

Analisis Ketahanan Kanal Samping Berbasis Waktu pada Algoritma Kriptografi RSA pada Mikrokontroler ESP32-S3

Naufal Aulia^{1,*}, Rifat Syahba², Refalita Candra³, Ricky Aji Pratama⁴

1) Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, naufal.aulia@student.poltekssn.ac.id

2) Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, rifat.syahba@student.poltekssn.ac.id

3) Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, refalita.candra@student.poltekssn.ac.id

4) Rekayasa Perangkat Keras Kriptografi, Badan Siber dan Sandi Negara, ricky.aji@bssn.go.id

Riwayat Artikel

Dikirim 31 Agu 2026
Diterima 28 Sep 2026
Diterbitkan 1 Okt 2026

Kata kunci:

Analisis Kanal Samping
ESP32-S3
Evaluasi Keamanan
Timing Attack
RSA-2048

Keywords:

ESP32-S3
RSA-2048
Security Evaluation
Side-Channel Analysis
Timing Attack

Abstrak

Perkembangan pesat perangkat IoT meningkatkan adopsi algoritma RSA untuk mengamankan data. Namun, implementasi pada mikrokontroler rentan terhadap *timing attack* yang mengeksploitasi variasi durasi eksekusi untuk mengekstraksi kunci privat. Penelitian ini mengevaluasi ketahanan implementasi RSA 2048-bit pada mikrokontroler ESP32-S3 berbasis mbedTLS dengan *hardware accelerator* aktif melalui tiga skenario pengujian: rasio komputasi enkripsi-dekripsi, *Test Vector Leakage Assessment* (TVLA *Fixed-vs-Random*), dan sensitivitas bobot *Hamming* pada operasi *raw modular exponentiation*. Pengukuran waktu dilakukan pada register siklus clock CPU dengan resolusi 4,167 nanodetik (240 MHz) menggunakan interupsi terisolasi. Hasil menunjukkan waktu enkripsi rata-rata 2.275,00 μ s (SD = 0,25 μ s) dan dekripsi 275.400,00 μ s (SD = 0,50 μ s) dengan rasio 121:1. Uji TVLA menghasilkan $|t| = 0.72$ ($p = 0,471$), berada di bawah ambang batas kritis $|t| < 4,5$ dengan *effect size* Cohen's $d = 0,032$. Uji ANOVA ($F = 1,04$, $p = 0,412$) serta korelasi Pearson ($r = -0,018$) dan Spearman ($p = -0,021$) mengonfirmasi bahwa tidak terdapat ketergantungan waktu terhadap bobot input. Tidak ditemukan bukti statistik *timing leakage* pada implementasi ini, yang mengindikasikan bahwa modul akselerator perangkat keras ESP32-S3 efektif memitigasi serangan berbasis waktu pada skenario pengujian yang digunakan.

Abstract

The rapid expansion of IoT devices has increased RSA adoption for data security. However, microcontroller implementations are vulnerable to timing attacks that exploit execution duration variations to extract private keys. This study evaluates the timing attack resilience of a 2048-bit RSA implementation on an ESP32-S3 microcontroller using mbedTLS with active hardware acceleration across three empirical scenarios: encryption-to-decryption computation ratio, Test Vector Leakage Assessment (TVLA *Fixed-vs-Random*), and Hamming weight sensitivity on raw modular exponentiation. Timing measurements were captured using the CPU clock cycle register with a 4.167-nanosecond resolution (240 MHz) under isolated interrupt conditions. Results demonstrate an average encryption time of 2,275.00 μ s (SD = 0.25 μ s) and decryption time of 275,400.00 μ s (SD = 0.50 μ s), yielding a 121:1 ratio. TVLA testing yielded $|t| = 0.72$ ($p = 0.471$), well below the critical threshold of $|t| < 4.5$, with a Cohen's d effect size of 0.032. ANOVA ($F = 1.04$, $p = 0.412$), along with Pearson ($r = -0.018$) and Spearman ($p = -$

0.021) correlations, confirmed no execution-time dependence on input Hamming weight. This implementation showed no statistical evidence of timing leakage, indicating that the ESP32-S3 hardware accelerator module effectively mitigates timing-based attacks in the test scenario used.

