Impossible differential is an attack that exploits on the behaviour of the MixColumns transformation. If we have a pair of plaintext which differs only in one byte, then the ciphertext in AES reduced to four rounds can not be the same in the following byte positions: {(0,0), (1,3), (2,2), (3,1)}, {(0,1), (1,0), (2,3), (3,2)}, {(0,2), (1,1), (2,0), (3,3)} nor {(0,3), (1,2), (2,1), (3,0)}. Wrong key bytes are eliminated if the impossible event occurs.

The attack was first presented on the AES-128 reduced to five rounds by Biham and Keller [2]. This was later improved by Cheon et al [7] to cover six rounds using $2^{91.5}$ chosen plaintexts and a time complexity of 2^{122}. For AES-192 and AES-256, Phan [28] managed to attack the cipher reduced to seven rounds. The attack requires 2^{92} (AES-192) and $2^{92.5}$ (AES-256) chosen plaintexts with time complexities of 2^{186} (AES-192) and $2^{250.5}$ (AES-256).

Currently, the best impossible differential attack penetrates AES-128 up to six rounds. Fro both AES-192 and AES-256, the best attack so far manages to break through seven rounds.

4.4 Boomerang

The boomerang attack [30] is an adaptive chosen plaintext and ciphertext attack which is an extension to differential cryptanalysis. The attack works by breaking the cipher into two parts and a differential is used in each part. These two differentials are later joined to suggest an adaptive chosen plaintext and ciphertext property of the algorithm that has high probability.

The attack on AES reduced to five and six rounds has data complexity of 2^{39} and 2^{71} respectively [4]. The total workload or time complexity of the attack is set at 2^{39} and 2^{71} for each reduced round.

We have not found other variants of this attack on the AES. Hence, this is the best boomerang attack on the cipher.

4.6 Impossible Related-Key Differential

The related key attack [1] is an attack that exploits the key scheduling of a cipher. Obvious relationship between the keys enables the attack to be mounted on weak key schedules. The attack observes the behaviour of a cipher by using different but related keys. This attack is independent of the number of rounds and the inner structure of a cipher. By combining this attack with impossible differential cryptanalysis, an impossible related-key differential attack is mounted on AES-192 [15].

The attack is able to penetrate up to seven rounds of AES using 2^{111} plaintext/ciphertext pairs with time complexity of 2^{116}. On the other hand, the time complexity of the attack on eight-round AES is 2^{183} and requires 2^{88} plaintext/ciphertext pairs.

4.7 Algebraic Attacks

Another recent attack is those which focused on the algebraic structure within the AES. The attacks are algebraic in nature, rather than statistical. The attacks rely on analyzing the internals of a cipher and deriving a system of quadratic simultaneous equations. These systems of equations are typically very large, for example 8000 equations with 1600 variables for the 128-bit AES. Several methods for solving such systems are known. In the eXtended Sparse Linearization (XSL) attack [9], a specialized algorithm is then applied to solve these equations and recover the key.

Another attack in this category is the interpolation attack [17]. The attack constructs polynomials from plaintext and ciphertext pairs. If the components of a cipher have a compact algebraic expression, then the expressions can be combined to represent the entire cipher. If the expression of the ciphertext as a polynomial of the plaintext has a manageable complexity i.e. low degree, then the coefficients of this polynomial can be determined with a small amount of plaintext/ciphertext pairs. The Lagrange interpolation formula is used to determine the coefficients of the polynomial.

However, the threat posed by algebraic attacks on AES is difficult to quantify [12] and it is unclear whether the attack should be regarded as a serious security threat [31]. Therefore, more research should be put into this area.

Table 1 shows the summary of the attacks on AES.

