S-box Analysis of Midori64

The Midori64 cipher is a lightweight block cipher designed for energy-efficient applications. It employs a 4-bit S-box in its substitution layer, which plays a critical role in ensuring the cipher's security. The S-box used in Midori64, along with its Differential Distribution Table (DDT), is analyzed to evaluate its resistance to differential cryptanalysis.

Midori64 S-box

The S-box used in the Midori64 cipher is shown below:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	A	D	3	E	B	F	7	8	9	1	5	0	2	4	6

Table 1: Midori64 S-box

Differential Distribution Table (DDT)

The Differential Distribution Table (DDT) of the S-box is presented below. It quantifies the probability of each output difference occurring for a given input difference.

Table 2: Differential Distribution Table (DDT)

in / out	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	2	4	-	2	2	2	-	2	-	-	-	-	-	2	-
2	-	4	-	-	4	-	-	-	-	4	-	-	4	-	-	-
3	-	-	-	-	2	-	4	2	2	2	-	-	-	2	-	2
4	-	2	4	2	2	2	-	-	2	-	-	2	-	-	-	-
5	-	2	-	-	2	-	-	4	-	2	4	-	2	-	-	-
6	-	2	-	4	-	-	-	2	2	-	-	-	2	2	-	2
7	-	-	-	2	-	4	2	-	-	-	-	2	-	4	2	-
8	-	2	-	2	2	-	2	-	-	2	-	2	2	-	2	-
9	-	-	4	2	-	2	-	-	2	2	-	2	2	-	-	-
A	-	-	-	-	-	4	-	-	-	-	4	-	-	4	-	4
B	-	-	-	-	2	-	-	2	2	2	-	4	-	2	-	2
C	-	-	4	-	-	2	2	-	2	2	-	-	2	-	2	-
D	-	-	-	2	-	-	2	4	-	-	4	2	-	-	2	-
E	-	2	-	-	-	-	-	2	2	-	-	-	2	2	4	2
F	-	-	-	2	-	-	2	-	-	-	4	2	-	-	2	4

Value Counts in the DDT:

The distribution of values in the Difference Distribution Table (DDT) is as follows:

Value	Count
0	159
2	72
4	24
16	1

Differential Distribution Table (DDT) Analysis

1. Differential Uniformity

- **Observation:** The maximum value in the DDT is 4, which is the largest count (excluding the first row). This means that the *differential uniformity* is $\Delta_{\text{max}} = 4$.
- **Conclusion:** The differential uniformity of 4 indicates that the cipher is somewhat resistant to differential cryptanalysis, but it is not as strong as S-boxes with $\Delta_{\text{max}} = 4$ (e.g., AES) which occurs only once in row. As in Midori cipher's DDT contains $\Delta_{\text{max}} = 4$ more than one for the row. However, for lightweight ciphers like Midori, this trade-off is acceptable, as it balances security with efficiency.

2. Uniform Distribution of Values

- **Observation:** The values in the DDT are relatively evenly distributed, and there are no particular input-output differential pairs that dominate the table.
- **Conclusion:** This suggests that the S-box does not have significant biases or vulnerabilities that would make it easier for attackers to exploit specific differentials. This balanced distribution enhances the cipher's resistance to differential cryptanalysis.

3. Null Entries in the DDT

- **Observation:** Several entries in the DDT are 0, which means that certain input differences do not produce specific output differences. This occurs in rows like the first and others.
- **Conclusion:** Null entries limit an attacker's ability to craft specific differential trails, as they indicate that some differentials cannot happen. This property adds an extra layer of security to the S-box.

4. Symmetry

- **Observation:** The DDT is symmetric, i.e., if $D(x, y)$ is an entry, then $D(y, x)$ is also an entry.
- **Conclusion:** This symmetry is expected for well-designed S-boxes and confirms the correctness of the DDT, ensuring that the cryptographic function behaves consistently in both directions (input to output and vice versa).

5. Compliance with DDT Properties

The following propositions hold true for the DDT of Midori64:

- **Proposition 1:** Every entry in the DDT is a non-negative even integer between 0 and 2^n.
- **Proposition 2:** The top-left entry of the DDT is 2^n.
- **Proposition 3:** The first row consists of all zeros except the first entry, which is 2^n.
- **Proposition 4:** The first column consists of all zeros except the first entry, which is 2^n.
- **Proposition 5:** The sum of the entries of each row is 2^n.
- **Proposition 6:** If the S-box is bijective, then every row and column of the DDT adds up to 2^n.

The DDT of the Midori64 S-box adheres to these properties, which confirms that the S-box is well-structured and complies with the expected cryptographic behaviors.

Comparative Analysis with Other Ciphers

- **Group 1** AES has an S-box with $\Delta_{\max} = 2$, which is more optimal than Midori64's $\Delta_{\max} = 4$. AES is stronger against differential cryptanalysis due to this lower value but is not as efficient as Midori in lightweight scenarios where energy consumption is a concern.
- **Group 2** The PRESENT cipher also has $\Delta_{\max} = 4$, similar to Midori64. Both ciphers offer a balance between security and efficiency, suitable for constrained environments.

