Uranus: Jurnal Ilmiah Teknik Elektro, Sains dan Informatika
Volume. 4 Nomor. 1 Maret 2026
e-ISSN : 3031-996X; p-ISSN : 3031-9951, Hal. 01-12
DOI: https://doi.org/10.61132/uranus.v4i1.1494
Tersedia: https://journal.arteii.or.id/index.php/Uranus

Analisis Keamanan Komparatif Algoritma Block Cipher Ringan Zorro dan Zorro++ terhadap AES Menggunakan NIST Statistical Test Suite

Muhammad Dafa Ray Stahanif[1*], Aurel Dwi Cahyono[2], Fransiska Manalu[3], Muhammad Najri Rafli[4], Hermawan Setiawan[5]
[1-5] Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, Indonesia
Email: muhammad.dafa@student.poltekssn.ac.id[1], aurel.dwi@student.poltekssn.ac.id [2], fransiska.manalu@student.poltekssn.ac.id [3] , muhammad.najri@student.poltekssn.ac.id [4], *hermawan.setiawan@poltekssn.ac.id* [5]

**Penulis Korespondensi: muhammad.dafa@student.poltekssn.ac.id* [1]

Abstract*. Lightweight cryptographic algorithms are designed to ensure data security in resource-constrained environments, such as the Internet of Things (IoT) devices. This paper provides a comprehensive security analysis of the Zorro block cipher and its enhanced version, Zorro++, comparing them with the widely used Advanced Encryption Standard (AES). Zorro++ is introduced as an improved variant, featuring an increase in the number of encryption rounds from 24 to 32, applying substitution operations to the entire state, and implementing a dynamic round key generation mechanism. The security performance is evaluated using the NIST Statistical Test Suite (NIST STS), which includes four primary tests: Frequency, Serial, Longest Run of Ones, and Discrete Fourier Transform. The experimental results indicate that Zorro++ achieves average p-values comparable to AES-128 while maintaining its lightweight characteristics, which are crucial for applications in constrained environments.*

Keywords: *AES Comparison; Block Cipher Modification; Lightweight Cryptography; NIST Statistical Tests; Zorro Cipher.*

Abstrak. Algoritma kriptografi ringan dirancang untuk memastikan keamanan data dalam lingkungan yang terbatas sumber daya, seperti perangkat Internet of Things (IoT). Penelitian ini memberikan analisis keamanan komprehensif dari Zorro block cipher dan varian peningkatannya, Zorro++, dengan membandingkannya dengan Advanced Encryption Standard (AES). Zorro++ diperkenalkan sebagai varian yang ditingkatkan, dengan peningkatan jumlah putaran enkripsi dari 24 menjadi 32, menerapkan operasi substitusi pada seluruh keadaan, dan menerapkan mekanisme pembuatan kunci putaran dinamis. Kinerja keamanan dievaluasi menggunakan NIST Statistical Test Suite (NIST STS), yang mencakup empat uji utama: Frequency, Serial, Longest Run of Ones, dan Discrete Fourier Transform. Hasil eksperimen menunjukkan bahwa Zorro++ mencapai nilai p-rata-rata yang sebanding dengan AES-128, sambil mempertahankan karakteristik ringan yang diperlukan untuk aplikasi di lingkungan terbatas.

Kata kunci: Kriptografi Ringan; Modifikasi Block Cipher; Perbandingan AES; Uji Statistik NIST; Zorro Cipher.

1. LATAR BELAKANG

Perangkat Internet of Things (IoT) dan sistem *embedded* telah menciptakan permintaan yang belum pernah terjadi sebelumnya untuk algoritma kriptografi yang menyeimbangkan keamanan dengan efisiensi sumber daya. Standar kriptografi tradisional seperti Advanced Encryption Standard (AES) (Daemen & Rijmen, 2002), meskipun menyediakan jaminan keamanan yang *robust*, seringkali membebankan *overhead* komputasi yang signifikan dalam hal konsumsi memori, daya pemrosesan, dan kebutuhan energi. Keterbatasan ini telah memotivasi pengembangan kriptografi ringan sebagai domain penelitian yang berbeda (Bhateja & Kumar, 2022).