Table 1: Summary of attacks on the AES

Attack	Key size	No. of rounds	Data complexity	Time complexity	Memory
Square []	All	6	2^{32}	2^{72}	2^{32}
Partial sum []	All	6	6×2^{32}	2^{44}	2^{32}
Partial sum []	192	7	19×2^{32}	2^{155}	2^{32}
Partial sum []	256	7	21×2^{32}	2^{172}	2^{32}
Partial sum []	All	7	2^{128} - 2^{119}	2^{120}	2^{64}
Partial sum []	192	8	2^{128} - 2^{119}	2^{188}	
Partial sum []	256	8	2^{128} - 2^{119}	2^{204}	
Partial sum []	256	9	2^{85}	2^{224}	
Square (Lucks) []	192	7	2^{32}	2^{184}	2^{32}
Square (Lucks) []	256	7	2^{32}	2^{200}	2^{32}
Collision []	192	7	2^{32}	2^{140}	2^{32}
Collision []	256	7	2^{32}	2^{192}	2^{32}
Impossible differential [Biham]	128	5	$2^{29.5}$	2^{31}	2^{42}
Impossible differential [Cheon]	128	6	$2^{91.5}$	2^{122}	2^{89}
Impossible differential [phan]	192	7	2^{92}	2^{186}	2^{153}
Impossible differential [phan]	256	7	$2^{92.5}$	$2^{250.5}$	2^{153}
Boomerang [Biryukov]	128	5	2^{39}	2^{39}	2^{33}
Boomerang [Biryukov]	128	6	2^{71}	2^{71}	2^{33}
Impossible related-key differential	192	7	2^{111}	2^{116}	
Impossible related-key differential	192	8	2^{88}	2^{183}	

5 Further Research

According to [20], square can be combined with the interpolation attack. Other than that, as of late, a breed of hybrid of new attacks has emerged, which combines existing attacks to form new attacks. Therefore, there are plenty of rooms to make further research. Ferguson et. al [13] note that there are many ways in which variations on their attack can be made, such as using a different key difference pattern or applying the partial-sum technique further to reduce the workload. For boomerang attack, the author states the possibility of the attack to penetrate seven rounds of AES-192. Other than that, the middle-round gaining trick used to attack Safer+ [5] might also be used to attack the AES.

6 Conclusion

Currently, the best attack on AES-128 is the partial sum technique which is able to cryptanalyze the cipher reduced to seven rounds. For AES-192 and AES-256, the same technique is the best attack which penetrates eight and nine rounds respectively. Therefore, three more rounds are needed to reach the maximum round of AES-128. Meanwhile, for AES-192 and AES-256, another four and five rounds each are required. All of the authors claimed that their attacks do not posed a serious threat to AES because most of the attacks are impractical (requires huge amount of data or memory). The results show certificational attacks that worked on the cipher and any attack which is faster than brute force is considered a shortcut attack. [Lucks]. We also look into some further extensions of the attack presented in this paper. The minimum size of key for AES is 128 bits prohibits an exhaustive key search on the cipher with current technologies. However, with the emergence of quantum cryptology, the time required to perform brute-force attack on a cipher might be shorten. DES managed to stay as a standard for nearly 30 years and AES is expected to exceed, if not match the period. Only time will tell whether the AES is able to stand the test of time or not.

7 References

[1] Biham, E. (1994). New Types of Cryptanalytic Attacks Using Related Keys. Advances in Cryptology, EUROCRYPT '93, LNCS 765, Springer-Verlag, pp. 398-409.

[2] Biham, E. and Keller, N. (2000). Cryptanalysis of Reduced Variants of Rijndael. Submitted to the 3rd AES Candidate Conference. Available at: http://csrc.nist.gov/encryption/aes/round2/conf3/papers/35-ebiham.pdf.

[3] Biham, E., and Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3-72.

[4] Biryukov, A. (2005). The Boomerang Attack on 5 and 6-round Reduced AES. 4th International Conference, AES 2004, LNCS 3373, Springer-Verlag, pp. 11-15.

[5] Biryukov, A., Canniére, C.D. and Dellkrantz, G. Cryptanalysis of SAFER++. Advances in Cryptology – CRYPTO 2003. LNCS 2729, Springer-Verlag, pp. 195-211.

[6] Biryukov, A., and Shamir, A. (2001). Structural Cryptanalysis of SASAS. Advances in Cryptology - EUROCRYPT 2001. LNCS 2045, Springer-Verlag, pp. 394-405.

[7] Cheon, J.H., Kim, M., Kim K., Lee, J.-Y. and Kang, S. (2002). Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. Information Security and Cryptology - ICISC 2001: 4th International Conference Seoul, Korea, December 6-7, 2001, LNCS 2288, Springer-Verlag, Kim, K. (Ed.), pp. 39-49.

[8] Clark, J. A. (2001). Metaheuristic Search as a Cryptological Tool. Ph.D dissertation. University of York, December 2001.

