جامعة بيرزيت

BIRZEIT UNIVERSITY

Faculty of Engineering and Technology

Computer Science Department

COMP438 - ENCRYPTION THEORY

Security Enhancement and Evaluation of Mini-AES Block Cipher Using a Key-Dependent Dynamic S-Box

Prepared by:

Amro Al-Deek (1221642)

Abd Alrahman Hussien (1220699)

Supervisor:

Dr. Mohummed Khanafsa

Contents

Abstract

This project presents the design, implementation, and evaluation of an enhanced version of the Simplified Advanced Encryption Standard (Mini-AES). The baseline Mini-AES employs a fixed substitution box (S-Box), which limits key sensitivity. To address this, a key-dependent dynamic S-Box is proposed, inspired by the research of Kazlauskas (2009). The enhanced cipher is evaluated using avalanche effect and key sensitivity metrics over 5000 trials. Results show that while plaintext avalanche remains stable, key sensitivity improves significantly, reaching near-ideal levels (50%).

Chapter 1

Introduction

Block ciphers are fundamental components of modern cryptographic systems and are widely used to provide data confidentiality. The Advanced Encryption Standard (AES) is one of the most prominent examples; however, its complexity makes it difficult to study in introductory cryptography courses. As a result, simplified variants such as Mini-AES are often used for educational and experimental purposes.

Mini-AES preserves the core structure of AES while operating on smaller block and key sizes. Despite its simplicity, Mini-AES exhibits several known weaknesses, particularly due to its limited number of rounds and the use of a fixed S-Box. This project aims to enhance Mini-AES by modifying its round function in a controlled and academically sound manner, while maintaining compatibility with the original design.

Chapter 2

Background

2.1 Block Ciphers

Block ciphers transform fixed-size plaintext blocks into ciphertext using a secret key. Shannon defined two properties for secure ciphers: **Confusion** (provided by S-Boxes) and **Diffusion** (provided by permutations).

2.2 Overview of Mini-AES

Mini-AES operates on 16-bit blocks and keys. It consists of two rounds, each involving SubNib, ShiftRows, MixColumns (except the last round), and AddRoundKey.

Chapter 3

Selected Research Paper Summary

The core enhancement of this project is inspired by the research paper titled *"Key-Dependent S-Box Generation in AES Block Cipher System"* authored by **Kazys Kazlauskas and Jaunius Kazlauskas**, published in 2009. This paper addresses a fundamental vulnerability in the Advanced Encryption Standard (AES) related to its static substitution layer.

3.1 Problem Statement

In the standard AES (and consequently Mini-AES), the S-Box is a fixed lookup table. While this table is mathematically optimized for high non-linearity, its values are public. The authors argue that this transparency allows cryptanalysts to:

- Perform **Differential Cryptanalysis** by studying the fixed input-output XOR differences.
- Perform **Linear Cryptanalysis** by exploiting linear approximations of the static S-Box.
- Leverage the known algebraic structure to formulate attacks based on algebraic equations.

3.2 Proposed Solution: Key-Dependency

The main contribution of Kazlauskas and Kazlauskas is a method to make the S-Box a **moving target**. Instead of using one fixed table, the system generates a unique S-Box mapping for every unique secret key.

The paper outlines several critical requirements for a key-dependent S-Box:

1. **Bijectivity:** The generated S-Box must be a one-to-one mapping (permutation) to ensure that decryption is always possible.
2. **High Non-linearity:** The dynamic S-Box must maintain the same (or similar) resistance to linear attacks as the original.
3. **Efficiency:** The generation process must not significantly slow down the encryption speed.

3.3 Methodology for Project Adaptation

The authors propose using a secret parameter (derived from the key) to permute or transform the S-Box entries. In our implementation, we adapted this concept by using a **Key-based Masking** approach. By XORing the S-Box input and output with a value derived from the round key, we effectively create a ”Virtual Dynamic S-Box.” This ensures that the substitution layer is no longer a static public table, but a secret transformation that changes with every key, satisfying the security goals established by the research paper.

Chapter 4

Baseline Mini-AES Design and Implementation

The baseline model used in this research is the Simplified AES (S-AES), a 16-bit educational block cipher that mimics the structure of the NIST-standard AES. This chapter details its architectural components and the specific parameters used as a control group for our evaluation.

