Analisis Pengaruh Impedansi Input terhadap Kualitas Entropy Noise ADC pada ESP32 sebagai Sumber Seed Kriptografi

Klovinki Purnama (13222119)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13222119@std.stei.itb.ac.id, klovinkipurnama14@gmail.com

Abstrak—Sistem kriptografi modern bergantung pada bilangan acak berkualitas tinggi, khususnya dalam pembentukan seed CSPRNG. Pada perangkat embedded, sumber entropy sering terbatas dan salah satu kandidatnya adalah noise dari analog-to-digital converter (ADC). Kualitas entropy ADC dipengaruhi oleh konfigurasi impedansi input. Penelitian ini mengevaluasi pengaruh variasi impedansi input (1 MΩ dan 2 MΩ) terhadap kualitas entropy noise ADC pada platform ESP32. Data mentah direkam dan diproses secara offline menggunakan ekstraktor Von Neumann. Hasil menunjukkan bahwa konfigurasi 2 MΩ meningkatkan fraksi bit '1' secara signifikan dibanding 1 MΩ dan menghasilkan keluaran Von Neumann yang jauh lebih banyak dengan distribusi bit yang seimbang. Temuan ini menegaskan pentingnya desain hardware dalam memanfaatkan noise ADC sebagai sumber entropy untuk seed kriptografi.

Kata Kunci — Entropy, ADC, Von Neumann, Sumber seed, ESP32, Kriptografi

I. PENDAHULUAN

A. Latar Belakang

Bilangan acak memegang peranan penting dalam sistem kriptografi modern, khususnya dalam pembentukan kunci kriptografi, nonce, dan parameter inisialisasi pada protokol keamanan.Kualitas bilangan acak yang digunakan secara langsung memengaruhi tingkat keamanan sistem sehingga diperlukan sumber entropy yang tidak dapat diprediksi oleh pihak penyerang [1].

Pada sistem embedded dan Internet of Things (IoT), ketersediaan sumber entropy sering kali terbatas. Tidak semua perangkat dilengkapi dengan modul true random number generator (TRNG) khusus sehingga berbagai fenomena fisik dimanfaatkan sebagai kandidat sumber entropy, salah satunya adalah noise pada analog-to-digital converter (ADC) [2]. Noise ADC, khususnya pada bit paling tidak signifikan (least significant bit/LSB), sering dimanfaatkan karena sensitivitasnya terhadap fluktuasi kecil pada sinyal analog.

B. Permasalahan Penelitian

Meskipun noise ADC dapat dimanfaatkan sebagai sumber entropy, kualitas entropy yang dihasilkan sangat dipengaruhi oleh konfigurasi hardware, khususnya impedansi input ADC. Konfigurasi impedansi yang tidak tepat dapat menyebabkan sinyal ADC menjadi terlalu stabil atau sangat bias sehingga entropy yang dihasilkan menjadi rendah atau bahkan runtuh sepenuhnya. Kondisi ini berpotensi menghasilkan seed kriptografi yang dapat diprediksi, yang pada akhirnya melemahkan keamanan sistem kriptografi secara keseluruhan [1], [3].Oleh karena itu, diperlukan evaluasi eksperimental untuk meninjau pengaruh variasi impedansi input terhadap kualitas entropy noise ADC pada perangkat embedded.

C. Tujuan Penelitian

Penelitian ini bertujuan untuk:

- Mengevaluasi karakteristik entropy noise ADC pada ESP32 dengan variasi impedansi input.
- Menganalisis pengaruh impedansi input terhadap kelayakan entropy sebagai seed generator bilangan acak kriptografis.
- Mengevaluasi efektivitas ekstraksi Von Neumann sebagai alat analisis entropy terhadap data mentah ADC.

D. Batasan Penelitian

Penelitian ini dibatasi pada evaluasi kualitas entropy noise ADC dan tidak bertujuan untuk membangun generator bilangan acak kriptografis siap pakai. Proses conditioning menggunakan metode Von Neumann digunakan sebagai alat evaluasi dan tidak dimaksudkan sebagai solusi akhir pembangkitan bilangan acak. Pengujian statistik lanjutan seperti NIST SP 800-22 berada di luar cakupan penelitian ini.