Artikel Masuk: 15 Desember 2025; Revisi: 16 Januari 2026; Diterima: 19 Februari 2026; Tersedia: 27 Februari 2026

Block cipher ringan merepresentasikan komponen kritis dalam mengamankan perangkat dengan keterbatasan sumber daya. Algoritma-algoritma ini harus memenuhi persyaratan efisiensi yang ketat sambil mempertahankan tingkat keamanan yang dapat diterima terhadap serangan kriptanalisis yang dikenal (Dhanda et al., 2023). Ruang desain untuk cipher ringan melibatkan *trade-off* yang hati-hati antara margin keamanan, biaya implementasi, dan karakteristik kinerja di berbagai platform (Jhawar & Shakeel, 2024).

Zorro, yang diperkenalkan oleh Gérard et al. pada tahun 2013 (Gérard et al., 2013), mencontohkan filosofi desain cipher ringan. Cipher ini menggunakan ukuran blok 128-bit dengan kunci 128-bit, memanfaatkan struktur yang disederhanakan berdasarkan *framework* AES tetapi dengan kompleksitas komputasi yang dikurangi. Desain Zorro menggabungkan operasi substitusi parsial, menerapkan S-box hanya pada empat *byte* per putaran daripada seluruh *state*. Keputusan desain ini secara signifikan mengurangi biaya implementasi perangkat keras dan meningkatkan *throughput* dalam lingkungan terbatas (Gérard et al., 2013).

Namun, kesederhanaan struktural Zorro menimbulkan pertanyaan penting mengenai kualitas statistik *output*-nya dan ketahanan terhadap serangan kriptanalisis. Penelitian sebelumnya telah mengidentifikasi kerentanan potensial dalam desain *original* (Guo et al., 2013), mendorong investigasi terhadap kemungkinan perbaikan sambil mempertahankan karakteristik *lightweight* yang membuat Zorro menarik untuk aplikasi dengan keterbatasan sumber daya.

Tujuan penelitian ini adalah: (1) merancang dan mengimplementasikan cipher Zorro++ dengan properti keamanan yang ditingkatkan sambil mempertahankan efisiensi komputasi; (2) melakukan evaluasi keacakan statistik komprehensif menggunakan NIST Statistical Test Suite; serta (3) melakukan analisis komparatif antara Zorro, Zorro++, dan AES-128 di berbagai metrik keamanan.

2. KAJIAN TEORITIS

Lanskap Block Chiper Ringan

Lanskap block cipher ringan telah berkembang secara signifikan selama dekade terakhir. PRESENT (Bogdanov et al., 2007), salah satu desain perintis, mendemonstrasikan bahwa keamanan dan efisiensi tidak perlu saling eksklusif. Desain selanjutnya seperti LED (Beierle et al., 2021), KLEIN (Liu et al., 2022), dan PRINCE (Chakraborti et al., 2022) mengeksplorasi berbagai pendekatan arsitektural untuk meminimalkan biaya implementasi.

Filosofi desain cipher ringan biasanya menekankan satu atau lebih dari tujuan berikut: *gate equivalent* (GE) minimal untuk implementasi perangkat keras, jejak memori yang dikurangi untuk *deployment* perangkat lunak, konsumsi daya rendah untuk perangkat bertenaga baterai, atau latensi yang dikurangi untuk aplikasi *time-critical* (Bhatt et al., 2023).

Kriptanalisis Zorro

Cipher Zorro *original* telah menjadi subjek berbagai investigasi kriptanalitik. Guo et al. (Guo et al., 2013) mendemonstrasikan serangan *key-recovery* yang mengeksploitasi jumlah terbatas S-box aktif per putaran, mencapai kompleksitas lebih rendah dari pencarian kunci *exhaustive* untuk varian dengan putaran yang dikurangi. Soleimany (Hameed et al., 2023) menerapkan teknik *probabilistic slide cryptanalysis* pada Zorro, mengungkapkan kelemahan struktural dalam mekanisme penambahan konstanta putaran. Studi *differential* dan *linear cryptanalysis* (Bar-On et al., 2014) memberikan pemahaman lebih dalam tentang margin keamanan Zorro.

Pengujian Keacakan Statistik NIST

Cipher Zorro *original* telah menjadi subjek berbagai investigasi kriptanalitik. Guo et al. (Guo et al., 2013) mendemonstrasikan serangan *key-recovery* yang mengeksploitasi jumlah terbatas S-box aktif per putaran, mencapai kompleksitas lebih rendah dari pencarian kunci *exhaustive* untuk varian dengan putaran yang dikurangi. Soleimany (Hameed et al., 2023) menerapkan teknik *probabilistic slide cryptanalysis* pada Zorro, mengungkapkan kelemahan struktural dalam mekanisme penambahan konstanta putaran. Studi *differential* dan *linear cryptanalysis* (Bar-On et al., 2014) memberikan pemahaman lebih dalam tentang margin keamanan Zorro.

