A Survey of the Attacks on AES

Ali DOĞANAKSOY, Aslı DARBUKA, Dilek ÖZBERK, Neşe ÖZTOP, Fatih SULAK

***Abstract*—In this paper, a survey of the attacks on AES is given. The aim of the paper is to make a collection of the academic cryptanalysis of 3 different variants of AES. In this survey, side-channel attacks and related-key attacks are not covered. Most efficient attacks such as square attack, impossible differential attack, boomerang attack, algebraic attack and meet in the middle attack are given. All attacks can only break reduced variants of AES. Also, complexities of the mentioned attacks are tabulated.**

***Keywords* —AES, cryptanalysis, square attack, impossible differential attack, boomerang attack, algebraic attack, meet in the middle attack.**

I. Introduction

After the cryptanalysis of Data Encryption Standard (DES), NIST made a competition for the new standard for block ciphers. Rijndael, a block cipher designed by Rijmen and Daemen, won the competition and was adopted as Advanced Encryption Standard (AES) in 2000. It is the most widely used block cipher in the world.

AES has a block length of 128 bits and 3 different key sizes; 128 bits (AES-128), 192 bits (AES-192) and 256 bits (AES-256). Since the most powerful attacks for block ciphers are differential and linear cryptanalysis, AES is designed to be provably secure against these attacks.

AES is a very simple substitution permutation network (SPN) type block cipher and operates on bytes. S-box which is based on the inverse operation in GF(2) is the only nonlinear part of AES and for diffusion, shift row and mix column operations are used. Despite its simple structure, it is secure against known attacks.

In this paper, we collect all important attacks on AES. All of the attacks are for reduced round versions of AES and complexities are not realistic. Due to space limitations, we omit the description of AES. In section 2, square attack is given, in section 3, impossible differential attack on AES is presented. Boomerang attack is presented in section 4. Section 5 is for algebraic attack and in section 6, meet in the middle attack is given. After that, we conclude the paper and give all the complexities in Table I.

Notation: Let SB, SR, MC and AR denote the operations SubBytes, ShiftRows, MixColumns, and AddRoundKey, respectively.
Let K_i denote the subkey in the i^{th} round, and K_w denote the initial whitening subkey. In some cases, the order of the MixColumns and the AddRoundKey operations in the same round is changed so, the subkey K_i is changed with $W_i = MC^{-}(K_i)$
Let $(x_i)_{col\ k}$ denote the k^{th} column of x_i, where k=0,1,2,3 and $(x_i)_j$ is the j^{th} byte of x_i (j=0,1,...,15). Here, Column(0) includes bytes 0,1,2,3 and Column(1) includes bytes 4,5,6,7 etc.

Ali Doğanaksoy, Aslı Darbuka, Dilek Özberk, Neşe Öztop and Fatih Sulak are with the Department of Cryptography, Middle East Technical University, Ankara, Turkiye e-mail: {aldoks, aslid, dilek, noztop, sulak}@metu.edu.tr.

II. Square Attack on Reduced-Round AES

Square attack is a chosen plaintext attack invented by Lars Knudsen particularly for breaking substitution-permutation network cryptosystems. It was originally applied to the block cipher Square [1], so named as Square attack. The attacker uses complete sets of carefully chosen plaintexts and the concept of multisets, where a multiset is a group of values which can appear more than once. In the original proposal of AES [2], a square attack on 4-round AES-128 and its extension up to 6 rounds are presented. Then, this attack is applied to AES-192 and AES-256. Moreover, a 7-round attack on AES for all key sizes is introduced. However, exhaustive search is much faster than the 7-round attacks on AES-128 and AES-192 [3]. So, they are impractical. Lastly, the attacks presented in [2] and [3] are further improved and 8-round attacks on AES-192 and AES-256 are given in [4].

