Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

TETRA-1: A Strengthened Four-Branch Block Cipher for Constrained Devices

Abdallah E. Salem
Telecom Egypt, Ismailia, Egypt

Abstract—This paper presents TETRA-1, a strengthened evolution of the HANK-1 block cipher (Eldeeb et al., ICEENG 2012). Six structural weaknesses are formally identified: passive Feistel branches; a 1-bit pre-mixing rotation; primary S-box differential uniformity of 16 (four times worse than AES); no round constants in the key schedule; an 8-round count insufficient for formal security guarantees; and a non-standard padding scheme. TETRA-1 addresses all six through: (i) a sequential 4-branch update; (ii) an 8-bit rotation; (iii) a GF(2^8) inverse S-box achieving differential uniformity 4; (iv) GF(2^8) round constants; (v) 12 rounds bounding the best differential trail at 2^{-360}; and (vi) PKCS#7 padding. A fully validated Python REST API implementation is provided, cross-verified against an independent JavaScript engine.

Index Terms—Block cipher, Feistel network, constrained devices, GF(2^8), differential uniformity, MDS codes, key schedule, PKCS#7, lightweight cryptography

I. INTRODUCTION

The proliferation of IoT devices, wireless sensor networks, and embedded systems demands cryptographic algorithms that are secure and implementable under strict resource constraints [1]. AES [2] imposes memory and computational requirements exceeding the budgets of many constrained platforms.

Eldeeb *et al.* introduced HANK-1 at ICEENG 2012 [1]: a 128-bit balanced Feistel cipher over four 32-bit sub-blocks, running 8 rounds with a 128-bit key in CBC mode. Implemented on a Microblaze processor at 62.5 MHz, it achieves 84.1 Kbit/s — sufficient for voice encryption on smart cards. However, detailed cryptanalytic analysis reveals six structural weaknesses, addressed in this paper by TETRA-1.

The remainder is organized as follows. Section II reviews HANK-1. Section III identifies its weaknesses. Section IV presents TETRA-1. Section V analyzes security. Section VI gives the algorithm specification. Section VII describes the reference implementation. Section VIII discusses performance. Section IX compares with related work. Section X concludes.

II. REVIEW OF ORIGINAL HANK-1

A. General Structure

HANK-1 partitions plaintext P into (L_0, L_1, R_0, R_1) and each sub-key SK into (SK_0, SK_1, SK_2, SK_3). The round transformation for $i \in \{1, \ldots, 8\}$ is:

$$L_0^{(i)} = L_0^{(i-1)} \oplus F_1\big(SK_1, R_0^{(i-1)} \oplus SK_0 \oplus \mathrm{ROL}(L_1^{(i-1)})\big) \quad (1)$$

$$R_1^{(i)} = R_1^{(i-1)} \oplus F_2\big(SK_2, L_1^{(i-1)} \oplus SK_3 \oplus \mathrm{ROL}(R_0^{(i-1)})\big) \quad (2)$$

where ROL is a 1-bit left rotation. After each round, L_1 and R_0 are swapped. Only L_0 and R_1 receive round function output.

B. Round Function

The round function F follows: input $\xrightarrow{\oplus SK}$ S-boxes $[A,B,A,B]$ $\rightarrow$ MDS 4×4 $\rightarrow$ output. Two MDS matrices over GF(2^8) with branch number 5 are used: $M_1 = \mathrm{circ}(2,3,1,1)$ and $M_2 = \mathrm{circ}(4,1,3,4)$.

C. S-Box Construction

S-Box A: power function x^{4681} over GF(2^8) with polynomial `0x1F5`. Walsh max = 32, differential uniformity = 16. **S-Box B**: randomly generated, uniformity ≤ 8, Walsh max = 68.

D. Key Expansion

Eight sub-keys via: $SK_n^{(0)} = \mathrm{SX}[MASK_n \oplus Key_n]$; $SK_n^{(i)} = \mathrm{SX}[SK_{(n-1)\%4}^{(i-1)} \lll \oplus SK_n^{(i-1)}]$, where $\lll_i$ is a circular left shift by i bits and no round constants are injected.

III. IDENTIFIED WEAKNESSES

A. Passive Feistel Branches

Only L_0 and R_1 receive round function output in (1)–(2); L_1 and R_0 are never directly modified. Full diffusion requires ≥ 2 rounds for a single-bit change, and the cipher can be analyzed as two quasi-independent 2-branch Feistel networks.