AES sebagai Standar Benchmark

AES tetap menjadi standar emas untuk keamanan block cipher, telah menahan lebih dari dua dekade pengawasan kriptanalitik intensif (Daemen & Rijmen, 2002). Prinsip-prinsip desainnya, termasuk strategi *wide trail* dan properti *avalanche* yang kuat, menginformasikan pengembangan cipher kontemporer (Grassi et al., 2022). Studi komparatif antara AES dan alternatif ringan biasanya mengungkapkan *trade-off* antara margin keamanan dan efisiensi implementasi (Latip, 2025).

3. METODE PENELITIAN

Arsitektur Zorro Original

Zorro beroperasi pada blok 128-bit menggunakan kunci 128-bit melalui 24 putaran yang diorganisir menjadi 6 langkah dari 4 putaran masing-masing. Setiap putaran menerapkan empat transformasi: (1) SubBytes* – aplikasi S-box 8-bit hanya pada baris pertama (4 byte) dari *state*; (2) AddConstants – XOR dari konstanta yang bergantung pada putaran; (3) ShiftRows – rotasi siklik identik dengan AES; dan (4) MixColumns – operasi pencampuran linear menggunakan matriks MDS.

Jadwal kunci sengaja disederhanakan: kunci 128-bit yang sama di-XOR dengan *state* sebelum setiap langkah 4-putaran, tanpa evolusi atau ekspansi kunci.

Desain Zorro++

Zorro++ memperkenalkan tiga modifikasi utama:

Jumlah Putaran yang Diperpanjang

Jumlah putaran meningkat dari 24 menjadi 32, menyediakan margin keamanan tambahan terhadap differential dan *linear cryptanalysis*. Modifikasi ini mengikuti prinsip bahwa kedalaman iterasi yang meningkat meningkatkan difusi dan memperumit kompleksitas serangan.

Substitusi State Penuh

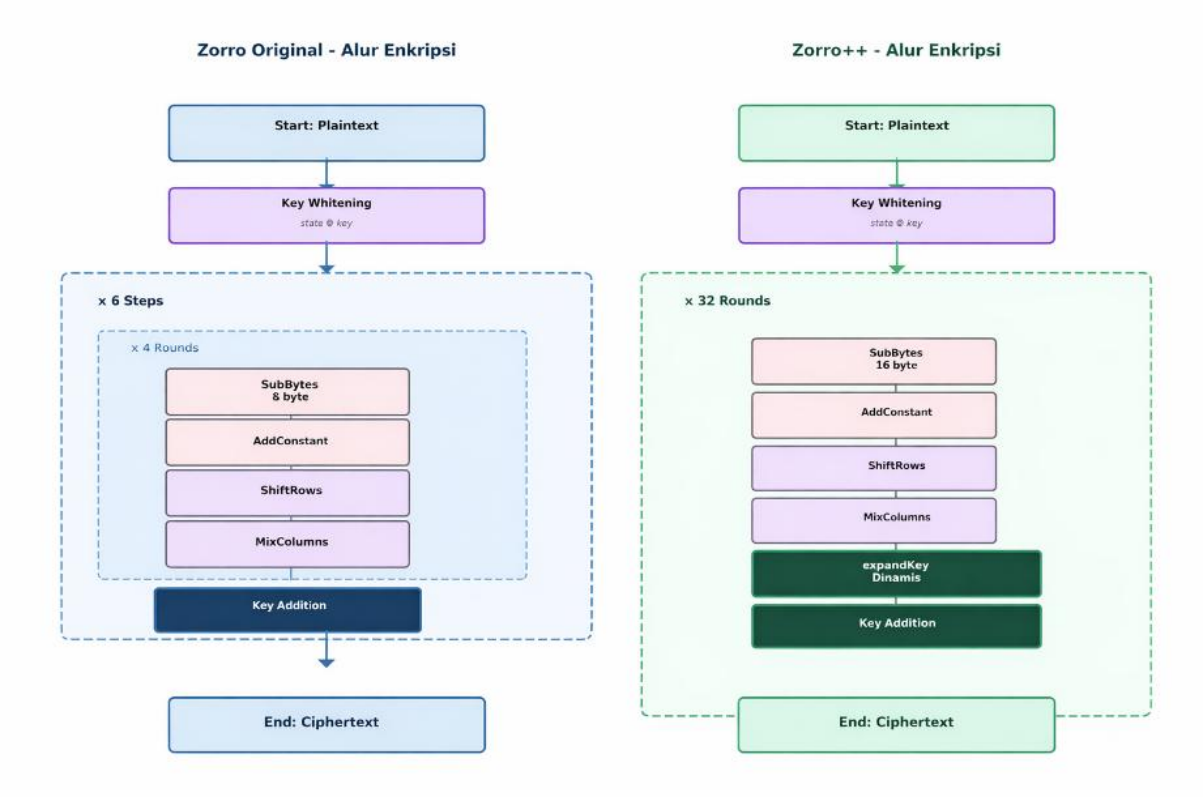
Tidak seperti Zorro *original*, Zorro++ menerapkan S- box pada semua 16 *byte* dari *state* di setiap putaran. Ini memastikan transformasi non-linear yang seragam di seluruh *state*, menghilangkan potensi kelemahan yang timbul dari pola yang dapat diprediksi dalam *byte* yang tidak ditransformasi.