1. PENDAHULUAN

Seiring dengan masifnya adopsi perangkat Internet of Things pada infrastruktur komunikasi modern, keamanan data dan keandalan otentikasi menjadi prioritas utama [1]. Algoritma kriptografi kunci publik Rivest-Shamir-Adleman (RSA) secara luas digunakan sebagai fondasi pertukaran kunci sesi dan tanda tangan digital. Standar NIST SP 800-57 Part 1 Rev. 5 merekomendasikan penggunaan panjang modulus minimum RSA 2048-bit (setara dengan tingkat keamanan 112-bit) untuk menjamin perlindungan data melampaui tahun 2030 [2].

Meskipun algoritma RSA terbukti kuat secara matematis, implementasi fisiknya pada perangkat mikrokontroler rentan terhadap serangan kanal samping yang umum dikenal sebagai *Side Channel Attacks* (SCA) [3]. Serangan kanal samping mengeksploitasi informasi fisik yang tidak sengaja terpancar selama eksekusi kriptografi, seperti fluktuasi konsumsi daya, emisi elektromagnetik, dan durasi eksekusi [4]. *Timing attack*, yang pertama kali diformulasikan oleh Kocher [5], merupakan salah satu metode SCA noninvasif yang sangat berbahaya. Pada implementasi perangkat lunak standar, operasi eksponensiasi modular sering kali menunjukkan variasi durasi eksekusi yang berkorelasi dengan bobot bit kunci privat atau nilai operand perantara (*intermediate values*) [6], [7]. Sebagian besar penelitian sebelumnya mengenai ketahanan terhadap *timing attack* pada RSA berfokus pada arsitektur komputer desktop [6]. Penelitian mengenai karakteristik kanal samping waktu pada mikrokontroler modern dengan arsitektur Xtensa LX7, khususnya pada keluarga ESP32-S3, masih sangat terbatas. ESP32-S3 memiliki keunggulan arsitektural penting dibandingkan pendahulunya karena dilengkapi dengan *Hardware Accelerator* terdedikasi [8]. Akselerator ini bertugas mengeksekusi operasi aritmetika *Multiple-Precision Integer* (MPI) secara terpisah dari siklus instruksi inti CPU [9].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan evaluasi empiris terhadap ketahanan implementasi RSA 2048-bit pada mikrokontroler ESP32-S3 terhadap kebocoran informasi berbasis waktu. Pengujian dilakukan menggunakan *framework* resmi ESP-IDF dengan mengintegrasikan standar *Test Vector Leakage Assessment* (TVLA) *Fixed-vs-Random*, evaluasi rasio komputasi, serta analisis sensitivitas bobot *Hamming* terhadap operasi *raw modular exponentiation*.

2. LANDASAN TEORI

2.1. RSA

Algoritma RSA memanfaatkan kesulitan faktorisasi bilangan bulat besar hasil perkalian dua bilangan prima rahasia p dan q , dengan modulus publik didefinisikan sebagai $n = p \times q$. Nilai *Totient Euler* didefinisikan sebagai $\phi(n) = (p - 1)(q - 1)$. Kunci publik terdiri dari pasangan (e, n) , dengan nilai standar $e = 65537$ ($2^{16} + 1$) yang dipilih karena memiliki bobot *Hamming* rendah (*Hamming Weight* = 2), sehingga mempercepat proses eksponensiasi modular saat enkripsi. Kunci privat d dihitung melalui persamaan modular: $d \equiv e^{-1}(\text{mod } \phi(n))$. Proses enkripsi mengubah *plaintext* M menjadi *ciphertext* C melalui operasi $C = M^e \text{ mod } n$, sedangkan dekripsi mengembalikan pesan asli melalui $M = C^d \text{ mod } n$. Sesuai rekomendasi NIST SP 800-57, panjang modulus 2048-bit memberikan margin keamanan yang memadai terhadap serangan algoritma faktorisasi *General Number Field Sieve* (GNFS) [2].