II. LANDASAN TEORI

A. Entropy dan Seed dalam Sistem Kriptografi

Dalam konteks kriptografi, entropy merepresentasikan tingkat ketidakpastian atau ketidakmampuan pihak penyerang untuk memprediksi nilai suatu variabel acak. Entropy merupakan komponen fundamental dalam pembentukan seed bagi cryptographically secure pseudorandom number generator (CSPRNG), yang selanjutnya digunakan untuk menghasilkan bilangan acak deterministik dengan sifat kriptografis yang kuat [1].

CSPRNG bersifat deterministik sehingga seluruh kualitas keamanan outputnya bergantung pada kualitas seed awal yang digunakan. Apabila seed memiliki entropy yang rendah atau dapat diprediksi, maka seluruh keluaran CSPRNG dapat direkonstruksi oleh penyerang [2]. Oleh karena itu, seed CSPRNG harus berasal dari sumber ketidakpastian fisik atau fenomena yang sulit diprediksi, yang umumnya disebut sebagai true random number source (TRNG).

B. Sumber Entropy Fisik pada Sistem Embedded

Pada sistem embedded, ketersediaan sumber entropy sering kali terbatas akibat keterbatasan hardware dan sumber daya. Berbagai fenomena fisik telah dimanfaatkan sebagai kandidat sumber entropy, seperti jitter osilator, noise termal, variasi waktu interrupt, serta noise pada analog-to-digital converter (ADC) [2].

ADC berpotensi menjadi sumber entropy karena sensitivitasnya terhadap fluktuasi kecil pada sinyal analog, terutama ketika masukan ADC berada dalam kondisi tidak stabil atau floating. Noise yang muncul pada proses sampling ADC dapat berasal dari berbagai sumber, termasuk noise termal, coupling elektromagnetik, serta ketidakidealan internal rangkaian ADC itu sendiri.

C. Noise ADC dan Least Significant Bit (LSB)

Bit paling tidak signifikan (least significant bit/LSB) pada hasil konversi ADC sering dimanfaatkan sebagai kandidat sumber entropy karena perubahan kecil pada sinyal analog dapat menyebabkan perubahan nilai pada bit tersebut. Dalam kondisi ideal, LSB ADC diharapkan menunjukkan distribusi yang mendekati acak akibat dominasi noise dibandingkan sinyal deterministik.

D. Von Neumann Extractor

Von Neumann extractor merupakan metode sederhana untuk mengurangi bias pada bitstream acak dengan memproses bit secara berpasangan. Pada metode ini, pasangan bit 01 dan 10 masing-masing dipetakan menjadi bit keluaran, sementara pasangan 00 dan 11 dibuang [4].

Metode Von Neumann efektif dalam menghilangkan bias statistik sederhana, namun memiliki keterbatasan fundamental, yaitu tidak mampu menciptakan entropy baru. Apabila bitstream masukan memiliki variasi yang sangat rendah atau hampir deterministik, maka Von Neumann extractor akan menghasilkan keluaran yang sangat sedikit atau bahkan tidak menghasilkan keluaran sama sekali [3], [4]. Oleh karena itu, Von Neumann extractor lebih tepat digunakan sebagai alat evaluasi kualitas entropy dibandingkan sebagai solusi utama pembangkitan bilangan acak.

III. METODOLOGI PENELITIAN

A. Alur Umum Penelitian

Penelitian ini dilakukan melalui tahapan konfigurasi perangkat keras, akuisisi data mentah dari ADC, pemrosesan data secara offline menggunakan metode Von Neumann, serta analisis hasil ekstraksi entropy. Proses akuisisi data dan evaluasi entropy dipisahkan secara jelas untuk memastikan bahwa hasil yang diperoleh merepresentasikan karakteristik sumber entropy fisik tanpa dipengaruhi oleh mekanisme pemrosesan lanjutan.