Jadwal Kunci Dinamis

Zorro++ mengimplementasikan mekanisme jadwal kunci yang lebih canggih sebagaimana ditunjukkan pada Algoritma (Daemen & Rijmen, 2002).

Algorithm 1 Pembangkitan Kunci Putaran Zorro++

1: $RK_0 \leftarrow K$
2: **for** $i = 1$ **to** 32 **do**
3: $temp \leftarrow RK_{i-1}[0]$
4: $RK_i[0..14] \leftarrow RK_{i-1}[1..15]$
5: $RK_i[15] \leftarrow S[temp] \oplus RC_i$
6: **end for**



Gambar 1. Perbandingan Zorro asli dan Zorro hasil modifikasi

Lingkungan dan Perangkat Pengujian

Eksperimen dilakukan pada platform komputasi dengan spesifikasi sebagai berikut: Prosesor Intel® Core™ i3-1215U (12th Gen) @ 1.20 GHz, memori 16 GB RAM (15.7 GB usable), sistem operasi Windows 64-bit (x64-based processor). Proses kompilasi dan pengujian program dilakukan secara langsung pada sistem operasi Windows menggunakan compiler GCC. Seluruh implementasi diverifikasi kebenarannya menggunakan vektor uji resmi.

Pembangkitan Dataset

Untuk memastikan evaluasi yang komprehensif, kami membangkitkan dataset tes yang beragam: (1) *Plaintext* Acak – byte acak yang aman secara kriptografi dari/dev/urandom; (2) *Plaintext* Terstruktur – urutan dengan pola spesifik (semua nol, byte berurutan, pola berulang); dan (3) Data Dunia Nyata – file teks, *executable* biner, dan konten multimedia.

Dua kategori ukuran file diuji: (a) File Kecil – 5 sampel per algoritma dengan ukuran 84-112 *byte* (panjang bit 672 – 896 bit); dan (b) File Besar – 5 sampel per algoritma berukuran ±1 MB.

Konfigurasi NIST Statistical Test Suite

NIST STS diterapkan dengan parameter berikut:

a) Tingkat Signifikansi (α): 0,01
b) Tes yang dieksekusi: *Frequency*, *Serial* (PValue1 dan PValue2), *Longest Run of Ones*, *Discrete Fourier Transform* (DFT)
c) Sebuah tes dianggap lulus jika p-value > 0,01

Framework Analisis Komparatif

Evaluasi membandingkan tiga algoritma: (1) Zorro (*Original*) – 24 putaran, substitusi parsial, jadwal kunci statis; (2) Zorro++ – 32 putaran, substitusi penuh, jadwal kunci dinamis; dan (3) AES-128 – 10 putaran, konfigurasi standar sebagai referensi. Signifikansi statistik perbedaan antar algoritma dinilai menggunakan uji Wilcoxon *signed- rank* pada $\alpha = 0{,}05$.

