

Analysis of a 7-Round Cryptanalytic Attack

Riya Jana

August 28, 2025

This document summarizes the complexity of a specific cryptanalytic attack, likely an impossible differential attack, on a 7-round version of the AES block cipher. The attack's requirements are broken down into three primary metrics: data, time, and memory.

1 The Structure Technique

A structure is a set of 2^{32} chosen plaintexts. These plaintexts are generated for a fixed 12-byte constant C , while the remaining bytes (represented by A) are varied. The specific form given in the text is:

$$X = (A, C, C, C, C, A, C, C, C, C, A, C, C, C, C, A)$$

By varying the 12-byte constant C , up to 2^{96} such structures can be constructed, but later on we optimize number of structures.

$$\binom{2^{32}}{2} \approx 2^{63}$$

For each structure, 2^{63} plaintext pairs can be generated.

2 Data Collection and Queries

The total number of plaintext pairs is determined by the number of structures, denoted as 2^N , and the number of pairs per structure (2^{63}). The total number of pairs is 2^{N+63} .

To generate these pairs, the attacker only needs to make 2^{N+32} queries to the encryption oracle. This is because each structure requires 2^{32} queries ($2^N \times 2^{32} = 2^{N+32}$). The value of N is optimized to balance the data collection against the computational cost of the entire attack.

3 Probability and Useful Pairs

The attack requires the plaintext pairs to have a specific ciphertext difference, ΔC , where 8 of the 16 bytes (or 64 bits) must have a zero difference.

The probability of a randomly chosen pair satisfying this condition is 2^{-64} , as each of the 64 bits must be zero. The number of "useful" pairs that actually

satisfy the required difference is calculated by multiplying the total number of pairs by this probability:

$$\text{Useful Pairs} = 2^{N+63} \times 2^{-64} = 2^{N-1}$$

These 2^{N-1} pairs are then used in the next stage of the attack for key recovery. the process of key space reduction in a cryptanalytic attack by using wrong key suggestions. The goal is to eliminate incorrect key candidates to find the single correct subkey.

4 Generating and Filtering Wrong Key Suggestions

The attack generates wrong key suggestions for a 14-byte (112-bit) subkey space.

- A total of 2^{N-1} "useful" pairs are obtained from a prior step.
- A lookup table, T , contains 2^{36} entries.
- The total number of wrong key suggestions is the product of these two numbers:

$$2^{N-1} \times 2^{36} = 2^{N+35}$$

- The total number of possible 112-bit subkeys is 2^{112} . The attack's objective is to reduce this space to a single key.

The size of the remaining key space is modeled by the following equation, which represents the probability of a key not being suggested as a wrong key:

$$\text{Remaining Keys} = 2^{112} \cdot \left(1 - \frac{1}{2^{112}}\right)^{2^{N+35}} \quad (1)$$

This expression approximates to $2^{112} \cdot \left(\frac{1}{2^{112}}\right)^{2^{112} \cdot 2^{N-77}}$, which further simplifies to $2^{112} \cdot \left(\frac{1}{e}\right)^{2^{N-77}}$, and finally to:

$$2^{112-2^{N-77}} \quad (2)$$

5 Determining the Optimal Number of Structures (N)

To ensure the attack is successful, the value of N (where 2^N is the number of structures) must be chosen carefully to reduce the remaining key space to 1.

5.1 Case 1: $N = 83$

If $N = 83$, the size of the remaining key space is:

$$2^{112-2^{83-77}} = 2^{112-2^6} = 2^{112-64} = 2^{48}$$

This result is still a very large number of keys, meaning the attack would fail.

5.2 Case 2: $N = 84$

If $N = 84$, the size of the remaining key space is:

$$2^{112-2^{84-77}} = 2^{112-2^7} = 2^{112-128} = 2^{-16}$$

A result of less than 1 indicates that the key space is effectively reduced to a single key, with a high probability of success.

6 Conclusion

The proper choice for the number of structures is $N = 84$. Therefore, the attack must generate 2^{84} structures to successfully recover the 112-bit subkey.

7 Attack Complexity Metrics

7.1 Data Complexity

The data complexity refers to the total number of plaintexts required to execute the attack.

- The attack leverages 2^{84} "structures," where each structure is a collection of related plaintexts.
- Each structure necessitates queries of 2^{32} chosen plaintexts.
- The total data complexity is calculated as the product of the number of structures and the plaintexts per structure:

$$\text{Data Complexity} = 2^{84} \times 2^{32} = 2^{116} \text{ chosen plaintexts.}$$

7.2 Time Complexity

The time complexity represents the total computational effort required to carry out the attack.

- The main computational cost is processing the 2^{116} ciphertexts received from the encryption oracle.
- The cost to generate a look-up table is around 2^{36} computations, which is considered negligible.

- The core of the attack involves deriving wrong key suggestions. The attack generates 2^{119} such suggestions.
- Each wrong key suggestion costs approximately $\frac{3}{7}$ of a full 7-round AES computation.
- The total time cost, which is the computational bottleneck, is less than 2^{118} 7-round AES computations, calculated as:

$$\text{Time Cost} < 2^{119} \times \frac{3}{7} \approx 2^{118} \text{ 7-round AES computations.}$$

7.3 Memory Complexity

The memory complexity is the amount of storage required for the attack.

- The largest memory requirement is for tracking a 112-bit subkey space.
- The attack requires memory to record the validity or invalidity of each of the 2^{112} possible subkey values.
- This storage requires 2^{112} .

7.4 Summary

In summary, the complexities for recovering the 112-bit subkey are:

- **Data:** 2^{116} chosen plaintexts
- **Time:** 2^{118} 7-round AES computations
- **Memory:** 2^{112} 128-bit state values