Improved Single-Key Attacks on 9-Round AES-192/256

Leibo Li[1], Keting Jia[2] and **Xiaoyun Wang**[1,3]

[1]Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, China

[2]Department of Computer Science and Technology, Tsinghua University, China

[3]Institute for Advanced Study, Tsinghua University,China

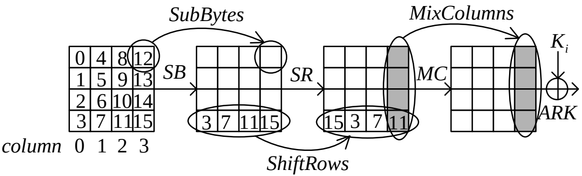
Fast Software Encryption 2014

Outline

Outline

A Brief Description of AES

- Designed by Daemen and Rijmen in 1997
- Selected as the Advanced Encryption Standard (AES) in 2001 by NIST
- AES is a 128-bit block cipher with SPN structure
- Rounds: 10 rounds for AES-128, 12 rounds for AES-192, 14 rounds for AES-256
- The round function:

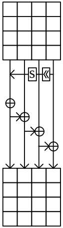


A Brief Description of AES

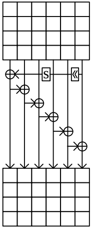
The key schedule of AES:

- For $i = N_k$ to $4 \times N_r + 3$ do the following:
  - If $i \equiv 0 \bmod N_k$, then
    $w[i] = w[i - N_k] \oplus SB(w[i-1] \lll 8) \oplus Rcon[i/N_k]$,
  - else if $N_k = 8$ and $i \equiv 4 \bmod 8$, then
    $w[i] = w[i - N_k] \oplus SB(w[i-1])$,
  - Otherwise $w[i] = w[i - N_k] \oplus w[i-1]$.

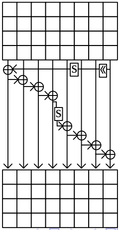
N_r is the number of rounds. N_k is the number of the words for master key, for AES-192, $N_k = 6$.



$AES-128$



$AES-192$



$AES-256$

Outline

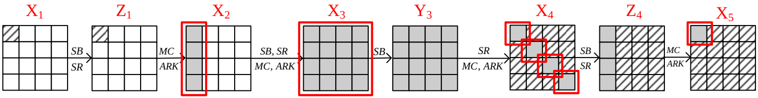
MITM Attacks on AES

- The MITM attack on AES introduced by Demirci and Selçuk at FSE 2008 to improve the collision attack proposed by Gilbert and Minier.
- Dunkelman, Keller and Shamir exploited the differential enumeration and multiset ideas to reduce the high memory complexity at ASIACRYPT 2010.
- Derbez and Fouque give a way to automatically model SPN block cipher and meet-in-the-middle attacks on AES at FSE 2013.
- Derbez, Fouque and Jean further improved Dunkelman et al.'s attack using the rebound-like idea to reduce the complexity at EUROCRYPT 2013.

Demirci and Selçuk attack (FSE 2008)

Divide the cipher E as $E_K = E^2_{K_2} \circ E^m \circ E^1_{K_1}$
Built a distinguisher in E^m

- Let $X_1[0]$ be the input variable and the output $X_5[0]$ are determined by 200-bit variable $X_2[0,1,2,3] \| X_3[0,\cdots,15] \| X_4[0,5,10,15] \| X_5[0]$.
- For X_1, construct a $\delta-$set, where $X_1[0]$ is the active bytes.
- There are 2^{200} values for 2048-bit sequence $E_m(X^0)[5] \| \cdots \| E_m(X^{255})[5]$

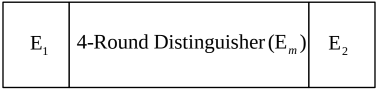


$\delta-$**set**$=(X^0,\cdots,X^{255})$, where there is a bytes traversing all values (**active byte**) and the other bytes are the same.

Demirci and Selçuk attack (FSE 2008)

The attack procedure:

1. Precomputation phase: compute all 2^{200} values $E_m(X^0)[5]\|\cdots\|E_m(X^{255})[5]$, and store them in a hash table.
2. Online phase:
   2.1 Guess values of the related subkeys in E_1, and construct a δ-set. Then partially decrypt to get the corresponding 256 plaintexts.
   2.2 Obtain the corresponding plaintext-ciphertext pairs from the collection data. Then guess the related subkeys in E_2, and partially decrypt the ciphertexts to get the corresponding 256-byte value of the output sequence of E_m.
   2.3 If a sequence value lies in the precomputation table, the guessed related subkeys in E_1 and E_2 may be right key.