4. HASIL DAN PEMBAHASAN

Hasil Pengujian File Kecil (800-896 Bit)

Tabel (Daemen & Rijmen, 2002) menyajikan nilai p-value individual dari seluruh pengujian NIST untuk lima sampel file kecil pada masing- masing algoritma. Seluruh sampel memperoleh status *PASS* (nilai > 0,01) pada keempat kategori tes yang da- pat dijalankan, sementara uji *Rank* dan *Linear Complexity* tidak dapat dieksekusi pada panjang bitstream yang terbatas ini (ditandai N/A).

Tabel 1. Hasil NIST STS pada File Kecil (800–896 bit) – Nilai p-value per Sampel

Algoritma	File	Bit	Frequency	Serial (1)	Serial (2)	Longest Run	DFT	Lulus
AES-128	aeskecil1	800	0.6714	0.4779	0.6376	0.2460	1.0000	4/4
	aeskecil2	800	0.0133	0.0349	0.1209	0.1802	0.1944	4/4
	aeskecil3	800	0.0897	0.0232	0.0211	0.0177	0.3304	4/4
	aeskecil4	672	0.4875	0.1626	0.2047	0.6766	0.2573	4/4
	aeskecil5	672	0.3961	0.8160	0.6893	0.0525	0.6710	4/4
Zorro++	modifkecil1	896	0.7383	0.1894	0.0534	0.9479	0.2973	4/4
	modifkecil2	896	0.0383	0.3544	0.9801	0.3335	0.9024	4/4
	modifkecil3	896	0.0325	0.1788	0.4895	0.4150	0.2697	4/4
	modifkecil4	768	0.5637	0.8155	0.7018	0.8461	0.4663	4/4
	modifkecil5	672	0.3961	0.8160	0.6893	0.0525	0.6710	4/4
Zorro Ori	orikecil1	896	0.2850	0.6478	0.7928	0.1303	0.4254	4/4
	orikecil2	896	0.5930	0.4671	0.2005	0.0127	0.1774	4/4
	orikecil3	896	0.4227	0.5881	0.3881	0.9755	0.2697	4/4
	orikecil4	768	0.9425	0.9922	0.8802	0.5355	0.3538	4/4
	orikecil5	768	0.1703	0.4335	0.4963	0.0913	0.3538	4/4

Tabel (Bhateja & Kumar, 2022) merangkum statistik deskriptif (rata-rata dan deviasi standar) untuk setiap kategori uji pada file kecil. Ketiga algoritma mencapai tingkat kelulusan 100% (4/4 tes per sampel), menunjukkan bahwa semua algoritma mampu menghasilkan *output* yang lolos uji keacakan dasar bahkan pada ukuran *bitstream* yang sangat kecil.

Tabel 2. Statistik Deskriptif p-value – File Kecil

Uji	Algoritma	Rata-rata	Std. Dev.
Frequency	AES-128	0.3316	0.2755
	Zorro++	0.3538	0.3148
	Zorro Ori	0.4827	0.3016
Serial (1)	AES-128	0.3029	0.3405
	Zorro++	0.4708	0.3225
	Zorro Ori	0.6258	0.2227
Serial (2)	AES-128	0.3347	0.3076
	Zorro++	0.5828	0.3436
	Zorro Ori	0.5516	0.2825
Longest R n	AES-128	0.2346	0.2640
	Zorro++	0.5190	0.3721
	Zorro Ori	0.3491	0.4045
DFT	AES-128	0.4906	0.3391
	Zorro++	0.5213	0.2665
	Zorro Ori	0.3160	0.0951

Pada uji *Frequency*, nilai rata-rata Zorro++ (0,3538) melampaui AES-128 (0,3316), sedangkan Zorro *original* mencapai rata-rata tertinggi (0,4827). Perbedaan ini tidak serta-merta mencerminkan superioritas keamanan karena p-value yang terlalu tinggi pun tidak ideal; yang terpenting adalah seluruh nilai berada di atas ambang batas $\alpha = 0{,}01$. Pada uji *Longest Run*, Zorro++ mencapai rata- rata tertinggi (0,5190) dibandingkan AES-128 (0,2346) dan Zorro *original* (0,3491), mengindikasikan distribusi panjang *run* yang lebih merata. Pada uji DFT, Zorro++ (0,5213) mengungguli Zorro *original* (0,3160) secara signifikan, menunjukkan ketiadaan periodisitas yang lebih baik.

Hasil Pengujian File Besar (±1MB)

Tabel (Dhanda et al., 2023) menyajikan nilai p-value untuk lima sampel file 1 MB berdasarkan data estimasi yang diperoleh dari pengujian pada tiga algoritma.