B. Konfigurasi Perangkat Keras

- Platform Eksperimen

  Eksperimen dilakukan menggunakan *board* ESP32 yang dilengkapi dengan ADC internal beresolusi hingga 12-bit. ADC dimanfaatkan sebagai sumber data mentah dengan memanfaatkan noise yang muncul pada proses sampling. Pin ADC yang digunakan adalah GPIO32 (ADC1) untuk menghindari konflik dengan subsistem internal lainnya.Resolusi ADC dikonfigurasikan pada 12-bit sehingga nilai hasil konversi berada pada rentang 0 hingga 4095.

- Variasi Impedansi Input

  Untuk mengevaluasi pengaruh impedansi input terhadap kualitas entropy, digunakan dua konfigurasi impedansi,1 MΩ, GPIO32 dihubungkan ke ground melalui satu resistor 1 MΩ dan 2 MΩ, GPIO32 dihubungkan ke ground melalui dua resistor 1 MΩ yang dirangkai secara seri.Setiap eksperimen dilakukan dengan satu konfigurasi impedansi pada satu waktu, dan perubahan konfigurasi dilakukan dalam kondisi perangkat tidak aktif.

C. Firmware Akuisisi Data

Firmware pada ESP32 dirancang khusus untuk melakukan akuisisi data mentah dari ADC. Pada setiap siklus sampling, nilai ADC dibaca dan bit paling tidak signifikan (LSB) dari hasil konversi diekstraksi sebagai bit mentah. Pemilihan LSB didasarkan pada sensitivitasnya terhadap fluktuasi kecil pada sinyal analog, yang umumnya didominasi oleh noise dibandingkan komponen deterministik.

Untuk mengurangi korelasi antar sampel berturut-turut, firmware menerapkan jitter waktu kecil berbasis penundaan mikrodetik dengan variasi acak. Firmware tidak melakukan proses conditioning atau ekstraksi entropy lanjutan sehingga seluruh data yang dikirimkan ke sisi PC merupakan data mentah hasil sampling ADC.

```
#include <Arduino.h>
#include <WiFi.h>
#include "esp_system.h"

static const int ADC_PIN = 32;
// GPIO32 (ADC1_CH4)
static const uint32_t BAUD = 921600;

// Jitter kecil untuk mengurangi
korelasi sampling
static inline void
tiny_jitter_delay() {
  delayMicroseconds(1 + (esp_random()
& 0x0F)); // 1..16 us
}

// Ambil 1 bit mentah dari LSB ADC
static inline uint8_t read_raw_bit()
{
  uint16_t v = analogRead(ADC_PIN);
  return (uint8_t)(v & 0x01);
}

// Bentuk 1 byte dari 8 bit
static uint8_t next_byte() {
  uint8_t out = 0;
  for (int i = 0; i < 8; i++) {
    uint8_t bit = MODE_VON_NEUMANN ?
read_vn_bit() : read_raw_bit();
    out = (uint8_t)((out << 1) | (bit
& 1));
    tiny_jitter_delay();
  }
  return out;
}

void setup() {
  // Matikan WIFI untuk stabilitas
eksperimen
  WiFi.mode(WIFI_OFF);
  btStop();

  Serial.begin(BAUD);
  delay(200);

  analogReadResolution(12);

  // Header singkat (setelah ini
biner terus)
  Serial.printf("\nESP32 ADC RAW |
PIN=%d | BAUD=%u\n", ADC_PIN, BAUD);
  Serial.flush();
  delay(200);
}

void loop() {
  uint8_t b = next_byte();
  Serial.write(&b, 1);
}
```

D. Akuisisi Data di Sisi PC

Data mentah hasil akuisisi dari ESP32 dikirimkan ke komputer melalui antarmuka serial dengan baud rate 921600 bps. Akuisisi data dilakukan hingga mencapai jumlah byte tertentu yang telah ditentukan sebelumnya. Untuk menghindari pengaruh data transien awal, sejumlah data awal yang dikirimkan oleh perangkat dibuang sebelum proses perekaman dimulai.

