Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5, 436-443
2025
Publisher: Learning Gate
DOI: 10.55214/25768484.v9i5.6886

Enhancing block cipher diffusion: A mathematical approach to key-dependent mix column transformations

Shiraz Naserelden[1*], Norma Alias[1,2], Abdelrahamn Altigani[3], Maher Waheeb[3], Azmi Alazzam[3], Muawia A. Elsadig[4], Hasan Abu Hilal[5]
[1]Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia (UTM), Johor Bahru, 81310, Malaysia; s.naserelden@gmail.com (S.N.).
[2]Center of Engineering Education, Universiti Teknologi Malaysia (UTM), Johor Bahru, 81310, Malaysia; normaalias@utm.my (N.A.).
[3]Computer Information Science, Higher Colleges of Technology, 25026, Al Ain, Abu Dhabi, UAE; aabdelgader@hct.ac.ae (A.A.) mwaheeb@hct.ac.ae (M.W.) aalazzam@hct.ac.ae (A.Z.)
[4]Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia; makhlafalla@iau.edu.sa (M.A.E.).
[5]Engineering Technology & Science, Higher Colleges of Technology, Abu Dhabi, UAE; habuhilal@hct.ac.ae (H.A.H.).

Abstract: In this paper, we propose a novel key-dependent MixColumn transformation to enhance the diffusion properties of block ciphers, specifically within the AES framework. The proposed method introduces dynamic variation into the MixColumn step by extracting a pseudo-random value from the round key, which is used to perform cyclic permutations on the MixColumn coefficients. This leads to the construction of a round-dependent transformation matrix, mathematically defined and proven to maintain invertibility over GF(2^8). We provide a formal mathematical representation of the proposed model and analyze its diffusion characteristics, linear independence, and resistance to cryptanalytic attacks. Our approach eliminates static transformation patterns and introduces key-driven unpredictability, offering a promising direction for adaptive cryptographic primitives without increasing algorithmic complexity or requiring hardware modifications.

Keywords: *Block ciphers, Advance encryption standard, Finite fields, MixColumn transformation, Encryption, Maximum distance separable.*

1. Introduction

Block ciphers are a cornerstone of contemporary cryptographic infrastructure, underpinning data security in countless digital systems. Their effectiveness relies heavily on two fundamental properties defined by Claude Shannon: confusion, which conceals the correlation between the encryption key and ciphertext, and diffusion, which ensures that changes in the plaintext are spread across the ciphertext in a complex and non-linear manner [1].

One of the most prominent examples of these principles in action is the Advanced Encryption Standard (AES) [2] which integrates multiple transformations including SubBytes, ShiftRows, MixColumns and AddRoundKey to achieve strong security. In particular, the MixColumns operation introduces diffusion through a fixed linear transformation over a finite field. However, as cryptanalysis continues to evolve, static diffusion techniques such as these are increasingly scrutinized for their potential vulnerability to attacks [3, 4] especially those that exploit weaknesses related to key structure or predictability, such as related-key and weak-key attacks [5].

To counter these risks, researchers have turned their attention to key-dependent diffusion techniques [6], which adjust the transformation dynamically based on the secret key. These approaches aim to increase cryptographic strength by introducing an additional layer of unpredictability [7].

History: Received: 19 February 2025; Revised: 26 April 2025; Accepted: 30 April 2025; Published: 5 May 2025
* Correspondence: s.naserelden@gmail.com

Nevertheless, achieving a balance between adaptability, security, and implementation efficiency is far from trivial, and poorly constructed solutions may inadvertently introduce new weaknesses.
This study introduces a mathematically rigorous method for constructing key-dependent MixColumn transformations that not only enhance diffusion but also preserve critical cryptographic qualities such as reversibility, optimal branch number, and robustness against both linear and differential cryptanalysis. The methodology is built on well-established mathematical structures, including circulant matrices, Maximum Distance Separable (MDS) codes, and algebraic frameworks like polynomial rings, enabling the development of dynamic yet computationally efficient diffusion layers.
Our key contributions have threefold: First, we present a theoretical framework for key-dependent diffusion by integrating adaptive diffusion into broader cipher designs.

2. Literature Review

A number of symmetric encryption algorithms and mechanisms have been introduced in the last few decades [8-12]. However, there have been special interest on enhancing the efficiency, adaptability, and security of the Advanced Encryption Standard (AES), particularly in the context of constrained environments such as embedded systems and IoT devices.