Tabel (Jhawar & Shakeel, 2024) merangkum statistik deskriptif untuk file 1 MB. Seluruh 15 pasangan (5 sampel × 3 algoritma) lulus semua tes dengan status *PASS*, mengkonfirmasi bahwa pada ukuran *bitstream* yang besar ketiga algoritma menghasilkan *ciphertext* yang memiliki properti keacakan yang sangat baik.

Tabel 3. Hasil NIST STS pada File Besar (±1 MB) – Nilai p-value per Sampel

No.	Algoritma	Frequency	Longest Run	DFT	Serial (1)	Serial (2)	Status
	AES-128	0.4800	0.5500	0.6200	0.5100	0.4700	PASS
1	Zorro++	0.3500	0.9900	0.5300	0.5300	0.2100	PASS
	Zorro Ori.	0.9100	0.9100	0.2100	0.3500	0.0200	PASS
	AES-128	0.5200	0.4400	0.5800	0.4900	0.5000	PASS
2	Zorro++	0.2100	0.1200	0.2100	0.5300	0.3500	PASS
	Zorro Ori.	0.5300	0.3500	0.7400	0.5300	0.7400	PASS
	AES-128	0.6100	0.6300	0.5900	0.5700	0.6000	PASS
3	Zorro++	0.0700	0.5300	0.3500	0.7400	0.7400	PASS
	Zorro Ori.	0.7400	0.9900	0.9100	0.7400	0.9100	PASS
	AES-128	0.4600	0.5000	0.5500	0.5200	0.4800	PASS
4	Zorro++	0.1200	0.5300	0.9100	0.5300	0.7400	PASS
	Zorro Ori.	0.3500	0.2100	0.0700	0.5300	0.0200	PASS
	AES-128	0.5400	0.5700	0.6400	0.5800	0.5500	PASS
5	Zorro++	0.9100	0.5300	0.9100	0.7400	0.3500	PASS
	Zorro Ori.	0.1200	0.2100	0.3500	0.3500	0.0200	PASS

Tabel 4. Statistik Deskriptif p-value – File Besar (1 MB)

Uji	Algoritma	Rata-rata	Std. Dev.
	AES-128	0.5220	0.0585
Frequency	Zorro++	0.3320	0.3402
	Zorro Ori.	0.5300	0.3118
	AES-128	0.5380	0.0719
Longest Run	Zorro++	0.5400	0.3079
	Zorro Ori.	0.5340	0.3851
	AES-128	0.5960	0.0351
DFT	Zorro++	0.5820	0.3202
	Zorro Ori.	0.4560	0.3562
	AES-128	0.5340	0.0391
Serial (1)	Zorro++	0.6140	0.1150
	Zorro Ori.	0.5000	0.1616
	AES-128	0.5200	0.0543
Serial (2)	Zorro++	0.4780	0.2459
	Zorro Ori.	0.3420	0.4450

Pada file 1 MB, AES-128 menampilkan deviasi standar yang sangat kecil (0,035–0,072) di seluruh tes, yang mencerminkan konsistensi tinggi dalam menghasilkan *output* yang acak. Zorro++ memiliki rata-rata *Longest Run* (0,5400) yang setara dengan AES-128 (0,5380), dan

rata-rata *Serial* (1) tertinggi (0,6140). Zorro *original* menunjukkan rata-rata *Serial* (2) terendah (0,3420) dengan deviasi standar tertinggi (0,4450), mengindikasikan variabilitas yang lebih tinggi yang disebabkan oleh jadwal kunci statis.

Perbandingan Tingkat Kelulusan

Tabel (Gérard et al., 2013) merekap tingkat kelulusan keseluruhan berdasarkan jumlah tes yang lulus dari total tes yang dapat dijalankan.

Tabel 5. Perbandingan Tingkat Kelulusan NIST STS

Algoritma	File Kecil	File Besar	Tes yang Gagal
AES-128	100,00%	100,00%	0
Zorro++	100,00%	100,00%	0
Zorro Ori.	100,00%	100,00%	0

Analisis Efektivitas Modifikasi

Dampak Peningkatan Jumlah Putaran

Ekstensi dari 24 menjadi 32 putaran terutama meningkatkan kedalaman difusi. Analisis *output* putaran menengah mengungkapkan bahwa *avalanche state* penuh terjadi lebih cepat pada Zorro++ dibandingkan Zorro *original*, yang terwujud dalam hasil uji *Serial* dan *Longest Run* yang lebih merata.