Data yang telah direkam disimpan dalam format hexadecimal (HEX) untuk memudahkan inspeksi manual dan analisis lebih lanjut tanpa mengubah representasi biner data.

```
import serial, time

PORT = "COM8"
BAUD = 921600
N_BYTES = 250_000

ser = serial.Serial(PORT, BAUD,
timeout=2)

# Buang header & transien awal
ser.read(2048)

t0 = time.time()
got = 0

with open("out.hex", "w") as f:
    while got < N_BYTES:
        chunk = ser.read(min(4096,
N_BYTES - got))
        if not chunk:
            continue

        f.write(chunk.hex() + "\n")
        got += len(chunk)

        if got % 50000 == 0:
            dt = time.time() - t0
            print(f"{got}/{N_BYTES}
bytes, {got/dt:.1f} B/s")

ser.close()
print("DONE")
```

E. Proses Von Neumann Offline

Proses ekstraksi Von Neumann dilakukan secara offline terhadap data mentah yang telah dikumpulkan. Pendekatan ini dipilih untuk memisahkan secara jelas antara proses akuisisi dan evaluasi entropy, serta untuk menghindari kondisi kegagalan ekstraksi akibat entropy mentah yang sangat rendah.

Data mentah dalam format HEX dikonversi menjadi bitstream, kemudian diproses menggunakan aturan Von Neumann, yaitu pasangan bit `01` dan `10` dipetakan menjadi bit keluaran, sedangkan pasangan `00` dan `11` dibuang. Hasil ekstraksi kemudian disimpan kembali dalam format HEX untuk keperluan analisis.

```
import numpy as np

# baca file HEX
def read_hex_file(path):
    with open(path, "r") as f:
        hexstr = "".join(line.strip()
for line in f if line.strip())
    if len(hexstr) % 2 == 1:
        hexstr = hexstr[:-1]
    data = bytes.fromhex(hexstr)
    return np.frombuffer(data,
dtype=np.uint8)

# Von Neumann extractor
def von_neumann(bits01):
    bits01 = bits01[:
(len(bits01)//2)*2]   # pastikan
genap
    a = bits01[0::2]
    b = bits01[1::2]
    valid = (a != b)
# 01 atau 10
    out = a[valid]
# 01->0, 10->1
    return out.astype(np.uint8)

# Konfigurasi
INFILE  = "2M_raw.hex"     # ganti:
1M_raw.hex / 2M_raw.hex
OUTFILE = "2M_vn.hex"

# Proses
raw_bytes = read_hex_file(INFILE)
raw_bits  =
np.unpackbits(raw_bytes).astype(np.ui
nt8)

vn_bits   = von_neumann(raw_bits)
vn_bytes  = np.packbits(vn_bits)

# Simpan HEX
with open(OUTFILE, "w") as f:
    f.write(vn_bytes.tobytes().hex()
+ "\n")

print("RAW bytes :", len(raw_bytes))
print("RAW bits  :", len(raw_bits))
print("RAW p(1)  :", raw_bits.mean())

print("VN bits   :", len(vn_bits))
print("VN bytes  :", len(vn_bytes))
print("VN p(1)   :", vn_bits.mean()
if len(vn_bits) else None)
print("VN eff    :", len(vn_bits) /
len(raw_bits))
```

F. Parameter Evaluasi

Evaluasi kualitas entropy dilakukan dengan mengamati parameter-parameter berikut:

- Fraksi bit ‘1’ pada data mentah dan hasil ekstraksi Von Neumann.
- Jumlah bit dan byte keluaran dari proses Von Neumann.
- Efisiensi Von Neumann, yang didefinisikan sebagai rasio antara jumlah bit keluaran terhadap jumlah bit mentah.

Parameter-parameter ini digunakan untuk menilai pengaruh variasi impedansi input terhadap karakteristik entropy noise ADC.

IV. Hasil Eksperimen

A. Data Mentah yang Diperoleh

Eksperimen dilakukan dengan merekam data mentah ADC ESP32 pada dua konfigurasi impedansi input, yaitu 1 MΩ dan 2 MΩ. Untuk setiap konfigurasi, data direkam sebanyak 250.000 byte, yang setara dengan 2.000.000 bit, dan disimpan dalam format hexadecimal (HEX). Data mentah ini kemudian digunakan sebagai dasar evaluasi kualitas entropy.