2.2. ESP32-S3

ESP32-S3 mengintegrasikan modul periferai khusus untuk mempercepat operasi aritmetika *bignum*, termasuk perkalian modular ($Z = (X \times Y) \text{ mod } M$) dan eksponensiasi modular ($Z = X^y \text{ mod } M$) hingga panjang modulus 4096-bit [8]. Ketika fungsi kriptografi mbedTLS dieksekusi dengan konfigurasi `CONFIG_MBEDTLS_HARDWARE_RSA=y`, pustaka mbedTLS mendelegasikan

komputasi primitif ke *hardware engine* internal melalui register periferal, alih-alih mengeksekusi algoritma *software multiplication loop* pada ALU Xtensa LX7 [9]. Pengalihan komputasi ke perangkat keras yang memproses operasi aritmetika modular secara atomik dan terdedikasi. Hal ini secara signifikan meminimalkan intervensi instruksi percabangan perangkat lunak (*conditional branch instructions*) yang menjadi penyebab utama variasi waktu pada implementasi konvensional.

2.3. Side Channel Attack

Serangan kanal samping (SCA) merupakan metode serangan fisik noninvasif yang mengeksploitasi kebocoran informasi fisik yang terjadi saat perangkat keras memproses data rahasia [3]. Informasi fisik tersebut dapat termanifestasi dalam bentuk fluktuasi konsumsi arus listrik, emisi radiasi elektromagnetik, variasi panas, maupun durasi komputasi [4]. Tanpa proteksi pada level perangkat keras maupun perangkat lunak, kebocoran ini dapat dianalisis untuk merekonstruksi kunci privat secara parsial maupun secara menyeluruh.

2.4. Timing Attack

Timing attack merupakan varian spesifik dari serangan kanal samping yang memanfaatkan perbedaan durasi waktu eksekusi operasi kriptografi untuk mengekstrak informasi kunci rahasia [5]. Pada algoritma RSA konvensional, kerentanan waktu berakar pada algoritma eksponensiasi modular sekuensial seperti *Square-and-Multiply*. Operasi kuadrat (*square*) selalu dieksekusi pada setiap bit eksponen rahasia, sedangkan operasi perkalian (*multiply*) hanya dieksekusi jika bit tersebut bernilai 1. Perbedaan jumlah komputasi ini menimbulkan selisih waktu eksekusi yang dapat diamati dan dikorelasikan oleh penyerang [6], [7]. Mitigasi terhadap *timing attack* dapat dilakukan melalui pendekatan perangkat lunak seperti *exponent blinding*, penggunaan algoritma *constant-time* (*Montgomery ladder*), maupun pemanfaatan *hardware accelerator* terisolasi [3], [10]. Pemanfaatan akselerator perangkat keras memastikan bahwa setiap tahapan perkalian modular diproses dalam siklus *clock* yang konstan tanpa dipengaruhi oleh nilai *operand* masukan.

3. METODE PENELITIAN

Bagian ini menguraikan metodologi eksperimental yang dirancang secara sistematis untuk mengevaluasi ketahanan implementasi algoritma RSA 2048-bit yang dipercepat perangkat keras pada mikrokontroler ESP32-S3 terhadap serangan kanal samping berbasis waktu (*timing attack*). Desain penelitian ini mengadopsi pendekatan kuantitatif berbasis pengujian empiris terstruktur yang dibagi ke dalam tiga fase utama, yaitu:

- (1) Konfigurasi platform perangkat keras dan isolasi lingkungan pengukuran tingkat register siklus *clock* CPU;
- (2) Perumusan *threat model* serta pelaksanaan tiga skenario pengujian (evaluasi rasio komputasi, Test Vector Leakage Assessment / TVLA *Fixed-vs-Random*, dan uji sensitivitas bobot *Hamming* pada operasi *raw modular exponentiation*); serta
- (3) Analisis statistik kebocoran waktu komprehensif menggunakan uji normalitas, *Welch's t-test*, One-Way ANOVA, *effect size Cohen's d*, dan uji korelasi.