A. A 3-Round Distinguisher of AES-128

To build a 3-round distinguisher, a Λ-set, which is defined as a collection of 256 states that differ in only one byte and equal in all the other bytes is constructed. The byte which takes all 256 values is called an active byte. To see the attack in a more clear way, consider a Λ-set in which only the first byte is active and all the other bytes take a constant value. One should understand the effects of round transformations on the sets of bytes to follow the steps of the attack. In the first round, the input of MC is again a Λ-set. Since SB is bijective, it leaves the types of sets of bytes unchanged. Also note that SR does not have an effect on the values of bits in the bytes. So, it does not change the type of the sets of bytes. Then, MC converts all the bytes of the first column into active bytes and hence, after one round encryption, the bytes in the first column take all 256 values, while the other 12 bytes take constant values. In the second round, the active bytes in the first column are diffused by SR so that all columns include one active byte. Then, the active bytes of these columns spread over all the bytes of the state by MC. Therefore, each byte of the input of the third round is active and this is also the case after the SB and SR of this round. Now, the sum of all bytes is zero because they take all 256 encryptions. Since MC and AR are linear transformations, the sum of each byte at the end of round three is zero. So, a 3-round distinguisher is constructed. These are illustrated in figure 1. A denotes the active bytes, C

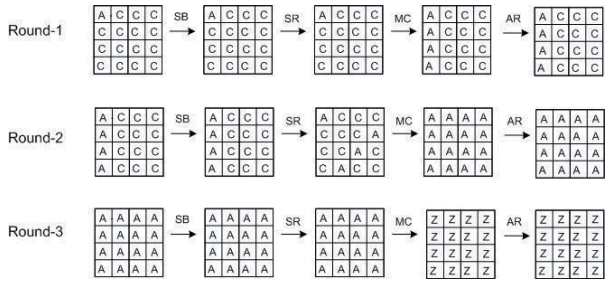

Fig. 1. A 3-round distinguisher for AES-128

denotes the bytes that take all constant values and Z denotes the bytes whose sum over all 256 encryptions is zero.

B. The Basic 4-Round Attack on Reduced-Round AES-128

The 4-round attack in [2] is based on the 3-round distinguisher which is described in the previous section and goes as follows:
For the attack, it is desired to compute a particular byte at the end of round 3. So, start decryption from round 4 by guessing a key byte corresponding to that particular byte. Then, add this key byte to the corresponding byte of the 256 ciphertexts one by one. Note that the last round, namely the fourth round, does not include MC and SR does not have an effect on the sum of the bytes. Therefore, continue with going backwards through the S-box. Then, check if the sum of all the decrypted values of this byte which corresponds to the output of the third round equals to zero or not. If it is not zero, then conclude that the guessed key byte is wrong. This can be achieved for finding other bytes of the key. This 4-round attack uses 2^9 plaintexts and their corresponding ciphertexts. The memory used is negligible.

C. A 6-Round Attack on AES-128

The 4-round attack is extended by first adding one round to the end of the cipher. The ciphertexts are partially decrypted up to end of round three by guessing the value of four bytes of the fifth round key and one byte of the fourth round key. Then, as in the previous attack, the values of the particular byte are summed together to check if the sum is zero. Number of required plaintexts is 2^{11} and number of ciphertext executions is 2^{40} since 40 key bits are guessed. Then, add one more round to the beginning. The output of this additional round should be a Λ-set in order to apply the basic 4-round attack after the first round. So, the output of MC in the first round has one active byte. This byte depends on four bytes of the plaintext and four bytes of the round key. A set of 2^{32} plaintexts are constructed by taking all possibilities of the four bytes which affect the active byte of the input of the second round. Then, a set of 256 plaintexts can be selected which result in a Λ-set in the second round by using the 2^{32} plaintexts and making an assumption for the value of the 4 relevant bytes of the first round key. This 6-round attack requires 2^{32} plaintexts and uses 2^{72} ciphertext executions. The memory used is 2^{32}.

D. Improvements of the 6-Round Attack

The 6-round attack presented in the original proposal is improved in [3] and [4]. First, the 6-round attack is adapted to AES-192 and AES-256 [3]. The writer takes the advantage of changing the order of round transformations and dependencies between the expanded key bytes. The key addition is achieved before SR. In this addition, a key which is equivalent to the actual round key is used. This attack uses 2^{32} chosen plaintexts and the time complexity is 2^{80}. In [4], an improved Square attack on 6-round AES suitable for all key sizes is described. Different from the previous attacks, this attack uses a new technique called 'partial sum' and all the 2^{32} chosen plaintexts, guesses just five bytes of the round keys at the last two rounds instead of guessing four round key bytes at the beginning. 2^{32} ciphertexts are partially decrypted two rounds by guessing one byte of the fifth round and four bytes of the sixth round. Then, the single byte determined at the end of decryption is summed over all ciphertexts. Now, this sum can be written in this way:

$$\sum_i S^{-1}[S_0[c_{i,0} \oplus k_0] \oplus S_1[c_{i,1} \oplus k_1] \oplus S_2[c_{i,2} \oplus k_2] \oplus S_3[c_{i,3} \oplus k_3]]$$

where S_i, $i \in \{0,1,2,3\}$, are bijective S-boxes such that each one is composed of an inverse AES S-box which is followed by a multiplication with a field element from the inverse MDS matrix, $c_{i,j}$ is the j^{th} attacked byte of the i^{th} ciphertext, and k_i, $i \in \{0,1,2,3\}$ denote the five guessed key bytes.
This sum is organised by introducing the 'partial sum' in a more effective way. For each k, a partial sum is defined as;

$$x_k := \sum_{j=0}^{k} S_j[c_j \oplus k_j]$$

here the subscript i of $c_{i,j}$ is not used since it is not considered about a particular text. The desired sum is computed by using the map $(c_0, c_1, c_2, c_3) \rightarrow (x_k, c_{k+1}, ..., c_3)$ which is obtained from the partial sum and counting on some particular images of that map by guessing the stated key bytes. The complexity for this 6-round attack is 2^{44} which shows the attack was improved vigorously.

E. 7-Round and 8-Round Attacks on AES-192 and AES-256

The 6-round attack presented in the proposal can be extended to 7-round AES-192 and AES-256 [3]. It is similar to 6-round attack, but this time the attacker simply starts decryption from the seventh round by guessing all bytes of the last round key. Naively, this causes guessing 128 more key bits. However, since there are dependencies between the expanded key bytes, the complexity of the attack is 2^{176} for AES-192 and 2^{192} for AES-256. In [4], two improvements are made for this 7-round attack. First improvement uses the new technique partial sum. This new technique helps to save work if there are more ciphertexts than possible values for the intermediate result. For AES-192, the guesses of the last round key give four key bytes in round 6 and one key byte in round 5. Then, using the partial sum technique, each structure is reduced to 2^{24} counters after guessing the last round key. This can be done for each of the 128 key bits guesses in about 2^{32} memory lookups by using some precomputed tables. Overall cost of the attack is in order of 2^{163} S-box lookups because there are three phases

each of which costs 2^{160}. This overall cost is approximated with 2^{155} trial encryptions. For AES-256, knowing the last round key does not provide any information about the sixth round key but gives most of the fifth round key. After guessing the last round key, the four bytes are computed for each of the 2^{32} texts for a total cost of 2^{160} lookups. Each of the next phases has cost of 2^{176}. So, the cost per structure is 2^{178} lookups, namely about 2^{170} trial encryptions. Since five structures are used, the overall complexity is 2^{172}. Then, a second improvement is made by introducing a new concept, "herd". The attacker focuses on a particular byte in round 1 after MC and fixes a value on this byte. Then, a set of 2^{120} encryptions are made. This set consists of a list of 2^{88} packs where each pack contains 2^{24} groups of 2^{8} encryptions varying in a single byte of the output of MC in round 2. This structure of 2^{120} encryptions is called a herd. Using this concept and some properties of the cipher, a second improvement for the 7-round attack can be made. By this improvement, one can break all key sizes with lower overall complexity but this requires the entire codebook of texts. Using these improvements, an 8-round attack can be mounted faster than exhaustive search. For AES-256, 2^{204} and for AES-192, 2^{188} work is needed. However, since again one needs the entire codebook of texts ($2^{128} - 2^{119}$ texts) , the attack is impractical.