Conclusion

The Midori64 S-box offers a reasonable trade-off between security and efficiency, making it suitable for lightweight cryptographic applications. While it does not have the optimal differential uniformity of $\Delta_{\max} = 2$ seen in AES, it remains secure against differential cryptanalysis and other attacks due to its balanced distribution and structural properties.

Linear Approximation Table (LAT) Analysis of the Midori64 S-box

The Linear Approximation Table (LAT) for the S-box is a key component for analyzing the resistance of the S-box to linear cryptanalysis. It quantifies how well the S-box behaves under linear approximations, with lower values indicating better resistance. The LAT for the Midori64 S-box is shown below:

Table 3: Linear Approximation Table (LAT) for the Midori64 S-box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	2	4	2	-2	.	2	.	-2	.	2	.	4	-2	.	-2
2	.	4	.	.	4	.	.	.	-4	.	.	.	.	4	.	.
3	.	2	.	2	-2	.	2	4	2	-4	-2	.	.	2	.	2
4	.	-2	4	-2	2	.	-2	.	-2	-4	-2	.	.	-2	.	2
5	.	.	.	.	.	.	.	.	.	.	-4	-4	.	.	4	-4
6	.	2	.	2	-2	.	2	-4	-2	.	-2	.	-4	-2	.	2
7	.	.	.	4	.	.	-4	.	.	.	.	-4	.	.	-4	.
8	.	-2	-4	2	-2	.	-2	.	-4	-2	.	2	2	.	2	.
9	.	.	.	-4	-4	.	.	.	-2	2	-2	-2	2	2	-2	2
a	.	2	.	-2	-2	-4	-2	.	.	-2	4	-2	-2	.	2	.
b	.	.	.	.	.	-4	.	-4	2	-2	-2	2	2	2	-2	-2
c	.	4	.	.	.	.	-4	.	2	2	-2	2	2	-2	2	2
d	.	-2	4	2	-2	.	-2	.	.	2	.	2	-2	4	2	.
e	.	.	.	.	.	4	.	-4	2	-2	2	-2	2	2	2	2
f	.	-2	.	2	2	-4	2	.	.	2	.	-2	2	.	2	4

Value Counts in the Linear Approximation Table (LAT) This table represents the counts of each value observed in the Linear Approximation Table (LAT) for the Midori64 S-box.

Value	**Count**
-4	21
-2	44
0	123
2	52
4	15
8	1

LAT Analysis

1. Linear Bias and Distribution of Values

- **Observation:** The values in the LAT table are spread between positive and negative numbers. A few entries show larger values such as ±4 and ±2, which represent the linear bias of the approximation. Most values are closer to 0, indicating weaker linear approximations.

- **Conclusion:** The distribution of values suggests that the S-box of Midori64 is somewhat resistant to linear cryptanalysis. Ideally, the values should be close to 0 for most of the entries, which is the case here, though some larger biases may still indicate potential vulnerabilities.

2. Symmetry in LAT

- **Observation:** The LAT is symmetric, i.e., the value at position (i, j) is equal to the value at position (j, i), which is expected from a well-designed S-box.
- **Conclusion:** The symmetry of the LAT confirms that the Midori64 S-box behaves consistently in both directions (input to output and vice versa), which is a desirable property for cryptographic functions and indicates correctness in design.

3. Even Integer Entries in LAT

- **Observation:** All the entries in the LAT are even integers, as expected from a bijective S-box. This property holds true for the Midori64 S-box, which confirms that the S-box is a bijection.
- **Conclusion:** The fact that all LAT entries are even integers, and the first row and column (except the upper-left entry) consist of zeros, is a strong indicator that the S-box is bijective. This makes the S-box more secure against linear cryptanalysis.

4. Compliance with LAT Properties

- **Observation:** The first row and the first column are zeros, except for the upper-left entry, which is 2^{n-1}, indicating that the S-box follows the LAT properties of bijective S-boxes.
- **Conclusion:** The Midori64 S-box adheres to the properties expected from a bijective S-box. This is a positive feature, enhancing its cryptographic strength by ensuring that no biases are introduced through linear approximations.

Comparison with Other Ciphers

- **Group 1: AES S-box:** AES has a very well-known and well-optimized S-box with low bias in its LAT. The linear approximation values in AES are very close to 0, indicating that it is highly resistant to linear cryptanalysis.
- **Group 2: PRESENT S-box:** The PRESENT cipher, similar to Midori64, uses a lightweight S-box with a differential uniformity of 4. While its LAT is less optimal than AES, it still provides decent resistance to linear cryptanalysis, making it suitable for constrained environments.
- **Group 3: Midori64 S-box:** The Midori64 S-box has reasonable linear approximation properties with some biases in the LAT, but these are not excessively large. The S-box's properties are well-suited for lightweight cryptography, where efficiency is prioritized.

Final Conclusion

The Midori64 S-box strikes a balance between security and efficiency, making it suitable for lightweight cryptographic applications. Although its LAT does show some biases, the values are relatively small, and the overall resistance to linear cryptanalysis is reasonable. The bijective nature of the S-box, along with its symmetry and even integer entries, further contributes to its security. While the Midori64 S-box may not be as optimal as the AES S-box in terms of linear approximation resistance, it offers a good trade-off between security and computational efficiency, which is crucial for lightweight cryptography.