[9] Courtois, N. T., and Pieprzyk, J. (2002). Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Advances in Cryptology - ASIACRYPT 2002. LNCS 2501, Springer-Verlag, pp. 267-287.

[10] Daemen, J., Knudsen, L., and Rijmen, V., 1997. The Block Cipher SQUARE. Fast Sofware Encryption, LNCS 1267, Springer-Verlag, pp. 149-165.

[11] Daemon, J. and Rijmen, V. (2002). The Design of Rijndael, AES – The Advanced Encryption Standard. Berlin: Springer-Verlag.

[12] Dobbertin, H., Knudsen, L. and Robshaw, M. 2005. The Cryptanalysis of the AES – A Brief Survey. Advanced Encryption Standard – AES: 4th International Conference, Bonn, Germany, May 10-12, 2004, LNCS 3373, Dobbertin, H., Rijmen, V. and Sowa, A. (Eds.), Springer-Verlag, pp. 1-10.

[13] Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D and Whiting, D. (2001). Improved Cryptanalysis of Rijndael. Fast Software Encryption 2000, LNCS 1978, Springer-Verlag, pp. 213-230.

[14] Gilbert, H. and Minier, M. (2000). A collision attack on 7 rounds of Rijndael. 3rd AES candidate conference, New York, April 13-14, pp. 230-241.

[15] Jakimoski, G. and Desmedt, Y. (2004). Related-Key Differential Cryptanalysis of 192-bit Key AES Variants. SAC 2003, LNCS 3006, Springer-Verlag, pp 208-221.

[16] Junod, P. (2005). Statistical Cryptanalysis of Block Ciphers. PhD Dissertation. Federal Institute of Technology, Lausanne.

[17] Jakobsen, T. and Knudsen, L (1997). The interpolation attack on block ciphers. Fast Software Encryption. LNCS 1267, Springer-Verlag, pp. 28-40.

[18] Kerchkoff, A. (1883). La Cryptographie Militaire. J*ournal des Sciences Militaires*. 9, 5-38.

[19] Knudsen, L.R. (1999). Contemporary Block Ciphers. Lectures on Data Security. LNCS 1561, pp. 105-125, Damgård, I. (Ed.), Springer-Verlag.

[20] Knudsen, L., and Wagner, D. (2002). Integral Cryptanalysis. Fast Software Encryption, LNCS 2365, pp. 112-127, Springer-Verlag.

[21] Landau, S. (2000). Designing Cryptography for the New Century. Communications of the Association for Computing Machinery, 43(5), 115-120.

[22] Lucks, S. (2000). Attacking Seven Rounds of Rijndael under 192-bit and 256-bit Keys.

Proceedings of the 3rd AES candidate conference, April 13-14, New York, pp. 215-229.

[23] Lucks, S. (2002). The Saturation Attack – A Bait for Twofish. Fast Software Encryption: FSE 2001. LNCS 2355, Springer-Verlag, pp. 1-15.

[24] Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology - EUROCRYPT '93, LNCS 765, Springer-Verlag, 386-397.

[25] Matsui, M. (1994). The First Experimental Cryptanalysis of the Data Encryption Standard. Advances in Cryptology - CRYPTO '94, LNCS 839, Springer-Verlag, Desmedt, Y. G. (Ed.), 1-11.

[26] National Bureau of Standards. Data Encryption Standard (1997). U.S. Department of Commerce, Washington D.C., January 1977.

[27] National Institute of Standards and Technology (2001). Advanced Encryption Standard (AES). FIPS PUB 197. Available at http://csrc.nist.gov/publications/fips/.

[28] Phan, R.C.-W. (2004). Impossible Differential Cryptanalysis of 7-round Advanced Encryption Standard (AES). Information Processing Letters, Elsevier Science, Vol. 91, No. 1, July 2004, pp. 33-38.

[29] Stallings, W. (2003). Cryptography and Network Security Principles and Practices, 3rd Edition. Upper Saddle River, New Jersey: Prentice Hall.

[30] Wagner, D. (1999). The Boomerang Attack. Fast Software Encryption 6, LNCS 1636, Springer-Verlag, pp. 156-170.

[31] Xiao, L. (2003). Applicability of XSL attacks to block ciphers. IEE Electronic Letters. Vol. 39 No. 25, pp. 1810- 1811.