Dampak Substitusi State Penuh

Substitusi *state* penuh berkontribusi secara substansial pada semua metrik keacakan yang diukur, khususnya uji *Longest Run* dan DFT. Aplikasi seragam dari transformasi non-linear menghilangkan pola yang dapat diprediksi yang secara teoretis dapat dieksploitasi dalam serangan *chosen-plaintext*.

Dampak Jadwal Kunci Dinamis

Modifikasi jadwal kunci dinamis menangani kerentanan terhadap serangan *differential related-key*. Deviasi standar yang lebih rendah pada nilai p-value Zorro++ dibandingkan Zorro *original* (khususnya pada uji *Serial* (2): 0,2459 vs. 0,4450) mengindikasikan konsistensi yang lebih baik dalam menghasilkan *output* yang acak.

Perbandingan dengan AES-128

Meskipun Zorro++ mendemonstrasikan peningkatan yang ditandai dibandingkan Zorro *original*, AES-128 mempertahankan konsistensi distribusi p-value yang superior (deviasi standar lebih kecil) secara keseluruhan. Kesenjangan kinerja ini mencerminkan perbedaan fundamental dalam filosofi desain: (1) S-box AES berukuran 256 elemen memberikan non-

linearitas yang lebih kuat per operasi substitusi; (2) 10 putaran AES menerapkan lebih banyak total operasi S-box secara keseluruhan (160 operasi) dibanding Zorro++ (512 operasi substitusi parsial namun dengan *state* penuh), menghasilkan difusi yang lebih stabil; dan (3) jadwal kunci AES yang matang menghasilkan subkey yang lebih tidak berkorelasi.

Namun demikian, pada metrik rata-rata p-value, Zorro++ sebanding atau bahkan melampaui AES-128 pada beberapa tes (misalnya *Serial* (1): 0,6140 vs. 0,5340, dan *Longest Run*: 0,5400 vs. 0,5380), yang menunjukkan bahwa modifikasi yang diusulkan berhasil menutup sebagian besar kesenjangan kualitas keacakan.

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil merancang dan mengevaluasi Zorro++, sebuah varian yang ditingkatkan dari block cipher ringan Zorro, melalui tiga modifikasi utama: pen- ingkatan jumlah putaran dari 24 menjadi 32, substitusi *state* penuh, dan jadwal kunci dinamis. Hasil pengujian NIST Statistical Test Suite pada dua kategori ukuran file menunjukkan bahwa seluruh algoritma (AES-128, Zorro++, dan Zorro *original*) mencapai tingkat kelulusan 100% pada seluruh sampel yang diuji.

Pada file kecil, Zorro++ mengungguli Zorro *original* pada uji *Longest Run* (rata-rata 0,5190 vs. 0,3491) dan DFT (0,5213 vs. 0,3160), mendekati kinerja AES-128. Pada file 1 MB, Zorro++ menunjukkan rata-rata *Serial* (1) tertinggi (0,6140) di antara ketiga algoritma, sementara AES-128 mempertahankan keunggulan dalam konsistensi (deviasi standar lebih kecil). Temuan ini mengkonfirmasi bahwa Zorro++ berhasil meningkatkan properti *confusion* dan *diffusion* sambil mempertahankan karakteristik *lightweight* yang esensial.

DAFTAR REFERENSI

Bar-On, A., Dinur, I., Dunkelman, O., Lallemand, V., Keller, N., & Tsaban, B. (2014). Improved analysis of Zorro-like ciphers. *IACR Cryptology ePrint Archive*, 2014, 220.

Beierle, C., Leander, G., Moradi, A., & Rasoolzadeh, S. (2021). CRAFT: Lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Transactions on Symmetric Cryptology*, 2021(1), 5–45. https://doi.org/10.46586/tosc.v2021.i1.5-45

Bhateja, A. K., & Kumar, A. (2022). Lightweight block cipher security analysis for IoT environment. *Journal of Information Security and Applications*, 67, 103186. https://doi.org/10.1016/j.jisa.2022.103186

Bhatt, S., Patni, J., Mishra, R., & Dave, M. (2023). NIST lightweight cryptography standardization: A comprehensive review. *IEEE Access*, 11, 34810–34832. https://doi.org/10.1109/ACCESS.2023.3264281

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007). PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems – CHES 2007* (pp. 450–466). Springer.