B. Karakteristik Data Mentah (RAW)

- Statistik Dasar Data Mentah

Karakteristik awal data mentah dianalisis dengan menghitung fraksi kemunculan bit ‘1’ pada bitstream hasil ekstraksi LSB ADC, dengan rincian pada Tabel 1.

TABLE I. STATISTIK DATA MENTAH

Impedansi Input	*Total Byte*	*Total Bit*	*Fraksi Bit ‘1’*
1 MΩ	250.000	2.000.000	0,0004735
2 MΩ			0,063759

Hasil pada Tabel 1 menunjukkan perbedaan yang sangat signifikan antara kedua konfigurasi impedansi. Pada impedansi 1 MΩ, bitstream didominasi hampir sepenuhnya oleh bit ‘0’, sedangkan pada impedansi 2 MΩ fraksi bit ‘1’ meningkat lebih dari seratus kali lipat.

- Distribusi Nilai Byte Data Mentah

Distribusi nilai byte pada data mentah juga menunjukkan perbedaan yang jelas. Pada konfigurasi 1 MΩ, sebagian besar byte bernilai 0x00, yang konsisten dengan fraksi bit ‘1’ yang sangat kecil. Sebaliknya, pada konfigurasi 2 MΩ, nilai byte yang muncul jauh lebih beragam, mencerminkan peningkatan variasi pada bitstream mentah.

C. Hasil Ekstraksi Von Neumann Offline

- Jumlah Data Keluaran Von Neumann

Data mentah kemudian diproses secara offline menggunakan metode Von Neumann. Jumlah bit dan byte keluaran dari proses ini dicatat sebagai indikator kemampuan ekstraksi entropy, dengan rincian pada Tabel 2

TABLE II. HASIL EKSTRAKSI VON NEUMANN

Impedansi Input	*VN Bit*	*VN Byte*	*Efisiensi VN*
1 MΩ	909	114	0,0004545
2 MΩ	71232	8904	0,035616

Efisiensi Von Neumann didefinisikan sebagai rasio antara jumlah bit keluaran Von Neumann terhadap jumlah bit mentah. Hasil pada Tabel 2 menunjukkan bahwa konfigurasi 2 MΩ menghasilkan keluaran Von Neumann yang jauh lebih besar dibandingkan konfigurasi 1 MΩ.

- Keseimbangan Bit pada Hasil Von Neumann

Selain jumlah keluaran, keseimbangan distribusi bit pada hasil Von Neumann juga dianalisis, dengan rincian pada Tabel 3

TABLE III. FRAKSI BIT '1' HASIL VON NEUMANN

Impedansi Input	*Fraksi Bit '1'*
1 MΩ	0,4774
2 MΩ	0,5046

Hasil ini menunjukkan bahwa meskipun jumlah bit keluaran berbeda secara signifikan, proses Von Neumann mampu menghasilkan bitstream dengan distribusi bit yang mendekati seimbang pada kedua konfigurasi impedansi.

D. Perbandingan Data Mentah dan Hasil Von Neumann

Perbandingan antara data mentah dan hasil ekstraksi Von Neumann menunjukkan bahwa:

- Data mentah pada impedansi 1 MΩ memiliki bias ekstrim dan variasi yang sangat rendah.
- Peningkatan impedansi input menjadi 2 MΩ secara signifikan meningkatkan variasi bit mentah.
- Metode Von Neumann mampu mengurangi bias statistik sederhana, namun dengan konsekuensi penurunan jumlah data keluaran.
- Efektivitas Von Neumann sangat bergantung pada kualitas entropy mentah yang tersedia.

V. ANALISIS DAN PEMBAHASAN

A. Pengaruh Impedansi Input terhadap Kualitas Entropy ADC

Hasil eksperimen pada Bab IV menunjukkan bahwa variasi impedansi input memberikan pengaruh yang sangat signifikan terhadap karakteristik entropy noise ADC. Pada konfigurasi impedansi 1 MΩ, fraksi bit '1' pada data mentah hanya sebesar 0,0004735, yang mengindikasikan bahwa bitstream hampir sepenuhnya didominasi oleh satu nilai. Kondisi ini menunjukkan bahwa node masukan ADC berada pada keadaan yang relatif stabil sehingga variasi noise yang tertangkap sangat terbatas.