Dunkelman *et al.*'s Attack (Asiacrypt 2010)

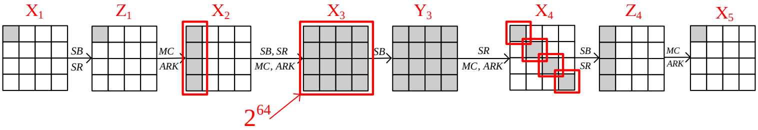
The number of the values of parameter $\mathcal{V}$ is reduced to 2^{128}

1. Use the multiset of $\Delta X_5[1]$ to replace the ordered sequence. $X_5[1]$ is not used for the multiset:

$$\{E_m(X^0)[5] \oplus E_m(X^0)[5], E_m(X^0)[5] \oplus E_m(X^1)[5], \cdots, E_m(X^0)[5] \oplus E_m(X^{255})[5]\}$$

2. Apply the differential enumeration technique to fix some values of intermediate parameters.
   - 2^{64} values for $X_3[0, .. \cdots, 15]$

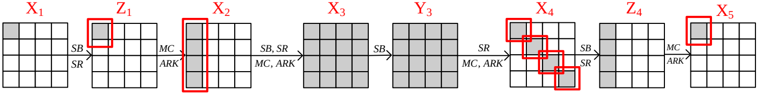
A step to find a pair satisfying the truncated differential is added, and the $\delta-$set is constructed only for such pair.



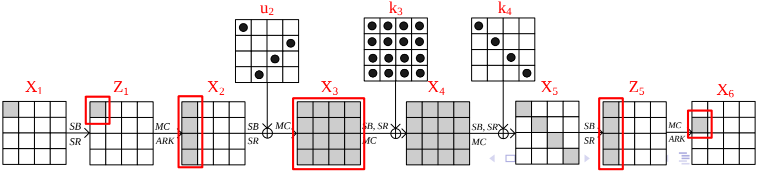
Derbez *et al.*'s Attack (Eurocrypt 2013)

- When $\Delta X_1[1] \neq 0, \Delta X_1[j] = 0, j = 2, \ldots, 15$. $\Delta X_5[1]$ is determined by 10-byte variable

$$\Delta Z_1[0] \| X_2[0,1,2,3] \| \Delta X_5[0] \| Z_4[0,1,2,3].$$



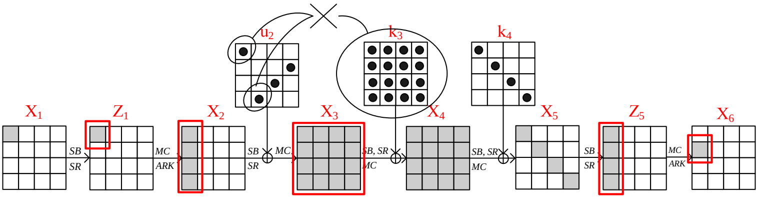
- They proposed to use a 5-round distinguisher to attack 9-round AES-256, where the value of multiset is determined by 26-byte parameters (2^{208} values).



Outline

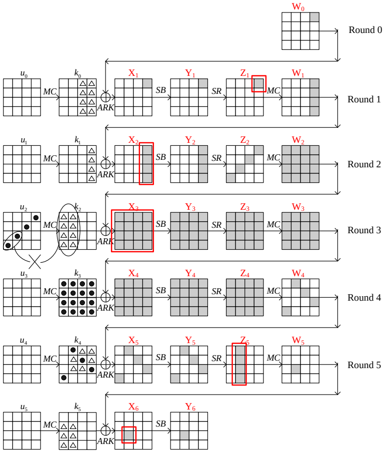
Key-Dependent Sieve

- Apply key relationship to filter the wrong states of multiset.
  - $u_2[0,7,10,13] \| k_3[0,\cdots,15] \| k_4[0,5,10,15]$ is deduced for every sequence.
  - $u_2[0] = MC^{-1}((S(k_3[4 \sim 7]) \lll 8) \oplus k_3[8 \sim 11] \oplus Rcon)[0]$.
  - $u_2[7] = MC^{-1}(k_3[8,9,10,11] \oplus k_3[12,13,14,15])[7]$.
- For AES-192, there are only about 2^{192} $(\frac{2^{208}}{2^{16}})$ values of multiset.