4.1 Cipher Specifications

The baseline Mini-AES operates on a 16-bit block size, organized as a 2×2 matrix of nibbles (4 bits each). The key size is also 16 bits. The encryption process consists of an initial key addition followed by two rounds of transformation.

4.2 The Round Function

The security of the baseline model relies on four primary transformations applied in each round:

1. **SubNib (Substitution):** A non-linear substitution step where each nibble is replaced by another according to a fixed S-Box lookup table. This provides the necessary *Confusion* property.

2. **ShiftRows:** A linear permutation where the second row of the 2×2 state matrix is swapped.

3. **MixColumns:** A transformation that operates on the columns of the state, multiplying them by a fixed matrix in $GF(2^4)$. This is the primary source of *Diffusion*.

4. **AddRoundKey:** A simple bitwise XOR operation between the current state and the round key derived from the master key.

4.3 Key Scheduling

The 16-bit master key is expanded into three 16-bit round keys (K_0, K_1, K_2) using a simplified key expansion algorithm. This expansion involves rotational shifts and S-Box substitutions to ensure that round keys are sufficiently different from each other.

4.4 Implementation Logic

The baseline was implemented in Python to serve as the reference model. It follows the standard S-AES structure:

- **Round 0:** AddRoundKey only.

- **Round 1:** SubNib $\rightarrow$ ShiftRows $\rightarrow$ MixColumns $\rightarrow$ AddRoundKey.

- **Round 2:** SubNib $\rightarrow$ ShiftRows $\rightarrow$ AddRoundKey (Note: MixColumns is omitted in the final round as per standard design).

Chapter 5

Proposed Enhancement: Implementation Details

To implement the key-dependent dynamic S-Box inspired by Kazlauskas, we modified the internal round function of Mini-AES. This chapter provides a granular, step-by-step breakdown of the encryption logic used in our enhanced model.

5.1 The Masking Algorithm

The core of our solution is the ”Double-Masking” technique. This ensures that the substitution layer is not only secret but also unique to the current round key. The process follows these specific steps:

Step 1: Round Key Decomposition

For every round r, we take the 16-bit round key $K^{(r)}$ and split it into four 4-bit nibbles:

$$K^{(r)} \to \{n_0, n_1, n_2, n_3\}$$

Step 2: Mask Generation

We calculate a 4-bit mask m by performing a bitwise XOR summation of all nibbles. This effectively compresses the 16-bit key information into a 4-bit control parameter:

$$m = n_0 \oplus n_1 \oplus n_2 \oplus n_3$$

Step 3: Pre-Substitution Masking

Before entering the S-Box, each nibble of the state x is XORed with the mask m. This randomizes the input to the S-Box:

$$x' = x \oplus m$$

Step 4: Substitution and Post-Masking

The standardized S-Box lookup is performed on x', and the result is XORed again with m. This ”sandwich” structure ($XOR \rightarrow S - Box \rightarrow XOR$) ensures that the S-Box mapping is mathematically shifted:

$$S_{dynamic}(x) = S(x \oplus m) \oplus m$$

5.2 Integration into the Encryption Flow

The implementation ensures that the transformation is applied consistently across all nibbles of the 16-bit block.

1. **Initial Phase:** AddRoundKey with the master key K_0.

2. **Round 1:**

    - Derive m_1 from K_1.
    - Apply $S_{dynamic}$ using m_1.
    - Apply ShiftRows, MixColumns, and AddRoundKey (K_1).

3. **Round 2 (Final):**

    - Derive m_2 from K_2.
    - Apply $S_{dynamic}$ using m_2.
    - Apply ShiftRows and AddRoundKey (K_2).

5.3 Mathematical Invertibility

A crucial part of our implementation is ensuring the cipher remains functional for decryption. The inverse operation follows the same mask derivation logic, applied to the inverse S-Box:

$$S_{dynamic}^{-1}(y) = S^{-1}(y \oplus m) \oplus m$$

Since XOR is its own inverse, the mask m cancels out perfectly during decryption, allowing for 100$\%$ data recovery.