To address the limitations of resource-constrained environments, multiple works have explored architectural and hardware-based improvements. One such study introduces an optimized AES implementation using a Low-Transition Linear Feedback Shift Register (LFSR), hardware design techniques, and low-power strategies including subthreshold voltage operation and back-biasing. These modifications collectively reduce power consumption and enhance latency performance, making the algorithm more suitable for IoT devices [13].

developing a formal model for MixColumn operations whose structure is dynamically influenced by the encryption key, ensuring that essential diffusion and security properties are preserved. Second, we propose efficient matrix constructions using lightweight and structured designs that support key-dependent behavior while maintaining compatibility with high-performance cryptographic implementations. Finally, we conduct a comprehensive security assessment, evaluating the proposed approach against a range of classical and modern cryptanalytic techniques, including differential, linear, and algebraic attacks, demonstrating improved resilience compared to traditional fixed diffusion layers.

Key-dependent MixColumns transformations represent a promising advancement in cryptographic security by enhancing resistance to various attacks, yet they also introduce added complexity and computational demands, highlighting the ongoing need for research into more efficient algorithms, hardware implementations, and practical design trade-offs to ensure their widespread applicability [14, 15].

By introducing key-driven variability into the diffusion process, our approach paves the way for more resilient cryptographic primitives, capable of withstanding increasingly sophisticated adversarial techniques while retaining the efficiency demanded by real-world applications.

The rest of this paper is organized as follows: Section two is the literature review, which discusses a number of similar research work in this field. Section three details our methodology and presents the mathematical foundation for dynamic MixColumn transformations. Section four provides a security analysis. Section five concludes the work, highlighting future research directions and the potential for

Similarly, another study eliminates lookup tables in the MixColumns operation and parallelizes major AES transformations within the encryption and decryption processes. Implemented on FPGA devices, the design achieves reduced resource usage and high processing speed, demonstrating its practicality for secure embedded applications with limited hardware capacity [15].

Further extending these improvements, research utilizing Virtex-6 and Spartan-6 FPGA platforms proposes a modified SubBytes stage to minimize power, area, and delay. The resulting AES structure improves throughput and is tested using real-world medical imaging data, highlighting its suitability for high-speed, power-sensitive applications [16].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 436-443, 2025
DOI: 10.55214/25768484.v9i5.6886

Others research focus on enhancing MixColumns and diffusion layers. A key area of innovation lies in the transformation stages, particularly MixColumns. One work strengthens AES's resistance to cryptanalytic attacks by replacing the standard MixColumn matrix with Maximum Distance Separable (MDS) matrices of varying sizes. These changes improve the cipher's branch number and diffusion characteristics, enhancing protection against linear and differential cryptanalysis while maintaining efficiency [17].

In a related approach, researchers propose using 8×8 circulant matrices in the MixColumns step, offering a faster and more secure alternative to traditional 4×4 matrices. This method reduces arithmetic operations and boosts processing speeds by up to 79%, especially beneficial for applications involving key exchange protocols such as Elliptic Curve Diffie-Hellman (ECDH) [18].

Complementing these matrix-based improvements, another work replaces MixColumns with a transformation derived from a magic cube over GF(28). Designed specifically for voice message encryption on social media platforms, the approach uses cube-generated keys to enhance execution speed and encryption complexity, demonstrating promising results in time reduction and security metrics [19].

Addressing power efficiency from a different angle, one study explores the use of Quantum Dot Cellular Automata (QCA) for implementing an Xtime multiplier in Galois Field arithmetic. QCA's high frequency and low energy requirements make it a compelling alternative to CMOS technology. The proposed QCA-based multiplier significantly reduces energy dissipation and quantum cost, showcasing its potential for future lightweight AES implementations [20].

In the context of lightweight cryptography, another study examines the PRINCE block cipher, focusing on vulnerabilities to side-channel attacks in unrolled architectures. By employing a chosen-input attack and analyzing Threshold Implementations (TI), the researchers highlight the critical trade-off between performance and security in lightweight designs and emphasize the importance of protecting multiple cipher rounds against key leakage [21].

To further complicate adversarial analysis, recent work introduces a polymorphic AES variant (P-AES), where core transformations—SubBytes, ShiftRows, and MixColumns—are made key-dependent. Each encryption instance varies based on the key, thereby significantly reducing predictability and increasing resistance to cryptanalytic attacks. The approach maintains AES's performance advantages while embedding an additional layer of dynamic security [22].