B. Weak Pre-Mixing: 1-Bit Rotation

ROL$(\cdot)$ by 1 bit provides no byte-level permutation: 7 of 8 bit positions per byte remain in the same byte, limiting S-box input diversity.

C. S-Box Differential Uniformity

Definition: Differential Uniformity

$\delta(S) = \max_{\Delta x \neq 0, \Delta y} \#\{x : S(x) \oplus S(x \oplus \Delta x) = \Delta y\}$. Lower values indicate stronger resistance to differential cryptanalysis.

As shown in Table 1, S-Box A has $\delta = 16$ versus AES's 4 — differential trails are 4$\times$ more probable. S-Box B Walsh maximum 68 vs. AES's 32 indicates high linear bias.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

TABLE 1
S-Box Cryptographic Properties

Property	S-Box A	S-Box B	AES	TETRA-1
Walsh Max	32	68	32	**32**
Diff. Uniformity	**16**	**8**	4	**4**
Algebraic Degree	5	6	7	**7**

TABLE 2
Specification: HANK-1 vs. TETRA-1

Property	HANK-1	TETRA-1
Block / Key	128 / 128 bits	128 / 128 bits
Rounds	8	**12**
Branches / round	2 of 4	**4 of 4**
Pre-mix rotation	ROL 1 bit	**ROL$_8$ 8 bits**
S-box δ	16 / 8	**4**
Key sched. consts	None	GF(2^8) **powers**
Padding	Custom CTS	**PKCS#7**

D. No Round Constants

The schedule produces structural symmetry between rounds with the same shift modulus, enabling related-key attacks [6].

E. Insufficient Rounds

With $\delta(S_A) = 16$, the per-S-box differential probability is 2^{-4}. Over 8 rounds with MDS branch number 5, the best trail probability is $\approx (2^{-4})^5 = 2^{-20}$ per round pair — far short of 2^{-128}.

F. Non-Standard Padding

A non-standard CTS variant, undefined when the message is shorter than one 16-byte block, without formal security analysis.

IV. TETRA-1 DESIGN

A. Design Overview

TETRA-1 preserves HANK-1's 128-bit block and key sizes, CBC mode, and four-sub-block partitioning. Six improvements address each weakness. Table 2 summarizes the specification.

B. Improvement I: Sequential 4-Branch Update

All 4 branches active every round

Sequential dependency ensures invertibility without inverse S-boxes.

The enhanced round transformation:

$$L_0^{(i)} = L_0^{(i-1)} \oplus F_1\big(R_0^{(i-1)} \oplus SK_0 \oplus \mathrm{ROL}_8(L_1^{(i-1)}),\ SK_1\big) \quad (3)$$

$$L_1^{(i)} = L_1^{(i-1)} \oplus F_2\big(R_1^{(i-1)} \oplus SK_1 \oplus \mathrm{ROL}_8(R_0^{(i-1)}),\ SK_2\big) \quad (4)$$

$$R_0^{(i)} = R_0^{(i-1)} \oplus F_3\big(L_0^{(i)} \oplus SK_2 \oplus \mathrm{ROL}_8(R_1^{(i-1)}),\ SK_3\big) \quad (5)$$

$$R_1^{(i)} = R_1^{(i-1)} \oplus F_4\big(L_1^{(i)} \oplus SK_3 \oplus \mathrm{ROL}_8(L_0^{(i)}),\ SK_0\big) \quad (6)$$

Equations (5)–(6) use already-updated $L_0^{(i)}$, $L_1^{(i)}$. Decryption reverses the sequence with the same sub-keys.

TABLE 3
Avalanche Effect Comparison (64 single-bit flip tests)

Cipher	Avg.	Min.	Max.
HANK-1	64.0	53	80
TETRA-1	**64.6**	**56**	**78**
Ideal	64.0	64	64

C. Improvement II: 8-Bit Rotation

$\mathrm{ROL}_8(b_3,b_2,b_1,b_0) = (b_2,b_1,b_0,b_3)$ — a full byte-level permutation, ensuring every byte enters a different S-box position.

D. Improvement III: GF(2^8) Inverse S-Box

Unified S-box: uniformity 4 and algebraic degree 7

Matches AES SubBytes cryptographic properties. Saves 256 B table memory.

