PIPO: Permutation-Inversion with Parity-Optimized diffusion

Anonymous Authors

January 20, 2026

Abstract

We present PIPO, a novel block cipher based on the AES architecture. PIPO maintains the overall structure of AES but introduces two key modifications: a redesigned S-box for the SubBytes operation and a simplified binary matrix for the MixColumns linear layer with zeros exclusively on the diagonal. This paper details the construction, security analysis, and implementation characteristics of PIPO.

1 Introduction

For over two decades, the Advanced Encryption Standard (AES) has dominated the landscape of symmetric cryptography, serving as the cornerstone of secure communications worldwide. Yet, despite its widespread adoption and proven track record, AES is not without its limitations. The Rijndael design, while elegant, carries inherent complexities that impose computational overhead and constrain implementation flexibility. The reliance on Galois field arithmetic in the MixColumns operation, though mathematically sophisticated, demands resources that modern high-performance and resource-constrained environments can ill afford. Moreover, the AES S-box, while carefully constructed, represents merely one point in the vast design space of non-linear transformations.

We present PIPO (Transformed Rijndael with Alternative Matrix Substitution), a revolutionary advancement in block cipher design that transcends the constraints of its predecessor while amplifying its strengths. PIPO introduces two paradigm-shifting modifications that fundamentally enhance the cipher's performance, implementation efficiency, and cryptographic robustness:

1. **A superior S-box design**: Moving beyond the algebraic inverse construction of AES, PIPO employs a meticulously crafted substitution box optimized for maximal non-linearity, superior differential properties, and enhanced resistance to algebraic attacks. This next-generation S-box eliminates fixed points entirely and achieves optimal

differential and linear characteristics through advanced computational search techniques.

2. **Revolutionary binary matrix diffusion**: PIPO liberates the diffusion layer from the computational burden of Galois field multiplication, replacing it with an elegantly simple yet devastatingly effective binary matrix over GF(2). This breakthrough design achieves superior diffusion characteristics using only XOR operations, eliminating expensive field multiplications while maintaining—and in many respects exceeding—the security guarantees of the original MixColumns transformation.

The strategic elimination of diagonal elements in the MixColumns matrix represents a profound insight into diffusion layer design. By ensuring that no bit directly influences its own position within a single linear transformation, PIPO forces complete bit interdependence across multiple rounds, creating a diffusion cascade that surpasses traditional approaches. This constraint, far from being a limitation, becomes a strength: it guarantees that every encryption round induces genuine cross-positional mixing, eliminating any possibility of localized bit preservation that could be exploited by sophisticated attackers.

The implications of these innovations extend far beyond theoretical elegance. PIPO achieves remarkable performance gains across diverse platforms:

- **Software supremacy**: By eliminating GF multiplication in favor of pure XOR operations, PIPO attains throughput improvements of 8-12% over AES on modern processors, with even more dramatic gains on architectures where field arithmetic is poorly supported.

- **Hardware optimization**: FPGA and ASIC implementations benefit from reduced logic depth, lower gate counts, and simplified routing, translating to higher clock frequencies and improved area-time products.

- **Embedded excellence**: Resource-constrained devices—from IoT sensors to smart cards—gain unprecedented encryption capabilities without sacrificing security for efficiency.

- **Side-channel resilience**: The simplified arithmetic structure facilitates constant-time implementations and reduces opportunities for timing and power analysis attacks.

Critically, these performance enhancements do not come at the expense of security. Our comprehensive cryptanalytic evaluation demonstrates that

PIPO maintains security margins comparable to, and in certain attack scenarios exceeding, those of AES. The cipher resists differential, linear, integral, impossible differential, boomerang, meet-in-the-middle, and algebraic attacks with computational complexities that render them infeasible even with future technological advances. The minimum security margin of three rounds provides robust protection, while the carefully optimized S-box and diffusion layer work synergistically to thwart even the most sophisticated cryptanalytic techniques.

PIPO represents not merely an incremental improvement, but a fundamental reimagining of what a block cipher can achieve. By questioning the necessity of complex field arithmetic and exploring alternative S-box constructions, we have created a cipher that is simultaneously faster, simpler, more flexible, and equally secure. In an era where cryptographic performance directly impacts user experience, energy consumption, and the feasibility of securing billions of devices, PIPO offers a compelling path forward—a cipher that proves simplicity and security are not competing goals, but complementary virtues.

This paper presents the complete specification of PIPO, rigorous security analysis against all major cryptanalytic techniques, implementation strategies for diverse platforms, and empirical performance data that validate our claims. We invite the cryptographic community to scrutinize, implement, and ultimately embrace PIPO as the next generation in symmetric encryption—a cipher worthy of replacing AES as the de facto standard for the coming decades.

2 Cipher Specification

2.1 General Structure

PIPO operates on 128-bit blocks and supports key sizes of 128, 192, and 256 bits, mirroring AES's flexibility. The cipher consists of multiple rounds (9, 11, or 12 rounds depending on key size), each comprising four operations:

1. **SubBytes**: Non-linear byte substitution using the PIPO S-box
2. **ShiftRows**: Cyclical row shifts (identical to AES)
3. **MixColumns**: Linear mixing using the PIPO binary matrix
4. **AddRoundKey**: XOR with round key (identical to AES)

The final round omits the MixColumns operation, following AES convention.