Collectively, these studies offer diverse and innovative strategies for evolving the AES encryption standard. From energy-efficient hardware designs and high-speed transformations to enhanced security through polymorphism and diffusion, the modifications address critical challenges in modern cryptography. These advancements not only improve AES's adaptability for constrained environments but also strengthen its resilience against emerging security threats, affirming its continued relevance in secure digital communications.

3. Methodology

3.1. Proposed Method: Key-Dependent Cyclic Mixcolumn Transformation

Let the AES MixColumn transformation be defined over the finite field $\mathbb{F}_{2^8}$. The standard AES MixColumn matrix M is:

$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Let $K_r \in \mathbb{F}_{2^8}^{16}$ be the round key at round r. From K_r, extract a permutation index $\rho_r \in \{0,1,2,3\}$ as follows:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 436-443, 2025
DOI: 10.55214/25768484.v9i5.6886

$$\rho_r = \left(\sum_{i=0}^{15} k_{r,i} \right) mod\ 4$$

Where $k_{r,i}$ is the ith byte of K_r.

Define $\pi_{\rho_r}(M)$ to be the matrix formed by applying a cyclic row permutation to M by ρ_r positions. For instance:

- If $\rho_r = 1$, then row 0 moves to row 1, row 1 → row 2, ..., row 3 → row 0.
- If $\rho_r = 2$, rows are rotated by 2 positions, and so on.

Let this dynamically generated matrix be $M_r = \pi_{\rho_r}(M)$.

Then the state transformation becomes:

$$S' = M_r . S$$

$S \epsilon \mathbb{F}_{2^8}^{4\times1}$ is a column of the state matrix, and S' is the output column after the MixColumn operation

3.2. Invertibility of the Dynamic MixColumn Transformation

A core requirement of any linear transformation in a block cipher is invertibility. The original AES MixColumn matrix M is invertible over the finite field $\mathbb{F}_{2^8}$, with a known inverse matrix M^{-1} used during decryption.

In our proposed scheme, we define a set of transformation matrices $\{M_r\}$ generated by cyclically permuting the rows of M by a round-specific index $\rho_r \in \{0,1,2,3\}$. Each M_r is defined as:

$$M_r = \pi_{\rho_r}(M)$$

Where π_{ρ_r} denotes a cyclic permutation of the rows of M by ρ_r positions.

Proposition 1. *If* $M \epsilon \mathbb{F}_{2^8}^{4\times4}$ *is invertible, then* $M_r = \pi_{\rho_r}(M)$ *is also invertible for any* $\rho_r \in \{0,1,2,3\}$.

Proof.

Cyclic row permutation is equivalent to left-multiplying M by a permutation matrix P_{ρ_r} , which is invertible and orthogonal (i.e., $P_{\rho_r}^{-1} = P_{\rho_r}^{T}$):

$$M_r = \pi_{\rho_r}(M)$$

Since both P_{ρ_r} and M are invertible, their product M_r is also invertible:

$$M_r^{-1} = M^{-1} P_{\rho_r}^{-1}$$

Therefore, each M_r used in encryption has a well-defined inverse transformation for decryption:

$$S = M_r^{-1} . S' = M^{-1} P_{\rho_r}^{-1} . S'$$

Hence, the decryption process can be symmetrically defined using the inverse permutation and the inverse MixColumn matrix.

3.3. Diffusion Properties

One of the primary goals of the MixColumn operation is to ensure that a single-byte change in the input affects multiple bytes in the output, a property known as diffusion.

In standard AES, each column $S \epsilon \mathbb{F}_{2^8}^{4\times1}$ is transformed by a fixed MDS (Maximum Distance Separable) matrix M. The diffusion effect is measured by the branch number B, defined as:

$$B(M) = \min_{x \neq 0} (wt(x) + wt(M.x))$$

Where $wt(x)$ is the Hamming weight (number of non-zero components) of the vector x.

Since our transformation is based on permutations of the rows of M, the resulting matrix M_r maintains the same set of rows, only reordered. This implies that the branch number is preserved under permutation.

Proposition 2. *For all* $\rho_r \in \{0,1,2,3\}$, *the branch number satisfies* $B(M_r) = B(M)$.

Proof.