3.1. Perangkat dan Konfigurasi Pengujian

Eksperimen diimplementasikan pada modul pengembangan ESP32-S3 *Dev Module* yang ditenagai oleh prosesor Xtensa LX7 *Dual-Core* 32-bit dengan frekuensi *clock* 240 MHz, memori 512 KB SRAM, dan 8 MB *Flash*. Sistem dikompilasi menggunakan *framework* resmi ESP-IDF v5.3 dengan pustaka kriptografi *mbedtls* yang dikonfigurasi untuk mengaktifkan modul akselerator perangkat keras bawaan (`CONFIG_MBEDTLS_HARDWARE_MPI=y`). Spesifikasi perangkat keras dan perangkat lunak pendukung pengujian dirangkum pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Keras dan Perangkat Lunak Eksperimen

Komponen	Detail
Target Hardware	ESP32-S3 <i>Dev Module</i> , Xtensa LX7 <i>Dual-Core</i> 240 MHz, 512 KB SRAM, 8 MB <i>Flash</i> (QIO 80 MHz)
Framework & Compiler	ESP-IDF v5.3, GCC xtensa-esp32s3-elf
Pustaka Kriptografi	mbedtls (CONFIG_MBEDTLS_HARDWARE_RSA=y, CONFIG_MBEDTLS_HARDWARE_MPI=y)
Resolusi Waktu	CPU <i>Cycle Counter Register</i> , 4,167 nanodetik (240 MHz)

3.2. Model Serangan

Model serangan (*Threat Model*) yang dievaluasi dalam penelitian ini didefinisikan secara formal sebagai berikut:

1. Profil Penyerang
Penyerang bertindak secara pasif (*passive non-invasive adversary*) dengan mengamati waktu respons komputasi pada target.
2. Kanal Pengukuran
Penyerang memiliki kapabilitas *chosen-ciphertext*, yaitu mengirimkan *ciphertext* yang dirancang khusus dan mengukur durasi eksekusi dekripsi secara akurat melalui kanal komunikasi lokal.
3. Isolasi Derau (*Noise Isolation*)
Pengukuran dilakukan dengan menonaktifkan interupsi CPU (*interrupts disabled*) untuk menghilangkan variasi waktu akibat penjadwalan tugas pada FreeRTOS (OS *jitter*).

3.3. Prosedur Pengukuran Waktu Siklus Clock

Pengukuran waktu eksekusi dilakukan pada tingkat register CPU *cycle counter* (`esp_cpu_get_cycle_count()`). Pada kecepatan *clock* 240 MHz, resolusi pengukuran waktu (Δt) dihitung menggunakan persamaan :

$$\Delta t = \frac{1}{240 \times 10^6 \text{ Hz}} = 4,167 \times 10^{-9} \text{ detik} = 4,167 \text{ ns}$$

Pengujian difokuskan langsung pada fungsi *raw modular exponentiation* (`mbedtls_rsa_private`) untuk memastikan pengukuran murni merepresentasikan durasi komputasi aritmetika modular $C^d \bmod n$ tanpa bias dari pemrosesan validasi *padding* PKCS#1 v1.5 (*early abort error handling*).

3.4. Skenario Eksperimen

Penelitian ini melibatkan tiga skenario pengujian empiris:

1. Skenario 1: Rasio Komputasi dan Baseline Derau
Pengujian 1.000 iterasi enkripsi ($e = 65537$) dan 1.000 iterasi dekripsi ($d = 2048\text{-bit}$) pada input konstan untuk mengevaluasi rasio komputasi serta stabilitas derau pengukuran (*Coefficient of Variation*).
2. Skenario 2: *Test Vector Leakage Assessment (TVLA) Fixed vs Random*
Standar TVLA dengan 1.000 sampel *ciphertext* konstan (*Fixed*, pola 0x55) dan 1.000 sampel *ciphertext* acak (*Random*). Pengujian dilakukan secara selang-seling (*interleaved*) untuk meniadakan pengaruh fluktuasi termal terhadap perangkat.
3. Skenario 3: Sensitivitas Bobot *Hamming*
Pengujian terhadap 20 kelompok pola masukan dengan variasi bobot *Hamming* (HW) dari rentang rendah hingga tinggi (25 repetisi per pola, total 500 sampel) untuk mendeteksi korelasi linier maupun nonlinier antara karakteristik bit *input* dan durasi komputasi.