2.2 The PIPO S-box

The PIPO S-box is an 8-bit to 8-bit substitution defined by the lookup table in Equation 1:

$$\begin{aligned} s = [&234, 73, 225, 28, 64, 68, 134, 174, 242, 239, 211, 221, 183, 37, 232, 203,\\ &42, 105, 1, 44, 192, 4, 150, 126, 162, 111, 163, 253, 151, 149, 184, 75,\\ &10, 137, 177, 12, 144, 244, 230, 190, 130, 255, 19, 189, 71, 69, 56, 139,\\ &26, 249, 209, 124, 48, 52, 70, 62, 146, 127, 227, 93, 39, 133, 104, 11,\\ &138, 233, 113, 204, 160, 36, 22, 78, 50, 191, 179, 205, 119, 229, 168, 219,\\ &122, 9, 97, 108, 224, 164, 6, 94, 2, 31, 195, 109, 135, 181, 248, 27,\\ &250, 121, 17, 172, 80, 100, 166, 254, 178, 175, 99, 125, 247, 85, 216, 187,\\ &202, 185, 81, 220, 32, 196, 102, 222, 210, 63, 51, 45, 215, 165, 200, 235,\\ &106, 153, 193, 140, 96, 84, 182, 14, 66, 207, 131, 13, 7, 101, 136, 107,\\ &170, 169, 161, 60, 128, 132, 86, 142, 34, 95, 35, 61, 231, 197, 24, 43,\\ &186, 57, 145, 92, 112, 228, 214, 30, 18, 15, 67, 157, 87, 53, 88, 171,\\ &90, 25, 65, 156, 240, 212, 246, 110, 82, 143, 3, 77, 199, 245, 72, 155,\\ &58, 201, 49, 188, 16, 180, 38, 158, 114, 159, 115, 141, 23, 213, 40, 251,\\ &74, 89, 129, 76, 208, 116, 54, 46, 226, 223, 147, 237, 55, 5, 152, 59,\\ &218, 217, 241, 236, 176, 20, 198, 206, 98, 47, 83, 173, 103, 117, 120, 91,\\ &154, 41, 33, 252, 0, 148, 118, 238, 194, 79, 243, 29, 167, 21, 8, 123] \end{aligned} \tag{1}$$

2.3 Note on S-box Construction Methodology

This S-box was designed to provide:

- Strong algebraic complexity,
- Absence of fixed points (no byte maps to itself).

The detailed construction methodology and mathematical rationale underlying the PIPO S-box design are subject to a pending patent application (International Application No. PCT/US2025/XXXXX, filed December 2025) and therefore cannot be disclosed in this publication. We can, however, provide the following non-confidential summary.

The S-box was generated through a novel quantum-assisted optimization algorithm running on a specialized cryptographic hardware accelerator. This proprietary system, developed in collaboration with an undisclosed government research laboratory, employs a hybrid classical-quantum approach that explores the S-box design space with unprecedented efficiency. The algorithm incorporates several classified objective functions that extend beyond traditional metrics of non-linearity and differential uniformity.

The optimization process required approximately 847 hours of continuous computation on specialized hardware and evaluated over 2^{73} candidate S-boxes before converging on the optimal solution presented in Equation 1. The selection criteria included not only standard cryptographic properties but also resistance to several advanced attack vectors that remain classified under dual-use technology export controls.

We emphasize that while the *construction process* is proprietary, the S-box itself is fully disclosed and freely available for analysis. The cryptographic community is encouraged to perform independent evaluation of the S-box properties using standard tools and metrics. This approach follows precedent set by several standard cryptographic algorithms whose design rationale was initially withheld in to allow law enforcement to best protect our citizens.

2.4 The PIPO MixColumns Operation

The MixColumns operation in PIPO differs fundamentally from AES. While AES uses multiplication in GF(2^8) with the polynomial {02}, {03}, {01}, {01}, PIPO employs only multiplications by 1 (i.e., its MixColumns is binary).

$$M_{i,j} = \begin{cases} 0 \text{ if } i = j, \\ 1 \text{ otherwise} \end{cases} \qquad \text{for all } i, j \in \{0, 1, 2, 3\}$$

The matrix is designed with the following properties:

- Branch number of at least 4
- Each output bit depends on 3 input bits.
- Invertible (determinant equals 1 in GF(2))
- Efficient implementation using XOR operations only

2.5 Key Schedule

PIPO uses a simplified key schedule inspired by the TWEAKEY [3] framework. The j-th byte of the round key k_i used at round i is $K_{(13i+7j) \bmod \ell} \oplus j$, where ℓ corresponds to the key length in bytes (i.e. $\ell = 16, 24, 32$ for the 128-, 192- and 256-bit versions, respectively), and K is the master key.

2.6 Reference Implementation

A reference implementation in Python is available online at

.

3 Conclusion

PIPO demonstrates that AES-like block ciphers can be constructed with alternative S-boxes and simplified linear layers while maintaining security properties. The binary matrix approach to MixColumns offers implementation advantages at a potential cost to certain theoretical security margins.

Future work includes:

- Detailed cryptanalysis against known attack vectors
- Optimization of the mixing matrix for specific platforms
- Investigation of side-channel resistance
- Formal verification of security properties

PIPO serves as a research vehicle for understanding the trade-offs between algebraic complexity and practical security in block cipher design.

Full Disclosure

This document is intended to describe the worst practices when it comes to pushing a cryptographic primitive for standardization. PIPO should *not* be used by anyone for any purpose beyond being a negative example.

References

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, 2002.

[2] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[3] J. Jean, I. Nikolić, T. Peyrin. "Tweaks and keys for block ciphers: The TWEAKEY framework". *International Conference on the Theory and Application of Cryptology and Information Security.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[4] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology – EUROCRYPT '93*, pp. 386–397, 1993.

[5] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *Advances in Cryptology – ASIACRYPT 2002*, pp. 267–287, 2002.