III. Impossible Differential Cryptanalysis of Reduced-Round AES

Impossible differential cryptanalysis exploits differentials that hold with probability 0 (impossible differentials) to eliminate the wrong keys and leave the right key candidate. Up to now, several impossible differential attacks on AES have been proposed. In 2000, Biham and Keller presented an attack on 5-round AES-128 using a 4-round impossible differential which is the first impossible differential attack on AES [5]. The attack eliminates wrong keys of the first round by showing that the impossible differential property holds in the last four rounds. In [6], this impossible differential attack was expanded to six rounds by using the same 4-round impossible differential. They put this impossible differential in the middle of six rounds and covered some bits of the first and last round's subkeys. Both in [5] and [6], the attacks were applied to AES-128 and based on the weaknesses which results from the characteristic of the optimal linear layer. These attacks are chosen plaintext attacks and they are independent of the specific choice of S-box, the multiplication polynomial of MC and the key schedule. Therefore, the same attacks in [5] and [6] can also be applied to AES-192 and AES-256. However, in [9], R.C.-W.Phan proposed an impossible differential attack on 7-round AES-192 and AES-256 which works by exploiting the weaknesses in the AES key schedule and improves the data and time complexities significantly. In 2007, Zhang et al. presented some new results on impossible differential cryptanalysis of AES. They introduced new attacks on 6-round AES whose complexity is much lower than that in [6]. Moreover, they extended the attack to both 7-round (which can be applied to all key variants of AES) and 8-round AES-256 and made an improvement of the 7-round attack on AES-192 which was given in [9]. Also again in 2007, Chen et al. presented two methods of impossible differential cryptanalysis of 7-round AES-192 and 8-round AES-256 combined with time-memory trade off by exploiting weaknesses in their key schedule [12]. Complexities of their attacks are slightly better than that of [10]. However, since the attacks given by Zhang et al. [10] can be applicable to all key variants of AES and we do not want to go into the details of the AES key schedule, in this paper we will deal with the attacks given in [10].
In [7], Phan and Siddiqi proved that there exists no impossible differential greater than four rounds that can be constructed with the miss-in-the-middle technique. In all of the above attacks, the same impossible differential property is used, so it is better to give these 4-round impossible differentials at first.

A. 4-Round Impossible Differentials of AES

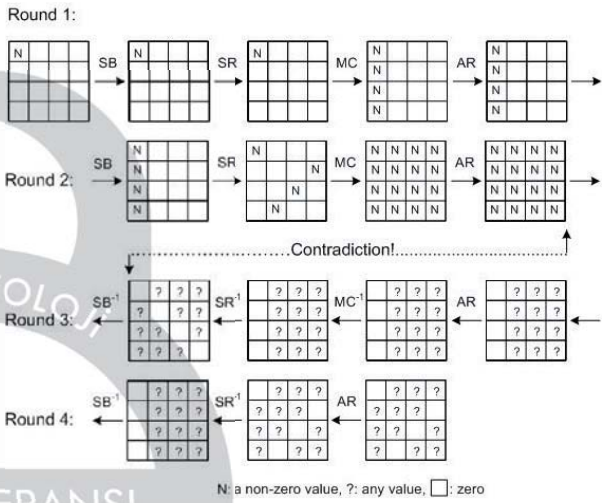

Fig. 2. A 4-Round Impossible Differential of AES

4-round impossible differentials are constructed as combining two 2-round probability-1 differentials in opposite direction where the intermediate differences induce a contradiction. This 4-round impossible differential states that given a pair of plaintexts which are equal in all bytes except one, then the ciphertexts after four rounds can not be equal in any of the following combination of impossible byte positions: (0,7,10,13), (1,4,11,14), (2,5,8,15) nor (3,6,9,12). This can be explained as follows: The difference before the first MC is in one byte, it diffuses to one column after MC. In the second round, after SR, every column has a difference in different bytes; when the second MC applied, the data differs in all bytes. On the other hand, if the ciphertexts are equal in one of the four impossible combinations of bytes, then before SR in the fourth round, the data is equal in one column and so is after SR in the third round. When SR^{-1} and then SB^{-1} are performed, the data is equal in four different bytes. This contradicts with the fact that the data differs in all bytes after the second MC.