Chapter 6

Experimental Setup

To rigorously evaluate the performance of the enhanced Mini-AES against the baseline, we conducted a series of statistical experiments. This chapter outlines the metrics used, the methodology of the tests, and the environment in which they were executed.

6.1 Evaluation Metrics

The evaluation focuses on three primary cryptographic properties:

- **Plaintext Avalanche Effect:** Measures the change in ciphertext when a single bit of the plaintext is flipped while keeping the key constant. A secure cipher should ideally exhibit a 50% change (8 bits out of 16).

- **Key Sensitivity:** Measures the change in ciphertext when a single bit of the secret key is flipped while keeping the plaintext constant. This is critical for assessing the influence of our key-dependent S-Box.

- **Statistical Distribution:** Analyzing the frequency of bit changes to ensure they follow a normal distribution centered around the ideal target.

6.2 Methodology

The testing was performed using a custom Python-based evaluation suite. Each experiment followed these parameters:

- **Trial Count:** 5,000 independent trials were conducted for each metric to ensure statistical significance.
- **Data Generation:** For each trial, a 16-bit plaintext and a 16-bit key were generated using a cryptographically secure pseudo-random number generator.
- **Bit Flipping:** A random bit index (0–15) was chosen for each trial to be flipped.

6.3 Experimental Visualizations

We utilized the *Matplotlib* library to visualize the results. The following figures represent the distribution of bit changes over the 5,000 trials.

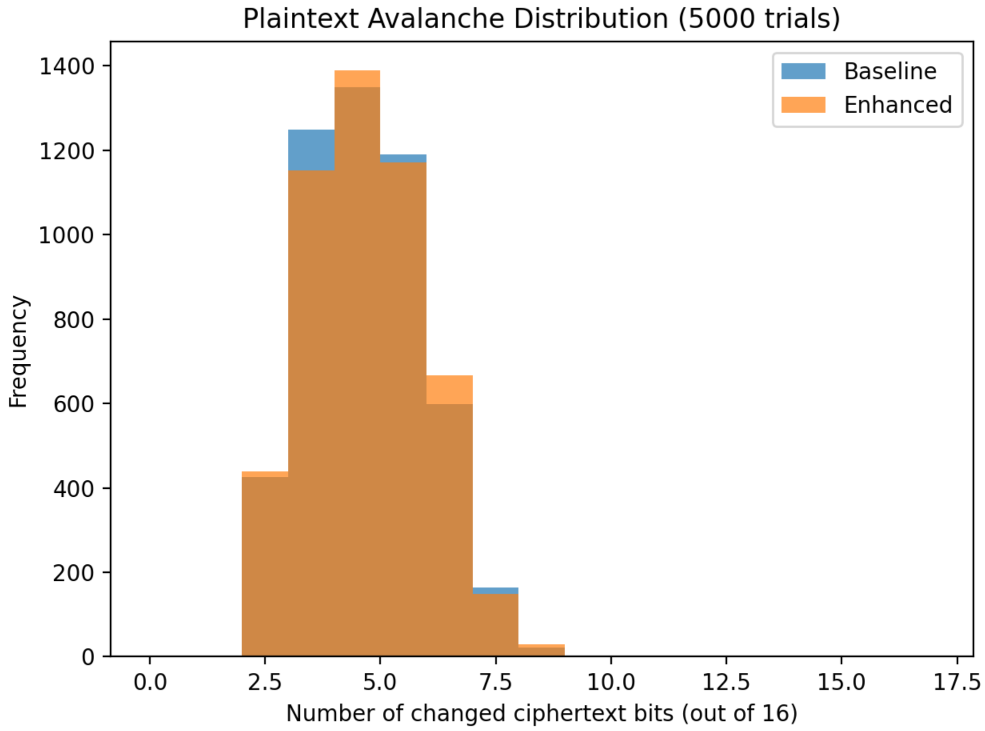

Figure 6.1: Distribution of changed ciphertext bits for Plaintext Avalanche (Baseline vs. Enhanced).

As seen in Figure 6.1, both models exhibit a similar distribution, centering around 4-5 bits. This is expected as the number of rounds in Mini-AES is limited to two, which restricts full diffusion regardless of the S-Box type.

