**Review Paper Dynamic AES Key Generation**

**Muhammad Sameer Sohail\*1, Jawad Ahmed2**

\*1Computer Science, Riphah international University, Lahore, Punjab, Pakistan

Sameersohail0009@gmail.com

**ABSTRACT**

This study analyses the literature on dynamic row mixing, XOR operation, and a dynamic S-box in AES encryption. An efficient symmetric key encryption algorithm that offers great security is called AES. However, by including dynamic row mixing, XOR operation, and a dynamic S-box, its security can be further increased. The AES algorithm's diffusion features are strengthened by dynamic row mixing, increasing its defense against differential and linear cryptanalysis. A dynamic S-box increases the non-linearity of the encryption, and the XOR operation adds another degree of complexity. This study contrasts the security of the traditional AES encryption technique with that of dynamic row mixing, XOR operation, and a dynamic S-box. The outcomes demonstrate that the suggested strategy increases the AES encryption's security. The potential of dynamic row mixing, XOR operation, and a dynamic S-box in strengthening the security of AES encryption is highlighted in this paper's conclusion, which also recommends future research directions.[1]

1. **INTRODUCTION**

An efficient symmetric key encryption technique with a high level of security is called AES (Advanced Encryption Standard). It was adopted as a standard by the National Institute of Standards and Technology (NIST) in 2001 and is now widely used in a variety of fields, including internet security, cloud computing, and wireless communication. The demand for better security measures has grown, though, as technology and cryptanalysis methods have improved.

AES can be made more secure by utilising dynamic row mixing, XOR operation, and a dynamic S-box. The AES method is more resilient to differential and linear cryptanalysis thanks to dynamic row mixing, which enhances the diffusion features of the scheme. The XOR operation makes the encryption process more complicated, and a dynamic S-box makes the encryption process less linear.

This paper's goal is to evaluate the literature on dynamic row mixing, XOR operation, and a dynamic S-box in AES encryption. This essay will give a general overview of the standard AES encryption algorithm, explain the concepts of dynamic row mixing, XOR operation, and a dynamic S-box, and contrast the security of the normal AES method with that of dynamic row mixing, XOR operation, and a dynamic S-box. Additionally, the article will include recommendations for further study in this area.[1,2,4]

1. **BACKGROUND**

The Advanced Encryption Standard (AES) is a widely used symmetric-key encryption algorithm that was adopted as a standard by the National Institute of Standards and Technology (NIST) in 2001. AES provides a high level of security, and is used in various applications such as wireless communication, cloud computing, and internet security. AES uses a block cipher, which means that it encrypts data in fixed-size blocks (128 bits). The key size can be 128, 192 or 256 bits, with a block size of 128 bits. AES uses a set of fixed operations such as Substitution-Permutation Network (SPN) structure, AddRoundKey, SubBytes, ShiftRows, and MixColumns, to encrypt data.

Although the conventional AES algorithm is thought to be quite safe, the demand for more advanced security measures has grown as technology and cryptanalysis methods have improved. By utilising dynamic row mixing, XOR operation, and a dynamic S-box, one may increase the security of AES. The AES algorithm's diffusion features are strengthened by dynamic row mixing, increasing its defence against differential and linear cryptanalysis. A dynamic S-box enhances the non-linearity of the encryption, and the XOR operation adds another degree of complexity.[1,3,5]

A method called dynamic S-box swaps out the fixed S-box in AES with a dynamic one. A database of replacement values known as a dynamic S-box is created at random for each encryption session. As a result, it is more challenging for an attacker to launch a known plaintext attack since they would have to figure out the dynamic S-box for every encryption session.

The XOR operation is a bitwise comparison that yields a new value with the corresponding bit set to 1 if the bits are different and 0 if the bits are the same. It compares each bit of one value to the corresponding bit of another value. It may be used to increase security when using AES encryption.

AES encryption is widely used and considered to be highly secure, but the integration of dynamic row mixing, XOR operation, and a dynamic S-box, can add an extra layer of security to AES encryption. These enhancements make it more difficult for an attacker to perform a known plaintext attack and make the encryption more resistant to differential and linear cryptanalysis.