B. An Impossible Differential Attack on 6-Round AES

Main idea of this attack is applying the 4-round impossible differential given in figure 2 between the second and the fifth

round, guessing some key bytes of the first and the last round for partial decryption, then eliminating all wrong keys by using impossible differentials. Illustration of the 6-round attack in which the prob. means that the probability is different from 1, is given in figure 3.
The attack procedure is as follows:

- Choose a set of 2^{32} plaintexts which have all different values in bytes (0,5,10,15). Generate n such structures.
- Choose the plaintext pairs whose ciphertext pairs have zero difference in all but the two bytes (3,6).
- Guess the value of the subkey bytes $(K_6)_3$, $(K_6)_6$ and partially decrypt these ciphertext pairs in order to get the outputs of the fifth round.
- Check whether the difference in at least one of the four 4-byte sets is zero where the four sets are (0,7,10,13), (1,4,11,14), (2,5,8,15) and (3,6,9,12). If not, discard the pairs.
- For every remaining ciphertext pair, consider their plaintexts and using the precomputed hash table and the list of all 2^{32} possible values of the bytes (0,5,10,15) of K_0 get rid of the wrong keys.

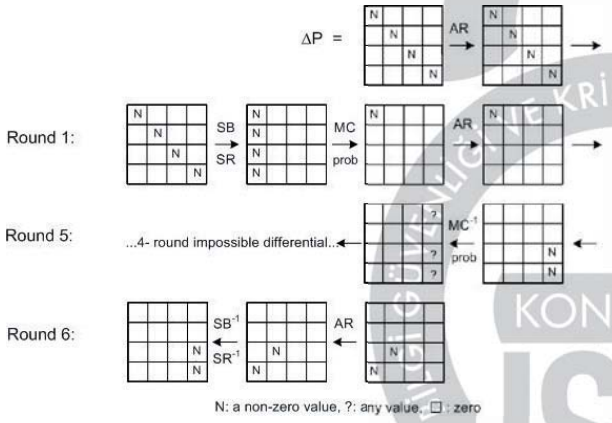

Fig. 3. Impossible Differential Cryptanalysis of 6-round AES

Data complexity of this attack is $2^{114.5}$ chosen plaintexts, time complexity is 2^{50} encryptions, and the required memory is 2^{45} bytes. In this attack, a data-time trade off can be done by guessing more bytes of subkey K_6 so that after partial decryption the number of nonzero bytes in the output of the fifth round reach the most possible. This trade-off reduces the data complexity to $2^{75.5}$ chosen plaintexts and increases the time complexity to 2^{104} encryptions.

C. Extending 6-round attack to 7-round

The above attack can be improved to attack 7-round AES. The main idea is guessing some bytes of the last round subkey K_7, decrypt the last round and apply the 6-round attack as described above. In this extension, different from the 6-round attack, the order of MC and AR in the fifth and sixth rounds is changed in order to guess less key material and the subkeys K_5 and K_6 are replaced with equivalent subkeys.
Data complexity of this attack is $2^{115.5}$ chosen plaintexts, time complexity is 2^{119} encryptions, and the required memory is 2^{45} bytes.
Note that, these two attacks are applicable to all key variants of AES and can be improved to attack 8-round AES-256.

IV. The Boomerang Attack on 5 and 6-Round Reduced AES-128

A. Overview of the Boomerang Attack

The Boomerang attack introduced in 1999 by Wagner [13] is a chosen plaintext-adaptive chosen ciphertext attack based on differential cryptanalysis. The attack treats the block cipher as a cascade of two sub-ciphers which have short, high probability differentials and combines these two differentials to make a successful attack on the given cipher. However, the boomerang attack has a strong assumption states that in order to attack a cipher, the attacker should have decryption box of the cipher besides the encryption box and this assumption makes this attack unrealistic. Furthermore, the boomerang attack can also be performed by using truncated differentials instead of using conventional differentials.

B. The Boomerang Attack on 5 and 6-Round Reduced AES-128

The attack presented by A. Biryukov [14] is a generic method to attack 5 and 6-round substitution-permutation networks (SPNs). In this study, the boomerang distinguisher is constructed by exploiting incomplete diffusion property of SPNs (including AES), not the properties of S-boxes or other components of the cipher. This attack is better than square attack in terms of speed, however, it has much more data complexity than square attack.