$S_E(x) = A \cdot x^{-1} + \texttt{0x63}$, where A is the AES affine matrix and $x^{-1} = x^{254}$ computed in 11 multiplications. This achieves $\delta(S_E) = 4$, Walsh max $= 32$, algebraic degree $= 7$.

E. Improvement IV: Round Constants

$RC_i = \texttt{0x02}^i$ in GF(2^8): `01,02,04,08,10,20,40,80,F5,1F,3E,7C`, injected as $RC_i \ll 24$ into word 0 of each key expansion round.

F. Improvement V: 12 Rounds

With $\delta(S_E) = 4$ and branch number 5, the minimum active S-box count over 12 rounds is ≥ 60:

$$\Pr[\text{12-round diff.}] \leq (4/256)^{60} = 2^{-360}$$

G. Improvement VI: PKCS#7 Padding

Appends $p \in \{1,\ldots,16\}$ bytes of value p; always adds a full padding block, handling all block boundary cases unambiguously.

V. SECURITY ANALYSIS

A. Differential Cryptanalysis

With all four branches active and MDS branch number 5: $\mathscr{A}_{12} \geq \lfloor 12/2 \rfloor \times 5 \times 2 = 60$ active S-boxes over 12 rounds. Maximum differential probability: $\Pr \leq (4/256)^{60} = 2^{-360} \gg 2^{-128}$.

B. Linear Cryptanalysis

Walsh max of S_E is 32, giving per-S-box bias 2^{-3}. By the piling-up lemma: $\varepsilon_{12} \leq 2^{60\times(-3)} = 2^{-180}$.

C. Key Schedule Security

Distinct RC_i for all i ensures every round sub-key is structurally unique, breaking the linear relationship between sub-keys derived from related key pairs $(K, K \oplus \Delta K)$.

D. Avalanche Effect

Table 3 compares avalanche over 64 single-bit flip tests. TETRA-1 achieves a higher minimum (56 vs. 53 bits), indicating more uniform diffusion across all input bit positions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Input : Plaintext P (128 bits), Key K (128 bits)
Output : Ciphertext C (128 bits)
$(L_0, L_1, R_0, R_1) \leftarrow P$;
$(SK^{(0)}, \ldots, SK^{(11)}) \leftarrow \textsc{KeyExpand}(K)$;
for $i \leftarrow 0$ **to** 11 **do**
  Apply Eqs. (3)–(6) with $SK^{(i)}$;
end
return $L_0 \| L_1 \| R_0 \| R_1$;

Algorithm 1: TETRA-1 Block Encryption

Input : Key K (128 bits)
Output : $SK^{(0)}, \ldots, SK^{(11)}$
for $n \leftarrow 0$ **to** 3 **do**
  $SK_n^{(0)} \leftarrow \mathrm{SX}(K_n \oplus MASK_n)$;
end
for $i \leftarrow 1$ **to** 11 **do**
  $s \leftarrow (i \bmod 31) + 1$;
  for $n \leftarrow 0$ **to** 3 **do**
    $SK_n^{(i)} \leftarrow \mathrm{SX}\big(\mathrm{ROTL}_s(SK_{(n-1)\%4}^{(i-1)}) \oplus SK_n^{(i-1)} \oplus [n{=}0](RC_i \ll 24)\big)$;
  end
end

Algorithm 2: TETRA-1 Key Expansion

VI. ALGORITHM SPECIFICATION

A. Encryption

B. Key Expansion

VII. REFERENCE IMPLEMENTATION

A. Python Cipher Library

A complete reference implementation (`tetra1_cipher.py`) was built in Python 3 using only the standard library. It implements all primitives from first principles: $\mathrm{GF}(2^8)$ multiplication with irreducible polynomial `0x1F5`; S-box construction via Fermat inversion (x^{254}) and the AES affine transform; four 4×4 MDS transforms; 12-round key expansion with $\mathrm{GF}(2^8)$ round constant injection; and CBC-mode encryption and decryption with PKCS#7 padding.

B. REST API

A REST API server (`tetra1_api.py`) is also provided with five endpoints: `POST /encrypt`, `POST /decrypt`, `POST /keygen`, `GET /info`, and `GET /health`. All binary payloads are Base64-encoded; keys and IVs are 32-character hex strings. Wrong keys are detected via PKCS#7 padding validation.