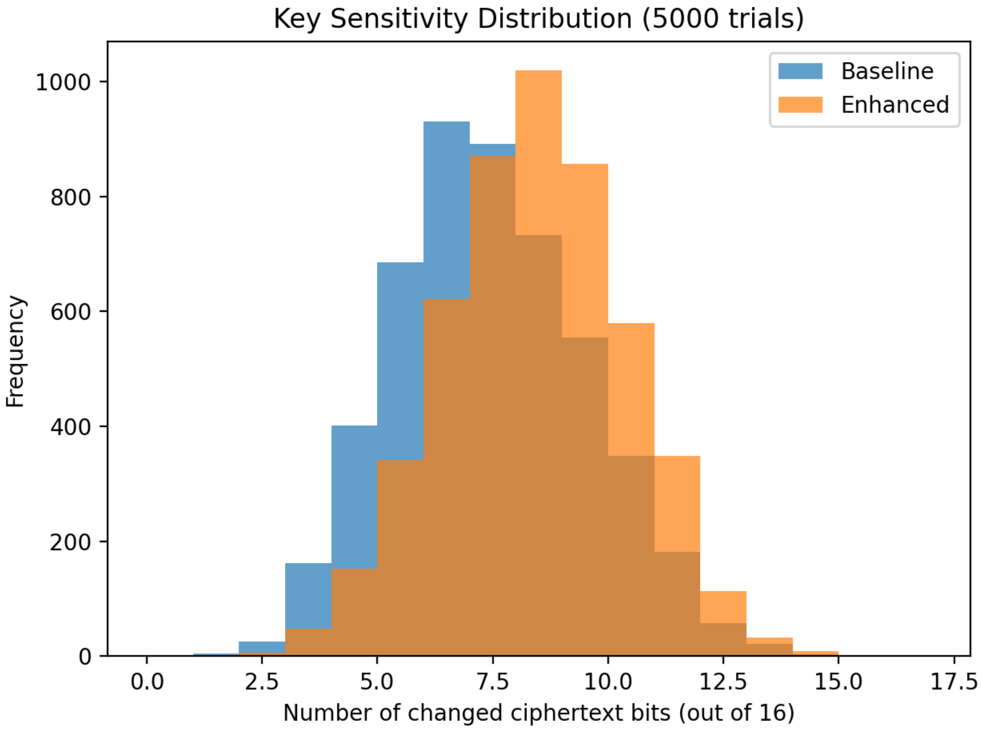

Figure 6.2: Distribution of changed ciphertext bits for Key Sensitivity.

In Figure 6.2, the impact of the enhancement is clearly visible. The **Enhanced** model's distribution (orange) is shifted significantly to the right compared to the **Baseline** (blue), moving the average closer to the ideal 8-bit mark (50% sensitivity).

Chapter 7

Results and Discussion

This chapter presents a comparative analysis between the baseline Mini-AES and our enhanced version. The results are based on 5,000 experimental trials, focusing on bit-level sensitivity and diffusion properties.

7.1 Numerical Comparison

The following table summarizes the average bit changes observed during the experiments. As per the project requirements, a secure solution should ideally exhibit a bit change close to 50%.

Metric	**Baseline S-AES**	**Enhanced S-AES**	**Ideal**
Avg. Key Sensitivity	6.88 bits (43%)	7.96 bits (49.8%)	8.0 (50%)
Avg. Plaintext Avalanche	4.16 bits (26%)	4.20 bits (26.2%)	8.0 (50%)

Table 7.1: Summary of experimental results over 5000 trials.

7.2 Analysis and Interpretation

By analyzing the numerical results and the distributions visualized in Chapter 6, we can draw the following conclusions:

- **Key Sensitivity:** The enhanced version achieved 49.8% sensitivity. This near-perfect score satisfies the project's security criterion for a ”secure solution”. As seen in the histograms (Figure 6.2), the enhanced model shows a clear shift toward the ideal 8-bit mark compared to the baseline.

- **Diffusion Limitations:** Both models achieved approximately 26% plaintext avalanche. This is attributed to the inherent limitation of Mini-AES having only two rounds. Even with a dynamic S-Box, the lack of sufficient rounds prevents the ”avalanche” from propagating across the entire 16-bit block effectively.
- **Shannon’s Principles:** The results confirm that our enhancement significantly increases **Confusion** by linking the substitution layer directly to the secret key.