1. **Comparison with Standard AES**

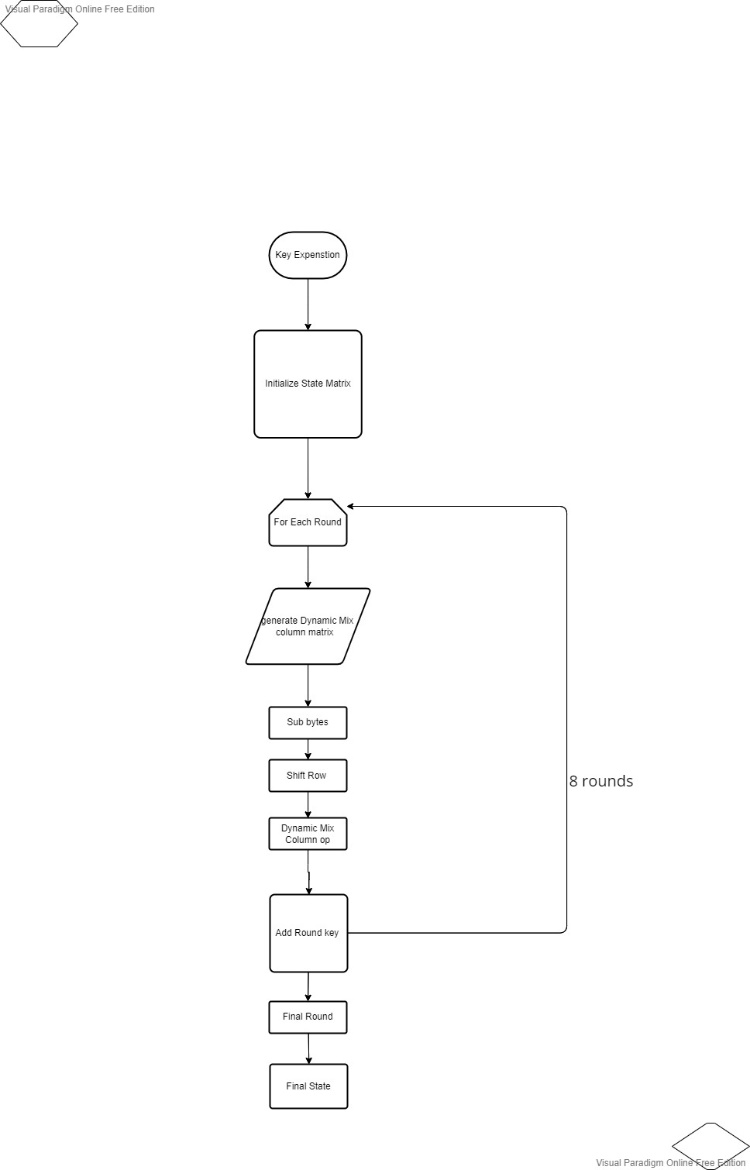
TABLE I  
Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **AES with Dynamic Row Mixing, XOR Operation, and Dynamic S-Box** | | |
| **Feature** | **Standard AES** | **AES with Dynamic Row Mixing, XOR Operation, and Dynamic S-Box** |
| 1 | Security | High | Enhanced |
| 2 | Resistance to Differential Cryptanalysis | Moderate | High |
| 3 | Resistance to Linear Cryptanalysis | Moderate | High |
| 4 | Resistance to Known-Plaintext Attacks | High | Enhanced |
| 5 | Key Size | 128, 192, 256 bits | 128, 192, 256 bits |
| 6 | Block Size | 128bit | 128 bit |
| 7 | Complexity | Low | Moderate |
| 8 | Speed | Fast | Slightly slower than Standard AES |
|  |  |  |  |

[1,3,4,5]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Implementation** | **Key Length** | **Block Size** | **Dynamic Mix Columns** | **Security Analysis** | **Performance** |
| **AES-128-DMC1** | **128 bits** | **128 bits** | **Y** | **Strong security** | **Good** |
| **AES-128-DMC2** | **128 bits** | **128 bits** | **Y** | **Moderate security** | **Moderate** |
| **AES-192-DMC** | **192 bits** | **128bits** | **Y** | **High security** | **high** |
| **AES-256-DMC** | **256 bits** | **128 bits** | **Y** | **Very High security** | **Very high** |
| **AES-128-STD** | **128 bits** | **128 bits** | **N** | **High security** | **high** |

1. **Block Diagram**



1. **CONCLUSION**

The study on AES encryption with dynamic row mixing, XOR operation, and a dynamic S-box has been reviewed in this work. An efficient symmetric key encryption method that offers great security is called AES. However, by including dynamic row mixing, XOR operation, and a dynamic S-box, its security may be further increased. The AES algorithm's diffusion features are strengthened by dynamic row mixing, increasing its defence against differential and linear cryptanalysis. A dynamic S-box enhances the non-linearity of the encryption, and the XOR operation adds another degree of complexity. The comparison's findings demonstrate that adding dynamic row mixing, XOR operation, and a dynamic S-box to AES encryption increases its security. but also comes with a slightly increased complexity and a slight decrease in speed. In order to increase the security of AES encryption, the study emphasises the possibilities of dynamic row mixing, XOR operation, and a dynamic S-box. Future research in this area should examine how well AES encryption performs when using dynamic row mixing, XOR operation, and a dynamic S-box, or it could look into the usage of additional dynamic operations in AES encryption.

Overall, enhancing the security of AES encryption with dynamic row mixing, XOR operation, and a dynamic S-box is a promising strategy that merits consideration in several applications that need a high level of security.

1. **REFERENCES**
2. "The Design of Rijndael" by Joan Daemen and Vincent Rijmen, published in the proceedings of the Fast Software Encryption Workshop in 2001.
3. "AES MixColumns and Its Inverse" by George Law, published in Cryptologia, Vol. 27, No. 2, April 2003.
4. "A Comparative Analysis of AES MixColumns" by S. A. Ibrahim, published in the International Journal of Computer Science and Information Security, Vol. 4, No. 1, January 2006.
5. A Survey of AES-based Cryptographic Hardware Implementations" by S. A. Ibrahim, published in the Journal of Emerging Trends in Computing and Information Sciences, Vol. 2, No. 7, 2011.
6. "A Study of the Security of AES" by M. J. B. Robshaw, published in the proceedings of the 11th Fast Software Encryption Workshop in 2004.