Sebaliknya, pada konfigurasi impedansi 2 MΩ, fraksi bit '1' meningkat menjadi 0,063759, atau lebih dari seratus kali lipat dibandingkan konfigurasi 1 MΩ. Peningkatan ini menunjukkan bahwa node masukan ADC menjadi lebih sensitif terhadap fluktuasi kecil dan noise lingkungan ketika impedansi input diperbesar sehingga variasi hasil sampling meningkat secara signifikan.

Hasil ini selaras dengan teori mengenai pengaruh impedansi input terhadap ADC, impedansi yang lebih tinggi cenderung membuat masukan ADC lebih rentan terhadap noise termal dan coupling elektromagnetik yang pada konteks ini berkontribusi terhadap peningkatan entropy.

B. Analisis Kegagalan dan Keberhasilan Ekstraksi Von Neumann

Proses ekstraksi Von Neumann yang diterapkan secara offline memberikan gambaran yang jelas mengenai kelayakan entropy mentah pada masing-masing konfigurasi impedansi. Pada konfigurasi 1 MΩ, dari total 2.000.000 bit mentah, hanya dihasilkan 909 bit keluaran Von Neumann dengan efisiensi sekitar 0,045%. Jumlah keluaran yang sangat kecil ini menunjukkan bahwa pasangan bit valid (01 atau 10) jarang terjadi, yang secara langsung mencerminkan rendahnya variasi pada data mentah.

Sebaliknya, pada konfigurasi 2 MΩ, proses Von Neumann menghasilkan 71.232 bit keluaran dengan efisiensi sekitar 3,56%. Meskipun efisiensi ini masih tergolong rendah secara absolut, peningkatan jumlah keluaran yang signifikan menunjukkan bahwa entropy mentah pada konfigurasi ini jauh lebih layak untuk diekstraksi.

Perbedaan hasil ini menegaskan keterbatasan fundamental metode Von Neumann, yaitu ketidakmampuannya untuk menciptakan entropy baru. Metode ini hanya mampu mengurangi bias statistik sederhana apabila entropy mentah memang tersedia, namun akan gagal atau menghasilkan keluaran yang sangat terbatas apabila sumber entropy bersifat hampir deterministik.

C. Keseimbangan Bit dan Implikasi terhadap Seed Kriptografi

Meskipun jumlah keluaran Von Neumann berbeda secara signifikan antara kedua konfigurasi impedansi, hasil ekstraksi menunjukkan bahwa distribusi bit keluaran relatif seimbang, dengan fraksi bit '1' mendekati 0,5 pada kedua kasus. Hal ini menunjukkan bahwa metode Von Neumann efektif dalam menghilangkan bias sederhana pada bitstream mentah.

Namun, keseimbangan distribusi bit saja tidak cukup untuk menjamin kelayakan suatu bitstream sebagai seed kriptografi. Jumlah entropy efektif yang dapat diekstraksi tetap bergantung pada kualitas sumber entropy fisik. Dalam konteks ini, konfigurasi 1 MΩ menghasilkan entropy efektif yang sangat terbatas sehingga tidak layak digunakan sebagai sumber seed tanpa modifikasi konfigurasi hardware. Sebaliknya, konfigurasi 2 MΩ menunjukkan potensi yang lebih baik sebagai sumber entropy awal untuk pembentukan seed CSPRNG, meskipun masih memerlukan proses conditioning lanjutan untuk penggunaan praktis.

D. Implikasi terhadap Perancangan Sistem Kriptografi Embedded

Hasil penelitian ini memiliki implikasi praktis terhadap perancangan sistem kriptografi pada perangkat embedded. Pertama, hasil ini menunjukkan bahwa pemanfaatan ADC sebagai sumber entropy tidak dapat dilakukan secara sembarangan tanpa mempertimbangkan konfigurasi hardware. Pemilihan impedansi input yang tidak tepat dapat menyebabkan runtuhnya entropy, meskipun mekanisme ekstraksi atau conditioning yang digunakan secara teoritis valid.