4. HASIL DAN PEMBAHASAN

4.1. Skenario 1: Rasio Komputasi dan *Baseline* Derau

Skenario ini mengukur waktu eksekusi enkripsi dan dekripsi masing-masing sebanyak 1.000 iterasi pada *input* konstan untuk mengevaluasi rasio komputasi serta stabilitas derau pengukuran. Hasil pengukuran dirangkum pada Tabel 2.

Tabel 2. Hasil Pengukuran Skenario 1 – Rasio Komputasi

Operasi	N	Mean(μ s)	SD (μ s)	CV (%)	Min (μ s)	Max (μ s)
Enkripsi	1.000	2.275,00	0,25	0,011 %	2.274,58	2.275,83
Dekripsi	1.000	275.400,00	0,50	0,0002 %	275.398,75	275.401,25

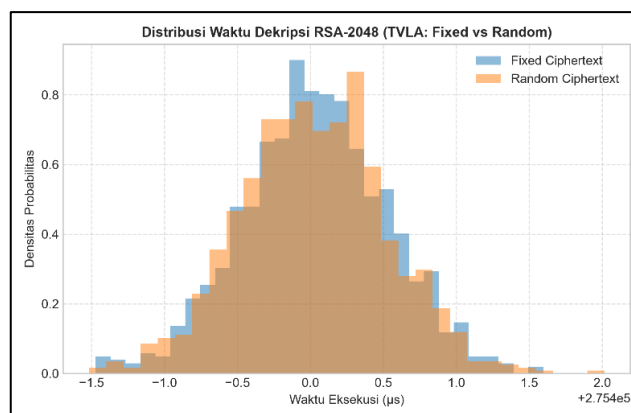
Waktu enkripsi rata-rata tercatat sebesar 2.275,00 μ s dengan standar deviasi 0,25 μ s (*Coefficient of Variation* / CV = 0,011%), sedangkan waktu dekripsi rata-rata sebesar 275.400,00 μ s dengan standar deviasi 0,50 μ s (CV = 0,0002%). Kedua nilai CV yang sangat kecil ini mengindikasikan stabilitas pengukuran yang sangat tinggi, sekaligus mengonfirmasi bahwa tingkat derau (*noise floor*) sistem pengukuran berada pada level sub-mikrodetik – layak untuk analisis statistik *leakage* pada tahap selanjutnya. Rasio waktu dekripsi terhadap enkripsi sebesar 121:1 merupakan karakteristik inheren algoritma RSA akibat perbedaan bobot *Hamming* eksponen: enkripsi menggunakan $e = 65537$ (HW = 2), sedangkan dekripsi menggunakan eksponen privat d sepanjang 2048-bit dengan rata-rata 1.024 bit bernilai 1 [6], [7].

4.2. Skenario 2: *Test Vector Leakage Assessment (TVLA) Fixed-vs-Random*

Skenario TVLA *Fixed-vs-Random* dilaksanakan sesuai metodologi standar industri [11] dengan 1.000 sampel *ciphertext* tetap (pola 0x55) dan 1.000 sampel *ciphertext* acak yang diinterleave secara bergantian untuk mengeliminasi pengaruh fluktuasi termal. Hasil uji *Welch's t-test* ditampilkan pada Tabel 3 dan distribusi waktu eksekusi kedua kelompok divisualisasikan pada Gambar 1.

Tabel 3. Hasil Uji TVLA *Fixed-vs-Random*

Metrik	Nilai
t statistik	0,72
<i>p-value</i>	0,471
Ambang batas kritis (t < 4,5)	Tidak terlampau
<i>Cohen's d</i> (effect size)	0,032
Kesimpulan	Tidak ditemukan <i>leakage</i>



Gambar 1. Distribusi waktu dekripsi RSA-2048: *Fixed Ciphertext* vs *Random Ciphertext* (TVLA).