5-Round Distinguisher of AES-192

The truncated differential characteristic of our distinguisher.



5-Round Distinguisher of AES-192

Proposition 1. Consider the encryption of the first 2^5 values $(W_0^0, \cdots, W_0^{31})$ of the $\delta-$set through 5-round AES-192, in the case of that a message pair (W_0, W_0') of the $\delta-$set conforms to the truncated differential characteristic outlined in Fig. 3, then the corresponding 256-bit ordered sequence $Y_6^0[6] \| \cdots \| Y_6^{31}[6]$ only takes about 2^{192} values (out of 2^{256} theoretically value).

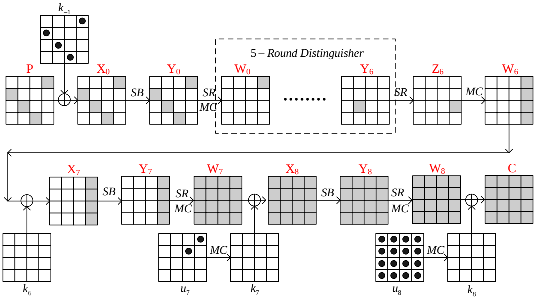
Our improvements:

- Propose a 5-round distinguisher for AES-192.
- Deduce more information of subkeys: $k_0[12], k_1[12, 13, 14, 15], u_2[3, 6, 9, 12], k_3[0, \cdots, 15], k_4[3, 4, 9, 14], k_5[6]$.
- Use an ordered sequence instead of the multiset.

Outline

The Key Recovery Attack on 9-Round AES-192

The attack is mounted by adding one round on the top and three rounds on the bottom of the 5-round distinguisher.



The Key Recovery Attack on 9-Round AES-192

The attack procedure:

1. Precomputation phase: Get 2^{192} 256-bit sequences described in Proposition 1.
2. Online phase:
   2.1 Encrypt 2^{81} structures of 2^{32} plaintexts, and collect 2^{144} pairs.
   2.2 For each pair, guess the difference $\Delta Y_7[12, 13, 14, 15]$ and deduce the subkey $u_7[3, 6, 9, 12] \| u_8$.
   2.3 Guess the difference $\Delta W_0[12]$, and deduce $k_{-1}[1, 6, 11, 12]$.
3. Construct the δ-set and get the corresponding sequence $Y_6^0[6] \| \cdots \| Y_6^{31}[6]$. Check whether the sequence lies in precomputation table.

The Key Recovery Attack on 9-Round AES-192

The complexities of the attack:

1. Precomputation phase: The time complexity of this phase is about $2^{192} \times 2^5 \times 2^{-2.2} = 2^{194.8}$ 9-round AES encryptions, the memory complexity is about 2^{193} 128-bit words.
2. Online phase: The time complexity of this phase is equivalent to $2^{144} \times 2^{32} \times 2^5 \times 2^{-2.6} = 2^{178.4}$ 9-round encryptions. The data complexity is about 2^{113} chosen plaintexts.

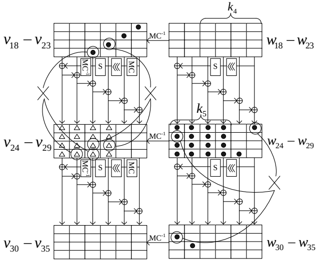
Data/time/memory tradeoff: Only precompute a fraction 2^{-8} of possible sequences, and repeat the attack 2^8 times in the online phase. Then the data complexity is 2^{121} chosen plaintexts. Time complexity, including the precomputation phase, is approximately $2^{187.5}$. The memory complexity reduces to $2^{193 \times 2^{-8}} = 2^{185}$.