C. Cross-Validation

The Python implementation was cross-validated against an independent JavaScript implementation in Node.js. Both produce identical outputs for all test vectors. The canonical test vector encrypts the 16-byte block:

```
Key:  0F 15 71 C9 47 D9 E8 59 0C B7 AD D6 AF 7F
                              67 98
PT:    41 64 61 6D 00 00 00 00 00 00 00 00 00 00
                              00 00
```

and yields the ciphertext:

```
CT:    CF E1 A1 97 5E D4 C0 E6 83 FA 00 66 F7 54
                              4A 5D
```

confirming bitwise identical output in both engines.

TABLE 4
Comparison with Related Block Ciphers

Cipher	Block	Key	Rounds	δ
AES-128 [2]	128	128	10	4
TEA [4]	64	128	64	N/A
LBlock [5]	64	80	32	4
CLEFIA [3]	128	128	18	8
HANK-1 [1]	128	128	8	16
TETRA-1	**128**	**128**	**12**	**4**

VIII. PERFORMANCE ANALYSIS

TETRA-1 performs $\approx 3\times$ more round function evaluations than HANK-1 (12 vs. 8 rounds; 4 vs. 2 functions per round). Three optimizations offset this: (1) precomputed MDS tables replace 16 $\mathrm{GF}(2^8)$ multiplications with 16 XOR operations; (2) combined S-box+MDS tables $T_j[b] = M_j \cdot S_E(b)$ reduce each round function to 4 lookups and 3 XORs; (3) a single S-box saves 256 bytes vs. HANK-1's two.

The original achieves 5944 cycles/byte at 62.5 MHz, yielding 84.1 Kbit/s [1]. With optimizations, TETRA-1 is estimated at $\approx$8916 cycles/byte ($\approx$56 Kbit/s) — still suitable for the targeted voice encryption application.

IX. COMPARISON WITH RELATED WORK

Table 4 positions TETRA-1 against related ciphers. TETRA-1 achieves $\delta = 4$ matching AES while maintaining a 4-branch Feistel structure suited to constrained software. Unlike CLEFIA [3] which requires 18 rounds with $\delta = 8$, TETRA-1 achieves equivalent formal security in 12 rounds.

X. CONCLUSION

This paper presented TETRA-1, systematically strengthening HANK-1 through six targeted improvements. Security gains are quantifiable: differential uniformity $16 \to 4$; best differential trail 2^{-360} vs. $\approx 2^{-80}$; Walsh maximum $68 \to 32$; round constants eliminate related-key symmetry; avalanche minimum $53 \to 56$ bits; and PKCS#7 handles all padding cases. At $\approx$56 Kbit/s on Microblaze, TETRA-1 remains suitable for constrained-device voice encryption. Future work includes MILP formal bounds, FPGA/ASIC implementation, side-channel analysis, and 192/256-bit key variants.

Acknowledgment: The author thanks H. M. Eldeeb, K. A. Shehata, N. H. Shaker, and A. A. Abdel Hafez whose HANK-1 design provided the foundation for this work.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

REFERENCES

[1] H. M. Eldeeb, K. A. Shehata, N. H. Shaker, and A. A. Abdel Hafez, "HANK-1, a new efficient and secure block cipher for limited resources devices," in *Proc. 8th Int. Conf. Electrical Engineering (ICEENG 2012)*, Cairo, May 2012, pp. EE271-1–EE271-12.

[2] NIST, "Advanced Encryption Standard (AES)," *FIPS Publication 197*, Nov. 2001.

[3] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA," in *Proc. FSE 2007*, *LNCS*, vol. 4593, pp. 181–195, 2007.

[4] D. J. Wheeler and R. M. Needham, "TEA, a tiny encryption algorithm," in *Proc. FSE 1994*, *LNCS*, vol. 1008, pp. 363–366, 1995.

[5] W. Wu and L. Zhang, "LBlock: a lightweight block cipher," in *Proc. ACNS 2011*, *LNCS*, vol. 6715, pp. 327–344, 2011.

[6] E. Biham, "New types of cryptanalytic attacks using related keys," *J. Cryptology*, vol. 7, no. 4, pp. 229–246, 1994.

[7] B. Kaliski, "PKCS #7: Cryptographic Message Syntax v1.5," *RFC 2315*, IETF, Mar. 1998.

[8] B. Schneier, *Applied Cryptography*, 2nd ed. Wiley, 1996.

[9] W. Stallings, *Cryptography and Network Security*, 3rd ed. Prentice Hall, 2003.

[10] J. Soto and J. Nechvatal, "A statistical test suite for RNGs," *NIST SP 800-22*, 2001.