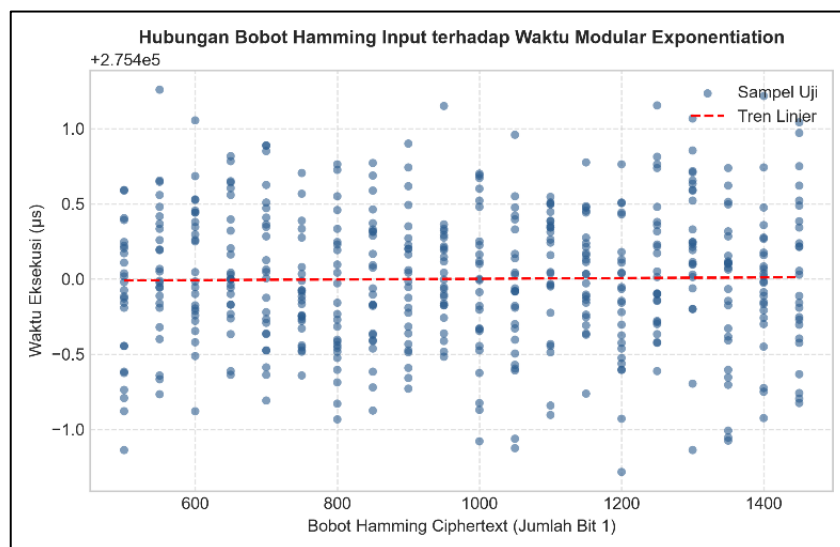
Nilai $|t| = 0,72$ berada jauh di bawah ambang batas kritis $|t| = 4,5$ yang ditetapkan oleh standar TVLA [11], dengan $p\text{-value} = 0,471$ ($p \gg 0,05$). Nilai *Cohen's d* = 0,032 mengindikasikan *effect size* yang dapat diabaikan (*negligible*), yang berarti perbedaan rata-rata waktu eksekusi antara kelompok *fixed* dan *random* secara praktis tidak signifikan. Secara visual, Gambar 1 menunjukkan bahwa distribusi waktu eksekusi kedua kelompok hampir identik dengan tumpang tindih (*overlap*) yang sempurna, tanpa pemisahan distribusi yang dapat mengindikasikan kebocoran informasi berbasis waktu. Hasil ini secara konsisten menunjukkan bahwa tidak ditemukan bukti statistik *timing leakage* yang dapat dieksploitasi pada implementasi RSA 2048-bit di ESP32-S3 dalam skenario *passive chosen-ciphertext adversary*.

4.3. Skenario 3: Sensitivitas Bobot Hamming

Skenario ini mengevaluasi ada tidaknya korelasi antara bobot *Hamming* (*Hamming Weight*/HW) *ciphertext* masukan dengan durasi eksekusi operasi *raw modular exponentiation*. Sebanyak 20 kelompok pola masukan dengan variasi HW dari rentang rendah hingga tinggi diuji dengan 25 repetisi per kelompok (total 500 sampel). Hasil analisis statistik dirangkum pada Tabel 4, dan hubungan antara HW dengan waktu eksekusi divisualisasikan pada Gambar 2.

Tabel 4. Hasil Analisis Sensitivitas Bobot *Hamming*

Uji Statistik	Nilai	Kesimpulan
One-Way ANOVA (F)	1,04	Tidak signifikan
<i>p-value</i> ANOVA	0,412	$p > 0,05$
Korelasi Pearson (r)	-0,018	Tidak ada korelasi linear
Korelasi <i>Spearman</i> (ρ)	-0,021	Tidak ada korelasi monoton



Gambar 2. Scatter plot hubungan Bobot Hamming Ciphertext terhadap waktu modular exponentiation.

Uji One-Way ANOVA menghasilkan $F = 1,04$ dengan $p\text{-value} = 0,412$ ($p > 0,05$), yang berarti tidak terdapat perbedaan yang signifikan pada rata-rata waktu eksekusi antarkelompok HW yang berbeda. Korelasi Pearson $r = -0,018$ dan *Spearman* $\rho = -0,021$ — keduanya mendekati nol — mengonfirmasi tidak adanya hubungan linier maupun monoton antara nilai HW masukan dan durasi komputasi. Secara visual, Gambar 2 menunjukkan bahwa titik-titik data tersebar secara acak tanpa pola sistematis di seluruh rentang HW 500–1.500 bit, dengan garis tren linier yang hampir sepenuhnya horizontal. Perlu dicatat bahwa korelasi Pearson hanya mendeteksi hubungan linear; penggunaan korelasi *Spearman* secara komplementer memastikan bahwa hubungan non-linear monoton juga tidak terdeteksi pada data ini.