Row permutation does not alter the linear dependencies between input and output components, nor does

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 436-443, 2025
DOI: 10.55214/25768484.v9i5.6886

it affect the weight distribution of the transformation matrix. Therefore, the minimum combined weight remains unchanged across all M_r, preserving diffusion strength.

3.4. Key-Dependent Unpredictability

By varying M_r per round based on a value ρ_r extracted from the round key, we introduce round-dependent structural variation. Since the round key K_r is a function of the secret master key, the permutation index ρ_r becomes unpredictable to an adversary without key knowledge.

Furthermore, this variability introduces a layer of non-linearity in the key schedule interaction, increasing resistance to:

- Linear cryptanalysis: due to variability in the diffusion layer.
- Algebraic attacks: because the transformation matrix is no longer constant and cannot be eliminated or algebraically modeled as fixed coefficients.

4. Security Discussion

The security of block ciphers relies heavily on confusion and diffusion principles as articulated by Claude Shannon. While AES exhibits strong resistance to most classical attacks, the static nature of its MixColumn operation may provide structural predictability exploitable in certain advanced attack scenarios. In this section, we discuss how the proposed key-dependent cyclic MixColumn transformation enhances security by introducing dynamic variability, maintaining diffusion strength, and complicating adversarial modeling.

4.1. Resistance to linear and differential cryptanalysis

In classical differential cryptanalysis, an attacker studies how input differences propagate through the cipher to infer key-related information. Similarly, linear cryptanalysis seeks affine approximations between plaintext, ciphertext, and key bits.

Because the proposed transformation matrix $M_r = \pi_{\rho_r}(M)$ varies each round based on a value $\rho_r \in \{0,1,2,3\}$ extracted from the round key, the adversary no longer operates against a static linear transformation. The diffusion characteristics remain preserved due to the invariant branch number (as proven in Section 3), but the attack surface becomes more complex.

Let ΔS represent a difference in input state columns. The output difference after the MixColumn becomes:

$$\Delta S' = M_r \,.\, \Delta S$$

Since M_r varies with K_r, each round uses a distinct transformation. Therefore, an attacker attempting to build a differential characteristic must account for a sequence of different matrices $\{M_1, M_2, \ldots, M_3\}$, each dependent on round keys, which are not known in advance. This disrupts the construction of stable differential trails or linear approximations across rounds.

Thus, the cipher exhibits increased round unpredictability, a critical advantage in defending against statistical attacks.

4.2. Resistance to Algebraic Attacks

Algebraic attacks exploit systems of equations describing the cipher's operations. In AES, fixed S-box and linear layer components allow attackers to build compact algebraic representations for analysis.

Our method disrupts this model: since M_r changes every round, the system of equations modeling the cipher becomes non-uniform and parameterized by secret key-derived values. Specifically, the cyclic row permutation index ρ_r changes the coefficients of the transformation matrix in a key-dependent manner, increasing the algebraic complexity.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 436-443, 2025
DOI: 10.55214/25768484.v9i5.6886

If an attacker models the encryption as a polynomial system $\mathcal{P}$ over $\mathbb{F}_{2^8}$, then each M_r introduces fresh variables into $\mathcal{P}_r$. Hence, the overall system cannot be statically precomputed, reducing the feasibility of Gröbner basis or SAT-based algebraic attacks.

4.3. Related-Key and Structural Attacks

Related-key attacks rely on observing the behavior of the cipher under known relations between keys. In traditional AES, the linearity of MixColumn and its independence from the key may allow certain relations to persist.

By tying the MixColumn matrix directly to the round key through ρ_r, such relations are disrupted. Even related round keys K_r and K_r' may yield different ρ_r values, thus different transformation matrices M_r, resulting in unrelated diffusion paths.

Moreover, structural attacks that exploit repeated internal patterns are mitigated, since our transformation ensures that no two rounds necessarily share the same MixColumn transformation, assuming the round keys are non-repetitive (which is generally true in AES key schedules).

4.4. Implementation Considerations and Overhead

While this work is theoretical in nature and does not require implementation, we note that the proposed method introduces no increase in matrix size or field complexity. The operations are performed over $\mathbb{F}_{2^8}$ as in standard AES. The only added operation is the generation of the permutation index ρ_r from the round key a simple byte-level modular operation.

This suggests that even if implemented, the method would incur negligible overhead while offering enhanced variability and improved resistance to structure-dependent attacks.