C. Attacking to 5-Round AES-128

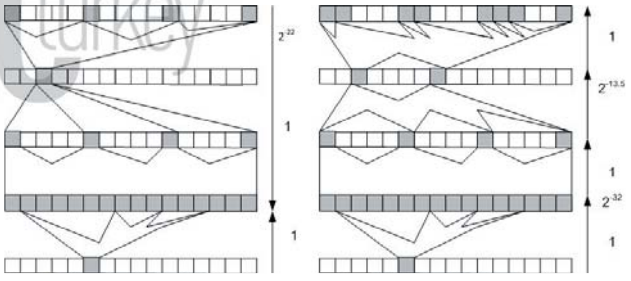

Fig. 4. The Boomerang Quartet for AES Reduced to 5-Rounds

Truncated differerentials are used in the construction of the boomerang distinguisher. (For further details about the construction of the boomerang distinguisher, see [14]). The probability of the above boomerang distinguisher is $2^{-22} \cdot 2^{-32} \cdot 2^{-13.5} = 2^{-67.5}$.
The attack algorithm goes as follows:

- Choose a pool of 2^{32} plaintexts P_i which have all possible values in the four bytes depicted in figure 4 and find their corresponding ciphertexts C_i.

- Construct a pool of ciphertexts C_i^* which have Δ difference between C_i, i.e $C_i^* = C_i \oplus \Delta$,Δ is a one-byte difference, and find their corresponding plaintexts P_i^*.
- Choose the pairs P_i^* and P_j^* which have non-zero differences in eight bytes.
- For each quartet P_i, P_j,P_i^* and P_j^* that pass third stage, guess 32-bit of the first round subkey corresponds to non-constant bytes.

The attack needs 2^6 pools of plaintexts, that is, in total 2^{38} chosen plaintexts and adaptively chosen ciphertexts. It necessitates 2^{39} running time of encryptions and 2^{36} bytes for the memory required.
In addition, by using the same boomerang distinguisher, this attack can be extented by adding one round at the bottom to attack 6-round reduced AES-128. In this way, by guessing extra 32-bit of the sixth round subkey, the attack on 6-round reduced AES-128 can be mounted with 2^{71} data and time complexities.

V. Algebraic Attack

Algebraic attack uses the algebraic structure of the cipher. In most of the block ciphers only nonlinear part is S-box. Algebraic attack uses this property and writes S-box as a Boolean function. If the degree of this function is low (2 for example), then one can rename the quadratic terms as other unknowns and try to solve this huge number of linear equations using mathematical methods, such as Gauss elimination. Actually algebraic attacks depends on algebraic structure of S-boxes, not the structure of the cipher. AES also has only nonlinear part as its S-box. However, since this S-box is based on inverse operation, algebraic degree is 254 in GF(2^8). Assume that S-box has input $x_1, x_2, \ldots, x_8$ and output $y_1, y_2, \ldots, y_8$. y_i has high algebraic degree in the x_i, but there are other implicit multivariate equations of the form $P(x_1, \ldots, x_8, y_1, \ldots, y_8)$ that are for low algebraic degree $d \leq 2$. Assume that the number of such equations is r and t is the number of monomials that appear in these equations. In general, t is around $\binom{s}{d}$. If t is very low, then we say that the equations are sparse. Also, if $r = s$, then equations give enough information about the S-box. However, if $r >> s$, then we say that the system is overdefined. In [16], a method for representing AES-128 with 8000 quadratic equations and 1600 variables is presented. The problem is solving multivariate quadratic equations which is known to be NP-hard. The most obvious way is to use linearization and eXtended Linearization (XL) with Gauss elimination. Using this method these equations can be solved in 2^{330} time. In [16], the authors show that if the MQ is sparse it is easy to solve and present a new method called eXtended Sparse Linearization (XSL). In normal XL method, all equations are multiplied by all possible monomials of some degree $D-2$, but in XSL only carefully chosen monomials are multiplied. However, for AES no results better than 2^{256} is found. Still, algebraic analysis of AES is a hot topic and researchers are trying to combine algebraic attacks with different type of attacks.

VI. Meet in the Middle Attack on Reduced Round of AES

In square attack, using 3-round distinguisher, one can attack to four rounds then, extend this attack to six rounds. Due to the special structure of AES, searching for more square like properties is essential.