Kedua, penelitian ini menegaskan bahwa proses conditioning seperti Von Neumann extractor sebaiknya diposisikan sebagai alat evaluasi atau tahap awal pengolahan, bukan sebagai solusi utama untuk menghasilkan bilangan acak kriptografis. Keandalan sistem kriptografi embedded tetap bergantung pada ketersediaan sumber entropy fisik yang memadai.

E. Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan. Evaluasi entropy dilakukan menggunakan metrik statistik dasar dan tidak mencakup pengujian statistik lanjutan. Selain itu, eksperimen dilakukan pada satu jenis platform dan dalam lingkungan pengujian tertentu sehingga hasil yang diperoleh belum tentu dapat digeneralisasi secara langsung ke seluruh sistem embedded.

Meskipun demikian, pendekatan eksperimental yang digunakan sudah cukup untuk menunjukkan pengaruh signifikan konfigurasi impedansi input terhadap kualitas entropy noise ADC.

VI. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil eksperimen dan analisis yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut.

1. Impedansi input ADC berpengaruh signifikan terhadap kualitas entropy noise ADC pada ESP32. Konfigurasi 2 MΩ menghasilkan variasi bit mentah yang jauh lebih besar dibandingkan konfigurasi 1 MΩ.
2. Pada konfigurasi 1 MΩ, fraksi bit '1' pada data mentah sangat kecil (0,0004735) yang menunjukkan runtuhnya variasi dan rendahnya entropy. Kondisi ini menyebabkan proses ekstraksi Von Neumann menghasilkan keluaran yang sangat terbatas.
3. Pada konfigurasi 2 MΩ, fraksi bit '1' meningkat menjadi 0,063759 (lebih dari seratus kali lipat) sehingga memungkinkan proses ekstraksi Von Neumann menghasilkan keluaran yang jauh lebih signifikan dengan distribusi bit yang mendekati seimbang.
4. Metode Von Neumann efektif dalam mengurangi bias statistik sederhana, namun tidak mampu menciptakan entropy baru. Jumlah keluaran Von Neumann sepenuhnya bergantung pada kualitas entropy mentah yang tersedia.
5. Noise ADC pada ESP32 berpotensi digunakan sebagai sumber entropy untuk pembentukan seed kriptografi, dengan catatan konfigurasi hardware khususnya impedansi input dirancang secara cermat dan disertai proses conditioning lanjutan untuk penggunaan praktis.

B. Saran

Berdasarkan keterbatasan dan temuan penelitian ini, beberapa saran untuk pengembangan selanjutnya adalah sebagai berikut.

1. Melakukan eksplorasi variasi impedansi input yang lebih luas untuk mengidentifikasi rentang konfigurasi yang optimal dalam menghasilkan entropy.
2. Mengombinasikan noise ADC dengan sumber entropy fisik lain pada sistem embedded, seperti jitter osilator atau variasi waktu eksekusi, untuk meningkatkan entropy total.
3. Menerapkan metode conditioning lanjutan, seperti fungsi hash kriptografis untuk mengevaluasi kelayakan hasil ekstraksi sebagai seed CSPRNG dalam aplikasi praktis.
4. Melakukan pengujian statistik lanjutan pada hasil ekstraksi untuk memperoleh evaluasi yang lebih komprehensif terhadap kualitas randomness.

REFERENSI

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
[2] D. Eastlake, J. Schiller, and S. Crocker, Randomness Requirements for Security, RFC 4086, IETF, Jun. 2005.Online: https://www.rfc-editor.org/rfc/rfc4086.Diakses: 17 Desember 2025, 21:33 WIB.
[3] M. Dichtl, "Bad and Good Ways of Post-processing Biased Physical Random Numbers," in Fast Software Encryption, vol. 4593, A. Biryukov, Ed. Springer, 2007, pp. 137–152.
[4] J. von Neumann, “Various techniques used in connection with random digits,” Applied Mathematics Series, vol. 12, pp. 36–38, 1951.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Desember 2025

Klovinki Purnama
13222119