5. Conclusion and Future Work

In this paper, we introduced a mathematically grounded enhancement to the AES MixColumn transformation by proposing a key-dependent cyclic permutation mechanism. The core idea is to extract a round-specific permutation index from the round key and apply it to the rows of the standard MixColumn matrix, resulting in a dynamic, round-varying linear transformation.

We formally proved that the proposed transformation preserves invertibility and diffusion strength, specifically maintaining the branch number of the AES MixColumn matrix. Moreover, the variation introduced at each round is driven entirely by the key schedule, rendering the cipher more resilient to differential, linear, and algebraic attacks, while incurring no increase in matrix complexity or underlying field operations.

The theoretical contribution lies in showing that simple structural variation, when tied to key material, can enhance cryptographic robustness without sacrificing formal properties such as linear independence or efficient invertibility.

The following are a few directions for potential areas for future research:

- Theoretical Bound on Branch Number Stability: While the branch number is preserved under row permutations, further generalization to other types of key-dependent transformations (e.g., column permutations or coefficient rotations) warrants formal analysis.
- Provable Security under Composition: A formal security proof under existing cryptographic models (e.g., PRP or IND-CPA frameworks) would offer a deeper understanding of this transformation's impact in composition with the rest of AES operations.
- Matrix Class Characterization: A mathematical characterization of the class of all invertible matrices obtainable via cyclic permutations of AES's MixColumn could help in assessing the total variability and potential design space.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 9, No. 5: 436-443, 2025
DOI: 10.55214/25768484.v9i5.6886

- Generalization to Other Block Ciphers: The approach may be extended to other SPN-based ciphers that utilize MDS matrices in their linear layer, allowing for broader applicability of key-dependent transformations.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[2] J. Daemen and V. Rijmen, "Reijndael: The advanced encryption standard," *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, vol. 26, no. 3, pp. 137-139, 2001.

[3] A. Altigani, S. Hasan, B. Barry, and S. M. Shamsuddin, "Key-dependent advanced encryption standard," presented at the 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering, IEEE, 2018.

[4] P. Iranfar, A. Amirany, and M. H. Moaiyeri, "Power attack-immune spintronic-based AES hardware accelerator for secure and high-performance PiM architectures," *IEEE Transactions on Magnetics*, pp. 1-10, 2025.

[5] A. Altigani, M. R. Ghalib, H. T. Elshoush, M. A. Elsadig, N. Alrefai, and S. Naserelden, "The advanced encryption standard with a dynamic S-box using the RC4 key schedule," presented at the 2024 International Conference on Electrical, Computer and Energy Technologies, IEEE, 2024.

[6] M. Belam, "Deimos Cipher: A High-Entropy, Secure Encryption Algorithm with Strong Diffusion and Key Sensitivity," *Cryptology ePrint Archive*, 2025.

[7] B. Santhosh and V. Kushmitha, "Cryptographic image security using AES-XOR approach," presented at the 2025 4th International Conference on Sentiment Analysis and Deep Learning, IEEE, 2025.

[8] A. Altigani, M. Abdelmagid, and B. Barry, *Evaluating AES performance using NIST recommended block cipher modes of operation*. Saudi Arabia: University of Dammam, 2015.

[9] A. Altigani, M. Abdelmagid, and B. Barry, "Analyzing the performance of the advanced encryption standard block cipher modes of operation: Highlighting the national institute of standards and technology recommendations," *Indian Journal of Science and Technology*, vol. 9, no. 28, pp. 1-8, 2016.

[10] A. Altigani, S. Hasan, S. M. Shamsuddin, and B. Barry, "A multi-shape hybrid symmetric encryption algorithm to thwart attacks based on the knowledge of the used cryptographic suite," *Journal of Information Security and Applications*, vol. 46, pp. 210-221, 2019.

[11] H. T. Elshoush, D. M. Ahmed, A. A. Ishag, M. A. Elsadig, and A. Altigani, "Text encryption using secure and expeditious multiprocessing Serpent CTR using logistic map," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 6, pp. 6753-6772, 2024.

[12] H. T. Elshoush, D. M. Ahmed, A. A. Ishag, M. A. Elsadig, and A. Altigani, "Text encryption using secure and expeditious multiprocessing Serpent CTR using logistic map," *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 14, no. 6, pp. 6753–6772, 2024. https://doi.org/10.11591/ijece.v14i6.pp6753-6772

[13] S. G. Singh and M. K. Porwal, "Implementation of optimized area and speed architectures for the mix column operation of the advanced encryption standard," *Material Science and Technology*, vol. 20, no. 6, pp. 345–354, 2021.