A. 4-Round Distinguisher

In [15], Gilbert and Minier presented a 4-round distinguisher. By considering how plaintext changes over four rounds, they observed that in a set of 256 plaintexts with only the first byte is active (takes all possible values) and other bytes are passive, after four rounds the first byte is determined by nine fixed 1-byte parameters.

Gilbert and Minier also observed that four of these constant bytes depend on the values in the first column, but four of them are independent of these values. Using this information they form a pool of 2^{16} plaintexts where the values are given randomly to the first column and the other columns are fixed. Using birthday paradox, a collision will be found with high probability and this distinguishing property is used to attack AES up to seven rounds.

B. 5-Round Distinguisher

Demirci and Selçuk improved this attack [17]. They expanded the attack one more round and under the same assumptions of [15], they observed that after five rounds, the first byte depends on 25 fixed 1-byte parameters instead of 36. In order to make an exhaustive search on these bytes, 2^{200} time complexity is needed. Therefore, this distinguisher can only work for AES-256.

C. A Meet in the Middle Attack on 7-Round AES

Attack on AES-256 can be summarized as follows:

- Considering 5-round AES as a function, first, all possible functions from the first byte before encryption to the first byte after five rounds is precomputed.
- Similar to the other attacks, one round is added before and after the distinguisher.
- The subkey blocks in both of the new rounds are guessed.
- By using the guessed subkeys, plaintext and ciphertext pairs are encrypted and decrypted one round, respectively.
- Using precomputed tables, keys are checked whether the distinguishing property is satisfied or not.

The attack needs 2^{40} chosen plaintext-ciphertext pairs which is not so many, but the critical part of the complexity is the precomputation part which is 2^{216}. Time and memory complexities are 2^{80} and 2^{218} respectively.

D. Extension to 8-Round

By guessing the last round key, 8-round AES can be broken with 2^{200} time complexity since the time complexity on 7-round attack is only 2^{80}. The attack described here can not be applied to AES-192. Demirci and Selçuk also present a time memory trade off approach in [17]. Since the complexity is dominated by the precomputation phase, this approach can be effectively applied. The results are given in Table I.

VII. Conclusion

In this paper, we try to cover all attacks on AES. The complexities of the attacks are given in Table I. None of the attacks is a real threat to AES, but these are used to understand the security margin of the number of the rounds used. The best attack for AES is time memory trade off attacks, however since they are applicable to all block ciphers we did not cover it. We plan to study deeply meet in the middle attack and algebraic attack as a future work.

TABLE I
Comparison of Attack Complexities

AES	Paper	Rou	Type	Data	Time	Memory
128	[2]	4	Squ	2^9	2^9	-
	[2]	5	Squ	2^{11}	2^{40}	-
	[2]	5	Squ	2^{32}	2^{40}	2^{32}
	[14]	5	Boo	2^{39}	2^{39}	2^{33}
	[2]	6	Squ	2^{32}	2^{72}	2^{32}
	[3]	6	Squ	2^{32}	2^{80}	2^{32}
	[4]	6	Squ	$6 \cdot 2^{32}$	2^{44}	-
	[14]	6	Boo	2^{71}	2^{71}	2^{33}
	[10]	6	ImpDif	$2^{114.5}$	2^{50}	2^{45}
	[18]	6	ImpBoo	$2^{112.2}$	$2^{112.3}$	-
	[3]	7	Squ	2^{32}	2^{208}	-
	[10]	7	ImpDif	$2^{115.5}$	2^{119}	2^{45}
	[18]	7	ImpDif	$2^{115.5}$	2^{119}	-
192	[3]	7	Squ	2^{32}	2^{184}	2^{32}
	[4]	7	Squ	$19 \cdot 2^{32}$	2^{155}	-
	[9]	7	ImpDif	2^{92}	2^{186}	2^{157}
	[10]	7	ImpDif	2^{92}	2^{162}	-
	[18]	7	ImpDif	$2^{91.2}$	$2^{145.5}$	-
	[12]	7	ImpDif	$2^{94.5}$	2^{157}	2^{129}
	[17]	7	MitM	2^{32}	2^{80}	2^{217}
	[17]	7	MitM-TM	2^{33+n}	2^{82+n}	2^{217-n}
	[4]	8	Squ	$2^{128} - 2^{119}$	2^{188}	-
256	[3]	7	Squ	2^{32}	2^{200}	2^{32}
	[4]	7	Squ	$19 \cdot 2^{32}$	2^{172}	-
	[17]	7	MitM	2^{32}	2^{80}	2^{218}
	[17]	7	MitM-TM	2^{34+n}	2^{82+n}	2^{218-n}
	[4]	8	Squ	$2^{128} - 2^{119}$	2^{204}	-
	[18]	7	ImpBoo	$2^{112.8}$	$2^{186.9}$	-
	[10]	8	ImpDif	$2^{166.5}$	$2^{247.5}$	-
	[18]	8	ImpDif	2^{89}	$2^{247.5}$	-
	[17]	8	MitM	2^{32}	2^{208}	2^{216}
	[17]	8	MitM-TM	2^{34+n}	2^{210+n}	2^{216-n}
	[12]	8	ImpDif	2^{101}	2^{228}	2^{201}