Outline

The Attack on 9-round AES-192 from the Third Round

There are only about $\frac{2^{208}}{2^{24}} = 2^{184}$ possible sequences for 5-round distinguisher starting from 3-rd round

- $u_4[3,6,9,12] \| k_5[0,\cdots,15] \| k_6[3,4,9,14]$ is deduced for each sequence
- $u_4[3] = (MC^{-1}k_5)[7] \oplus (MC^{-1}k_5)[11]$
- $u_4[6] = (MC^{-1}k_5)[10] \oplus (MC^{-1}k_5)[14]$
- $k_6[9] = k_5[1] \oplus S(k_6[9]) \oplus Rcon$



Reducing the Memory Complexity with Weak-Key Attacks

- There exists a subkey k' for every sequence in precomputation table.
- There exist some linear relations in k' and guessed subkey in the online phase $(\widehat{k})$, i.e., there exist $\widetilde{k} \subset (k' \cap \widehat{k})$.
- The precomputation table could be split into 2^m sub-tables with the index of m bit value $\widetilde{k}$.
- The sequences computed in the online phase could also be split into 2^m subsets with the same index $\widetilde{k}$.
- The whole attack could be sorted into 2^m weak-key attacks. Each weak-key attack contains a sub-table of precomputation, and all of these attacks are independent each other.
- If all weak-key attacks are worked in the streaming model, the memory complexity could be reduced by 2^m times.

Outline

Reducing the Complexities of the Attacks on AES-192

- Use 8-bit information $k_{-1}[6]$ as the index to split the attack to 2^8 weak-key attacks, where

$$k_{-1}[6] = SB(k_3[1] \oplus k_3[5]) \oplus k_3[10] \oplus k_3[14] \oplus Rcon[2][2].$$

- The memory complexity could be reduced to 2^{177} 128-bit words.
- For the attack starting from the third round, use the 16-bit information $k_1[6, 11]$ to split the attack, and the memory complexity reduce to $2^{165.5}$.
  - $k_1[6] = k_5[2] \oplus k_5[6] \oplus k_5[14]$
  - $k_1[11] = k_5[7] \oplus k_5[11] \oplus k_6[3]$

Outline

Reducing the Complexities of the Attack on AES-256

Our improvements:

- Propose a new distinguisher which only compute 32 values of the $\delta-$set.
- Use the 32-bit subkey $k_{-1}[10, 15]$ and $k_4[9, 14]$ to split the attack.
- The memory complexity is only about $2^{169.9}$ 128-bit words. Note that Derbez *et al.* attack (Eurocrpyt 2013) needs about 2^{203} 128-bit words.

Conclusion

Our contribution in this paper:

- Proposed to use the subkeys involved in distinguisher as the filter conditions to reduce the size of precomputation table.
- Constructed a 5-round distinguisher of AES-192 and mounted an attack on 9-round AES-192.
- Showed that the whole attack is able to be sorted into a series of weak-key attacks, then reduce the memory complexity of the attack.

Conclusion

Our results and some major previous results.

Cipher	Rounds	Attack Type	Data	Time	Memory	Source
AES-192	8	MITM	2^{113}	2^{172}	2^{129}	[DKS Asiacrypt 2010]
	8	MITM	2^{113}	2^{172}	2^{82}	[DFG Eurocrypt 2013]
	8	MITM	2^{113}	2^{140}	2^{130}	[DFG FSE 2013]
	9	Bicliques	2^{80}	$2^{188.8}$	2^{8}	[BKR Asiacrypt 2011]
	9	MITM	2^{121}	$2^{186.5}$	$2^{177.5}$	this paper
	9 (3-11)	MITM	2^{117}	$2^{182.5}$	$2^{165.5}$	this paper
	Full	Bicliques	2^{80}	$2^{189.4}$	2^{8}	[BKR Asiacrypt 2011]
AES-256	8	MITM	2^{113}	2^{196}	2^{129}	[DKS Asiacrypt 2010]
	8	MITM	2^{113}	2^{196}	2^{82}	[DFG Eurocrypt 2013]
	8	MITM	$2^{102.83}$	2^{156}	$2^{140.17}$	[DFG FSE 2013]
	9	Bicliques	2^{120}	$2^{251.9}$	2^{8}	[BKR Asiacrypt 2011]
	9	MITM	2^{120}	2^{203}	2^{203}	[DFG Eurocrypt 2013]
	9	MITM	2^{121}	$2^{203.5}$	$2^{169.9}$	this paper
	Full	Bicliques	2^{40}	$2^{254.4}$	2^{8}	[BKR Asiacrypt 2011]

Questions?

Thank you for your attentions!