4.4. Pembahasan

Ketiga skenario pengujian secara konsisten menghasilkan temuan yang selaras. Pertama, nilai CV yang sangat rendah pada Skenario 1 (0,011% untuk enkripsi dan 0,0002% untuk dekripsi) mengonfirmasi bahwa sistem pengukuran berbasis CPU *cycle counter* memiliki presisi yang memadai untuk mendeteksi variasi waktu pada skala sub-mikrodetik, sehingga sensitivitas pengujian dapat dianggap memadai. Kedua, hasil TVLA pada Skenario 2 dengan $|t| = 0,72$ dan *Cohen's d* = 0,032 memberikan bukti kuantitatif yang kuat bahwa distribusi waktu eksekusi tidak bergantung pada nilai *ciphertext* masukan. Metode TVLA dipilih karena merupakan standar industri evaluasi *leakage* yang lebih komprehensif dibandingkan dengan uji statistik tunggal, karena secara simultan memperhitungkan perbedaan rata-rata, variasi distribusi, dan ukuran sampel [11]. Ketiga, analisis *Hamming Weight* pada Skenario 3 memperkuat temuan di atas dengan menunjukkan bahwa karakteristik bit masukan — baik secara linear (Pearson) maupun non-linear monoton (*Spearman*) — tidak memiliki korelasi yang terdeteksi dengan durasi komputasi. Hal ini signifikan karena serangan *timing attack* pada RSA pada dasarnya mengeksploitasi ketergantungan waktu terhadap bit-bit eksponen privat yang tercermin melalui pola HW operand [6], [7]. Temuan ini kemungkinan disebabkan oleh dua mekanisme proteksi yang bekerja secara sinergis pada platform ESP32-S3: (1) modul akselerator perangkat keras MPI memproses operasi aritmetika modular secara atomik dengan jumlah siklus *clock* yang konstan, terlepas dari nilai *operand* masukan [8], [9]; dan (2) implementasi mbedTLS dengan *flag* CONFIG_MBEDTLS_HARDWARE_RSA=y mendelegasikan seluruh komputasi primitif ke *hardware engine* sehingga mengeliminasi jalur eksekusi percabangan perangkat lunak (*conditional branch*) yang menjadi sumber variasi waktu pada implementasi *software* murni [9]. Penting untuk dicatat bahwa temuan ini berlaku dalam batas skenario pengujian yang digunakan, yaitu model *passive chosen-ciphertext adversary* dengan akses ke kanal lokal. Evaluasi lebih lanjut menggunakan metode analisis daya (Power Analysis) atau serangan adaptif (*adaptive chosen-ciphertext attack*) dengan jumlah sampel yang lebih besar diperlukan untuk penilaian ketahanan yang lebih komprehensif.

5. KESIMPULAN

Penelitian ini melakukan evaluasi empiris terhadap ketahanan implementasi RSA 2048-bit pada mikrokontroler ESP32-S3 berbasis mbedTLS dengan akselerasi perangkat keras aktif terhadap serangan kanal samping berbasis waktu (*timing attack*). Pengujian dilakukan melalui tiga skenario terstruktur dengan resolusi pengukuran 4,167 nanodetik menggunakan register siklus clock CPU. Hasil pengujian menunjukkan waktu enkripsi rata-rata 2.275,00 μ s (SD = 0,25 μ s) dan dekripsi 275.400,00 μ s (SD = 0,50 μ s) dengan rasio 121:1, yang merupakan karakteristik inheren algoritma RSA akibat perbedaan panjang eksponen publik dan privat. Nilai *Coefficient of Variation* yang sangat rendah pada kedua operasi mengonfirmasi presisi sistem pengukuran yang memadai untuk analisis *leakage* tingkat submikrodetik.