References

[1] J. Daemen, L. Knudsen and V. Rijmen. *The Block Cipher Square*. Fast Software Encryption '97, pp. 149-165. Springer-Verlag, 1997.
[2] J. Daemen and V. Rijmen, *AES Proposal: Rijndael*, Second Version, AES submission.
[3] S. Lucks, *Attacking Seven Rounds of Rijndael under 192-bit and 256-bit keys*. The Third Advanced Encryption Standard Candidate Conferance, pp. 215-229. NIST April 2000.
[4] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner and D. Whiting, *Improved Cryptanalysis of Rijndael*, Fast Software Encryption 2000, volume 1978 of Lecture Notes in Computer Science, pp. 213-230, Springer-Verlag 2001
[5] E. Biham, N. Keller, *Cryptanalysis of Reduced Variants of Rijndael*, 3rd AES Conference, 2000.
[6] J.H. Cheon, M. Kim, K. Kim, J-Y. Lee, S. Kang, *Improved Impossible Differential Cryptanalysis of Rijndael and Crypton*, in: ICISC 2001, LNCS, vol.2288, pp. 39-49, Springer-Verlag.
[7] R.C.-W. Phan, M.U. Siddiqi, *Generalized Impossible Differentials of Advanced Encryption Standard*, Electronics Letters 37 (14)(2001), pp. 896-898.
[8] R.C.-W. Phan, *Classes of Impossible Differentials of Advanced Encryption Standard*, Electronics Letters 38 (11)(2002), pp. 508-510.
[9] R.C.-W. Phan, *Impossible Differential Cryptanalysis of 7-round AES*, Information Processing Letters 91 (1)(2004), pp. 29-32.
[10] W. Zhang, W. Wu, D. Feng, *New Results on Impossible Differential Cryptanalysis of Reduced AES*, in: ICISC 2007, LNCS, vol.4817, pp. 239-250, Springer-Verlag.
[11] B. Bahrak, M.R. Aref, *Impossible Differential Attack on Seven-Round AES-128*, IET.Inf.Secur., 2008, Vol.2, No.2, pp. 28-32.
[12] J.Chen, Y. Hu, Y. Zhang, *Impossible Differential Cryptanalysis of Advanced Encryption Standard*, Science in China Series F:Information Sciences, 2007, vol.50, No.3, pp.342-350.
[13] D. Wagner, *The Boomerang Attack*, FSE'99, LNCS vol.1636 , pp. 156-170, Springer-Verlag, 1999
[14] A. Biryukov, *The Boomerang Attack on 5 and 6-Round Reduced AES-128*, FSE'99, LNCS vol. 4593, Springer-Verlag, 2007.
[15] H. Gilbert, M. Minier *A collision Attack on 7 Rounds of Rijndael*, 3rd AES Conference, 2000
[16] N.T. Courtois, J. Pieprzyk *Cryptanalysis of block ciphers with overdefined system of equations*, in
ASIACRYPT 2002 volume 2501 of LNCS, pages 267-287. Springer-Verlag, 2002.
[17] H. Demirci, A. A. Selçuk *A Meet-in-the-Middle Attack on 8-round AES*, in FSE 2008
[18] J. Lu, *Cryptanalysis of Block Ciphers* Ph.D. Thesis , 2008.