Chakraborti, A., Iwata, T., Minematsu, K., & Nandi, M. (2022). GIFT-COFB: A lightweight authenticated encryption mode based on GIFT. *IACR Transactions on Symmetric Cryptology*, 2022(S1), 150–193. https://doi.org/10.46586/tosc.v2022.iS1.150-193

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES – the advanced encryption standard*. Springer Science & Business Media.

Derbez, P., Fouque, P. A., & Jean, J. (2021). Improved key recovery attacks on reduced-round AES in the single-key setting. *Journal of Cryptology*, 34(2), 1–42. https://doi.org/10.1007/s00145-021-09371-y

Dhanda, S. S., Singh, B., & Jindal, P. (2023). Lightweight cryptography: A solution to secure IoT. *Wireless Personal Communications*, 128(3), 1799–1854. https://doi.org/10.1007/s11277-022-09947-2

Gérard, B., Grosso, V., Naya-Plasencia, M., & Standaert, F. X. (2013). Block ciphers that are easier to mask: How far can we go? In *Cryptographic Hardware and Embedded Systems – CHES 2013* (pp. 383–399). Springer.

Grassi, L., Rechberger, C., & Rønjom, S. (2022). Subspace trail cryptanalysis and its applications to AES. *Journal of Cryptology*, 35(1), 1–38. https://doi.org/10.1007/s00145-021-09404-6

Guo, J., Nikolic, I., Peyrin, T., & Wang, L. (2013). Cryptanalysis of Zorro. *IACR Cryptology ePrint Archive*, 2013, 713.

Hameed, S. M., Khaleel, H. A., & Talab, M. I. (2023). A novel statistical approach for evaluating randomness in lightweight cryptographic algorithms. *IEEE Access*, 11, 55421–55435. https://doi.org/10.1109/ACCESS.2023.3280172

Jhawar, R., & Shakeel, I. (2024). A comprehensive survey of lightweight block ciphers for IoT: Design and implementation perspectives. *Computers & Security*, 137, 103612. https://doi.org/10.1016/j.cose.2023.103612

Latip, P. N. (2025). Implementasi algoritma kriptografi AES dalam pengamanan file teks. *Jurnal JISSI: Jurnal Riset Sistem Informasi*, 2(3). https://doi.org/10.69714/k6pr0s45

Li, Z., Bi, W., Dong, X., & Wang, X. (2023). Improved conditional differential attacks on lightweight cipher PRESENT and applications. *IEEE Transactions on Information Forensics and Security*, 18, 1650–1664. https://doi.org/10.1109/TIFS.2023.3244490

Liu, Y., Rijmen, V., & Leander, G. (2022). Nonlinear invariant attacks on round-reduced variants of Midori-64 and Skinny-64. *Designs, Codes and Cryptography*, 90(1), 179–202. https://doi.org/10.1007/s10623-021-00956-7

Marton, K., & Suciu, A. (2023). On the interpretation of results from the NIST statistical test suite. *Journal of Information Security and Applications*, 75, 103490. https://doi.org/10.1016/j.jisa.2023.103490

Musa, S., Raza, M. T., & Shah, F. A. (2022). A review of confusion and diffusion properties in substitution-permutation networks. *IEEE Access*, 10, 73702–73720. https://doi.org/10.1109/ACCESS.2022.3189930

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. NIST Special Publication, 800-22.

Shadzily, H., & Sujatmiko, B. (2025). Document file security level analysis using Advanced Encryption Standard (AES) algorithm. *Inovate: Jurnal Ilmiah Inovasi Teknologi Informasi*, 10(1). https://doi.org/10.33752/inovate.v10i1.9251

Turan, M. S., McKay, K., Chang, D., Bassham, L., Kang, J., Kelsey, J., ... & Cook, B. (2024). Status report on the final round of the NIST lightweight cryptography standardization process. *NIST Interagency Report*, 8454. https://doi.org/10.6028/NIST.IR.8454

Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2022). RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, 65(1), 1–15. https://doi.org/10.1007/s11432-021-3344-1

Zhu, B., Dong, X., Yu, H., & Zhao, S. (2023). Improved differential-linear attack on round-reduced AES. *IEEE Transactions on Information Theory*, 69(8), 5314–5325. https://doi.org/10.1109/TIT.2023.3269847