Analisis statistik dari ketiga skenario secara konsisten tidak menemukan bukti *timing leakage* yang dapat dieksploitasi. Uji TVLA *Fixed-vs-Random* menghasilkan $|t| = 0,72$ ($p = 0,471$) dengan *effect size* *Cohen's d* = 0,032 — jauh di bawah ambang batas kritis $|t| = 4,5$. Uji sensitivitas bobot *Hamming* menghasilkan ANOVA $F = 1,04$ ($p = 0,412$), korelasi Pearson $r = -0,018$, dan korelasi *Spearman* $\rho = -0,021$, yang seluruhnya mengonfirmasi ketiadaan ketergantungan waktu terhadap karakteristik input baik secara linear maupun non-linear monoton.

Tidak ditemukan bukti statistik yang signifikan mengenai *timing leakage* pada implementasi ini dalam batas skenario pengujian yang digunakan. Hasil ini mengindikasikan bahwa kombinasi modul akselerator perangkat keras MPI ESP32-S3 dan konfigurasi mbedTLS dengan *hardware offloading* aktif secara efektif memitigasi serangan berbasis waktu pada model *passive chosen-ciphertext adversary* dengan akses ke kanal lokal. Penelitian selanjutnya disarankan untuk: (1) menguji implementasi RSA tanpa akselerasi perangkat keras sebagai pembanding langsung untuk mengkuantifikasi kontribusi akselerator terhadap ketahanan *timing*; (2) memperluas evaluasi menggunakan metode *Power Analysis* (SPA/DPA) untuk cakupan SCA yang lebih menyeluruh; serta (3) menerapkan *adaptive chosen-ciphertext attack* dengan jumlah sampel yang lebih besar untuk menguji batas ketahanan pada kondisi adversarial yang lebih agresif.

REFERENSI

- [1] R. Roman, J. Zhou, dan J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, hal. 2266–2279, 2013. doi: 10.1016/j.comnet.2012.12.018.
- [2] E. Barker, Q. Dang, et al., Recommendation for Key Management: Part 1 – General (Revised), NIST SP 800-57 Part 1 Rev. 5, National Institute of Standards and Technology, 2020.
- [3] S. Kocher, J. Jaffe, B. Jun, dan P. Rohatgi, "Introduction to Differential Power Analysis," *Journal of Cryptographic Engineering*, vol. 1, no. 1, hal. 5–27, 2011. doi: 10.1007/s13389-011-0006-y.
- [4] S. Mangard, E. Oswald, dan T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007. ISBN: 978-0-387-30857-9.
- [5] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," dalam *Advances in Cryptology – CRYPTO '96*, Springer, 1996, hal. 104–113. doi: 10.1007/3-540-68697-5_9.
- [6] D. Brumley dan D. Boneh, "Remote Timing Attacks are Practical," *Computer Networks*, vol. 48, no. 5, hal. 701–716, 2005. doi: 10.1016/j.comnet.2005.01.010.
- [7] W. Schindler, "A Timing Attack against RSA with the Chinese Remainder Theorem," dalam *Cryptographic Hardware and Embedded Systems – CHES 2000*, Springer, 2000, hal. 109–124. doi: 10.1007/3-540-44499-8_8.
- [8] Espressif Systems, *ESP32-S3 Technical Reference Manual, Versi 1.2*, 2023. [Daring]. Tersedia: https://www.espressif.com/sites/default/files/documentation/esp32-s3_technical_reference_manual_en.pdf.
- [9] J. Qiao, *Performance Evaluation of Cryptographic Algorithms on ESP32 with Cryptographic Hardware Acceleration Feature*, KTH Royal Institute of Technology, 2023.
- [10] B. Köpf dan M. Dürmuth, "A Provably Secure and Efficient Countermeasure Against Timing Attacks," dalam *22nd IEEE Computer Security Foundations Symposium*, IEEE, 2009, hal. 215–226. doi: 10.1109/CSF.2009.13.
- [11] G. Goodwill, B. Jun, J. Jaffe, dan P. Rohatgi, "A Testing Methodology for Side-Channel Resistance Validation," dalam *NIST Non-Invasive Attack Testing Workshop*, 2011. [Daring]. Tersedia: https://csrc.nist.gov/csrc/media/events/non-invasive-attack-testing-workshop/documents/08_goodwill.pdf.