Simplified AES Under Attack: A Peer into Differential Cryptanalysis

Aiden Rivera

December 2, 2024

Contents

1 Introduction **2**

2 Research Objectives **2**
2.1 Analyze Differential Properties 2
2.2 Evaluate the Practicality of Differential Cryptanalysis 2
2.3 Understand the Latent Cryptographic Weaknesses 2

3 Key Elements **3**
3.1 Objectives 3
3.2 Methodology 3
3.3 Findings 3

1 Introduction

Simplified AES (S-AES) is a lightweight version of the Advanced Encryption Standard (AES) designed for educational purposes. Despite its simplicity, S-AES retains the fundamental structure of AES, including the substitution-permutation network, and provides a practical framework for studying cryptographic concepts. My research explores the application of differential cryptanalysis, a prominent method for analyzing block ciphers, to the S-AES cipher.

To contextualize the attack, I implemented a two-round version of S-AES encryption and decryption in software and studied the statistical properties of differential propagation through its structure. Differential cryptanalysis leverages high-probability differences in plaintexts and their resulting ciphertexts to deduce parts of the secret key. While this technique is powerful against many lightweight ciphers, the limited 16-bit keyspace of S-AES makes brute-force attacks computationally trivial in practice. As a result, differential cryptanalysis is more of an analytical tool for understanding this particular cipher's weaknesses rather than a practical method for key recovery.

2 Research Objectives

The primary objective of this research is to investigate the feasibility and effectiveness of applying differential cryptanalysis to S-AES. Specifically, the study aims to:

2.1 Analyze Differential Properties

Examine the propagation of input differences through the two-round S-AES encryption process to identify statistical patterns that can reveal key information.

2.2 Evaluate the Practicality of Differential Cryptanalysis

Assess the computational requirements of differential cryptanalysis when applied to S-AES, particularly in comparison to a brute-force approach, given the cipher's small 16-bit keyspace.

2.3 Understand the Latent Cryptographic Weaknesses

Explore the structural vulnerabilities in S-AES that make it susceptible to differential cryptanalysis, providing insights into how differential attacks exploit the cipher's design.

3 Key Elements

The main takeaways of my research lie in the following objectives, methodologies and findings.

3.1 Objectives

- **Investigate Differential Cryptanalysis:** Analyze how differential cryptanalysis applies to the S-AES cipher, focusing on the propagation of plaintext differences through its structure.
- **Compare Cryptanalysis and Brute Force:** Evaluate the practicality of differential cryptanalysis versus brute force for breaking S-AES's small 16-bit keyspace.

3.2 Methodology

- **Implementation of S-AES:** Developed a two-round implementation of S-AES encryption and decryption to understand its internal mechanics and to simulate key recovery experiments.
- **Study of Differential Properties:** Researched how input differences propagate through the S-boxes, shift rows, and MixColumns transformations of S-AES, building a theoretical basis for differential attacks.
- **Statistical Analysis of Differentials:** Examined differential distribution tables to identify high-probability input-output pairs that could be used to deduce key information.
- **Theoretical Key Recovery:** Outlined the process of using differential pairs to reduce the key search space, though this was not implemented, as brute-force key search was computationally cheaper.

3.3 Findings

- **Feasibility of Differential Cryptanalysis:** Differential cryptanalysis is theoretically applicable to S-AES, but not practical. The small 16-bit keyspace of S-AES renders brute-force attacks significantly faster and more practical than implementing a full differential attack.