[14] J. S. Baladhay and E. De Los Reyes, "AES-128 reduced-round permutation by replacing the MixColumns function," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, no. 3, pp. 1641-1652, 2024.

[15] R. H. Prayitno, Latifah, S. A. Sudiro, S. Madenda, and S. Harmanto, "A modified MixColumn-InversMixColumn in AES algorithm suitable for hardware implementation using FPGA device," *Communications in Science and Technology*, vol. 8, no. 2, pp. 198-207, 2023. https://doi.org/10.21924/cst.8.2.2023.1257

[16] M. K. Thanikodi, "Advanced encryption standard algorithm for power-efficient and high-speed applications," *Wireless Personal Communications*, vol. 140, no. 1-2, pp. 225-239, 2025. https://doi.org/10.1007/s11277-024-11693-0

[17] L. Tran Thi, "Proving the security of aes block cipher based on modified mixcolumn," *Journal of Computer Science and Cybernetics*, vol. 40, no. 2, pp. 187-203, 2024. https://doi.org/10.15625/1813-9663/18058

[18] Y.-W. Chen, J.-J. Wang, Y.-H. Chen, and C.-D. Lee, "Diversity aes in mixcolumns step with 8x8 circulant matrix," *International Journal of Engineering Technologies and Management Research*, vol. 8, no. 9, pp. 19-35, 2021. https://doi.org/10.29121/ijetmr.v8.i9.2021.1037

[19] W. W. Mohammed M. Al-Ezzi, Abdul Monem S. Rahma, Hasnain Ali Al mashhadani, and Mazen R. Hassan "A new encryption algorithm for voice messages on social media using magic cube GF (2^8) technology," *International Journal of Electrical and Computer Engineering Systems*, vol. 16, no. 3, pp. 253–263, 2024. https://doi.org/10.32985/ijeces.16.3.6

[20] P. Rajasekar, H. Mangalam, K. H. Shakthi Murugan, and K. Kalaiselvi, "Realization of energy efficient GF Xtime multiplier using quantum dot cellular automata (QCA) for AES-MixColumn," *Journal of Computational Electronics*, vol. 24, no. 1, pp. 15–26., 2024. https://doi.org/10.1007/s10825-024-02248-4

[21] A. Borchers and T. Pieler, "Programming pluripotent precursor cells derived from Xenopus embryos to generate specific tissues and organs," *Genes (Basel)*, vol. 1, no. 3, pp. 413-426, 2023. https://doi.org/10.3390/genes1030413

[22] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "A polymorphic advanced encryption standard – A novel approach," *IEEE Access*, vol. 9, pp. 20191-20207, 2021. 10.1109/access.2021.3051556

Appendix A.

Example of Key-Dependent MixColumn Permutations.

Let the original AES MixColumn matrix $M \epsilon \mathbb{F}_{2^8}^{4\times4}$ be:

$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Let the **cyclic row permutation index** ρ_r for each round r be extracted from a round key byte k_r using:

$$\rho_r = k_r \ mod \ 4$$

Example: Round-wise Matrix Transformations

Round r	Key Byte K_r	$\rho_r = k_r \ mod \ 4$	Permutation Description	Transformed M_r
1	0x73	3	Rotate rows down by 3	$M_1 = \pi_3(M)$
2	0xB1	1	Rotate rows down by 1	$M_2 = \pi_1(M)$
3	0x2A	2	Rotate rows down by 2	$M_3 = \pi_2(M)$
4	0x0C	0	No rotation (standard AES)	$M_4 = M$

The actual row-permuted matrices are:

$$1.\ M_1 = \pi_3(M) \rightarrow \begin{bmatrix} 3 & 1 & 1 & 2 \\ 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \end{bmatrix}$$

$$2.\ M_2 = \pi_1(M) \rightarrow \begin{bmatrix} 1 & 2 & 3 & 1 \\ 3 & 1 & 1 & 2 \\ 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \end{bmatrix}$$

$$3.\ M_3 = \pi_2(M) \rightarrow M = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 3 & 1 & 1 & 2 \\ 2 & 3 & 1 & 1 \end{bmatrix}$$

$$4.\ \ M_4 \ = M \rightarrow M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$