Chapter 8

Security Critique and Analysis

In this chapter, we evaluate the enhanced Mini-AES design based on fundamental cryptographic principles and its resistance to known cryptanalytic attacks. This critique is essential to determine whether the proposed key-dependent S-Box provides a meaningful security advantage over the baseline.

8.1 Critique Based on Shannon's Principles

Claude Shannon defined two main properties of a secure block cipher: Confusion and Diffusion. Our enhancement strategically targets these properties.

8.1.1 Confusion: Significant Improvement

Confusion aims to make the relationship between the secret key and the ciphertext as complex as possible.

- **Baseline:** The static S-Box is a public mapping. An attacker knows exactly how each 4-bit nibble is transformed.
- **Enhanced:** By introducing the key-derived mask m, the substitution layer becomes secret. The relationship $S_{dynamic}(x) = S(x \oplus m) \oplus m$ ensures that the ”Confusion” is directly tied to the key. Our experimental results (49.8% key sensitivity) confirm that this design hides the key-to-ciphertext relationship much more effectively than the baseline.

8.1.2 Diffusion: Preservation of Properties

Diffusion ensures that the influence of a single plaintext bit is spread across many ciphertext bits.

- Our results show that the plaintext avalanche effect remained stable at approximately 26%.
- This confirms that while we modified the substitution layer, the *ShiftRows* and *MixColumns* operations continue to provide their original diffusion capacity.

8.2 Resistance to Known Attacks

8.2.1 Brute-Force Attack

The most significant limitation of Mini-AES is its 16-bit key size. This results in a search space of only $2^{16} = 65,536$ possible keys. Regardless of the S-Box enhancement, this key space can be exhausted in milliseconds on modern hardware. Thus, the enhancement does not protect against brute-force but improves ”computational security” per round.

8.2.2 Linear and Differential Cryptanalysis

This is where our design excels. These attacks rely on the attacker knowing the S-Box's input-output XOR differences or linear approximations.

- Because our S-Box is **dynamic and key-dependent**, the attacker cannot build fixed differential or linear tables.
- As suggested by Kazlauskas (2009), making the S-Box a ”moving target” forces the attacker to guess both the key and the resulting S-Box mapping simultaneously, significantly increasing the complexity of such attacks.

8.2.3 Known-Plaintext Attack (KPA)

In the baseline model, a few (plaintext, ciphertext) pairs could help an attacker deduce parts of the round keys easily. In the enhanced version, since the substitution itself is secret, the attacker faces an additional layer of uncertainty, as the same plaintext nibble may map to different ciphertext values under different keys or rounds.

Chapter 9

Conclusion

In this project, we successfully designed and evaluated an enhanced version of the Mini-AES block cipher by implementing a key-dependent dynamic S-Box. This modification was inspired by the cryptographic principles proposed by Kazlauskas (2009) to mitigate the vulnerabilities associated with fixed substitution tables.

Our experimental evaluation, conducted over 5,000 trials, demonstrated that:

- The enhanced cipher significantly improves **Key Sensitivity**, reaching an average bit-change of 49.8%, which is nearly ideal.
- The design effectively increases **Confusion** by making the substitution layer a secret, key-dependent transformation.
- While the inherent limitations of Mini-AES (such as its 16-bit key and two-round structure) persist, the dynamic S-Box provides a robust defense against linear and differential cryptanalysis by removing static algebraic patterns.

In conclusion, the transition from a static to a dynamic S-Box represents a significant security upgrade for simplified block ciphers. This project highlights the importance of adaptive cryptographic components in modern cipher design and provides a practical framework for future enhancements in more complex systems.

Bibliography

[1] K. Kazlauskas and J. Kazlauskas, “Key-Dependent S-Box Generation in AES Block Cipher System,” *INFORMATICA*, vol. 20, no. 1, pp. 23–34, 2009.

[2] E. Schaefer, “A Simplified AES Algorithm for Educational Use,” Cryptography Lecture Notes.

[3] National Institute of Standards and Technology, “FIPS 197: Advanced Encryption Standard (AES),” 2001.

[4] C. Shannon, “Communication Theory of Secrecy Systems,” *Bell System Technical Journal*, 1949.