FINAL PROJECT

INTRODUCTION TO HARDWARE SECURITY

111000225 張皓翔

111000212 吳承翰

111000178 連正文

CLICK ME

OUTLINE

- Introduction
- Design
- Implementation
- Result & Analysis
- QA Time

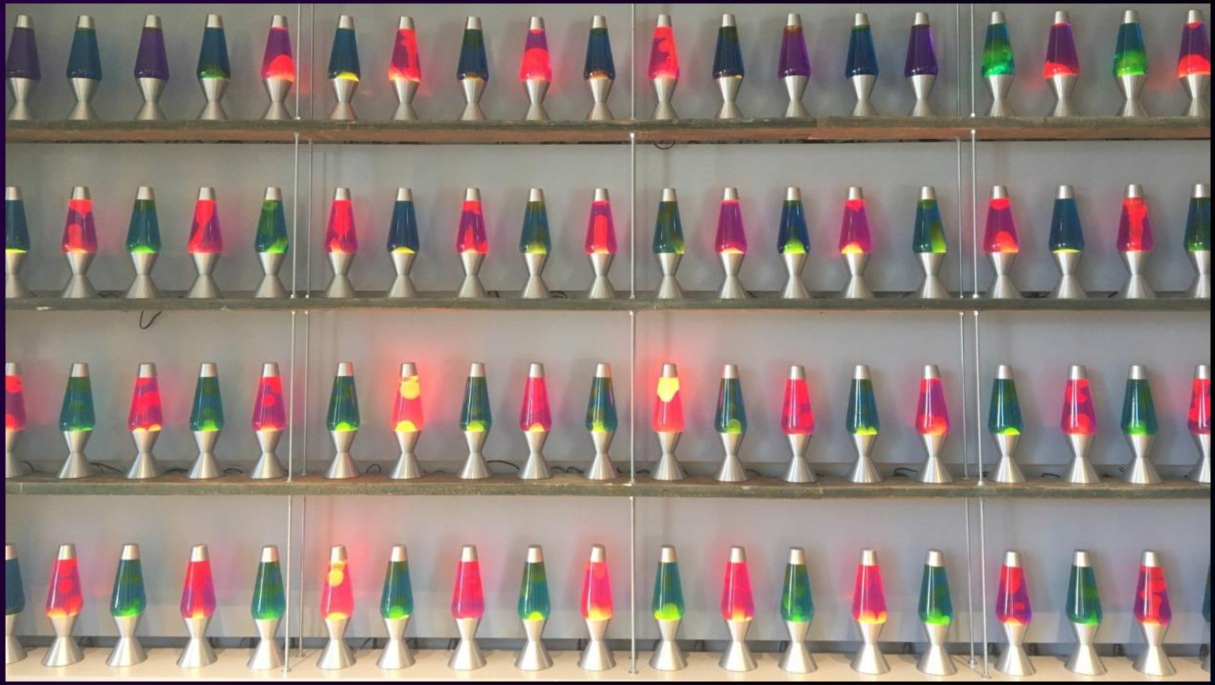
INTRODUCTION
概念簡介

Looking For Random Events

Common Random Events

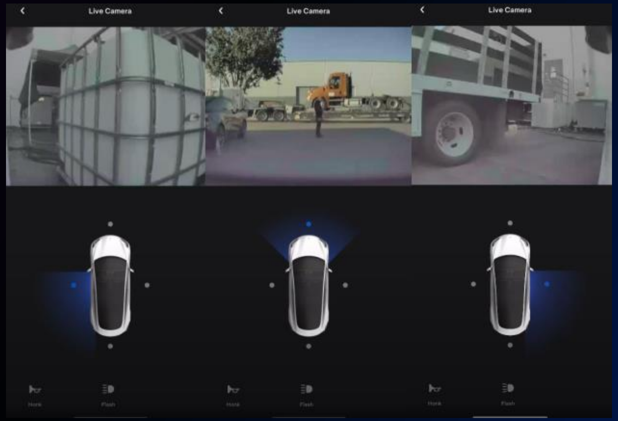
• 熱噪聲	Thermal Noise
• 射頻雜訊	Radio Frequency Noise
• 量子效應	Quantum Effects
• 放射性衰變	Radioactive Decay
• 混沌系統	Chaotic Systems
• 抖動噪聲	Clock Jitter Noise
• 大氣噪聲	Atmospheric Noise
• 外部感測器輸入	External Sensors
• 伽瑪射線或宇宙射線	Gamma Rays or Cosmic Rays

Cloudflare - Lava Lamps

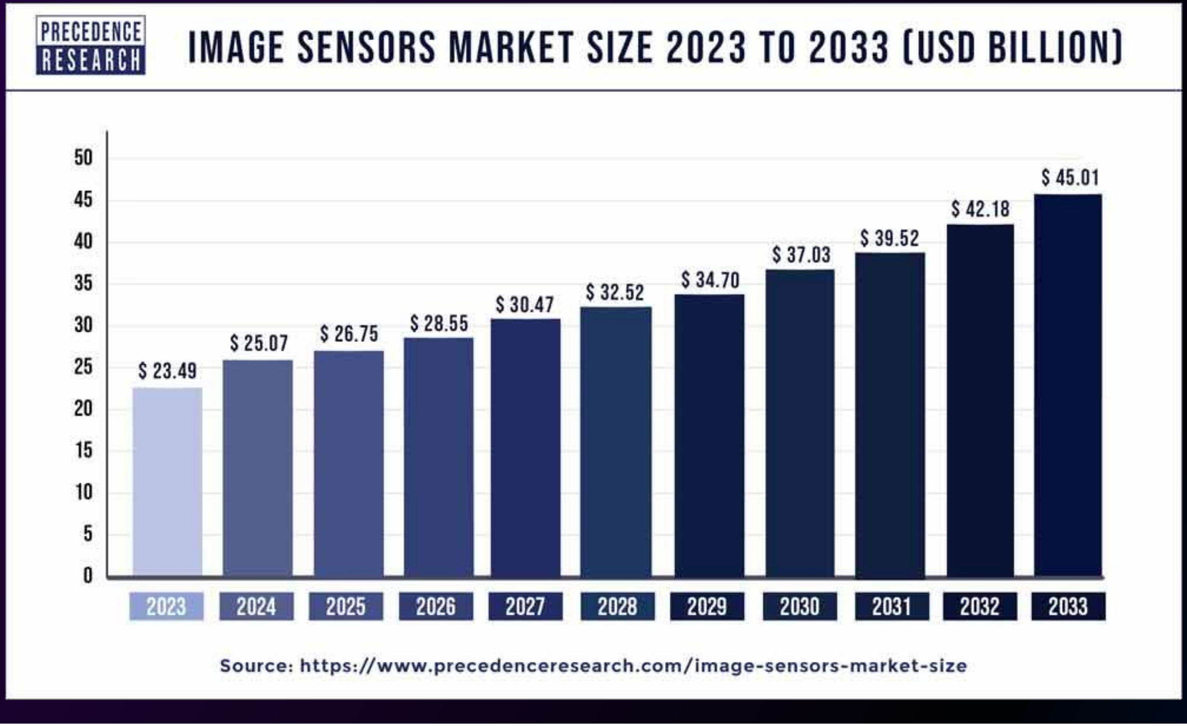


" The 'real world' turns out to be a great source for randomness, because events in the physical world are unpredictable. "

Most Common Sensor



Most Common Sensor



Source: https://www.precedenceresearch.com/image-sensors-market-size

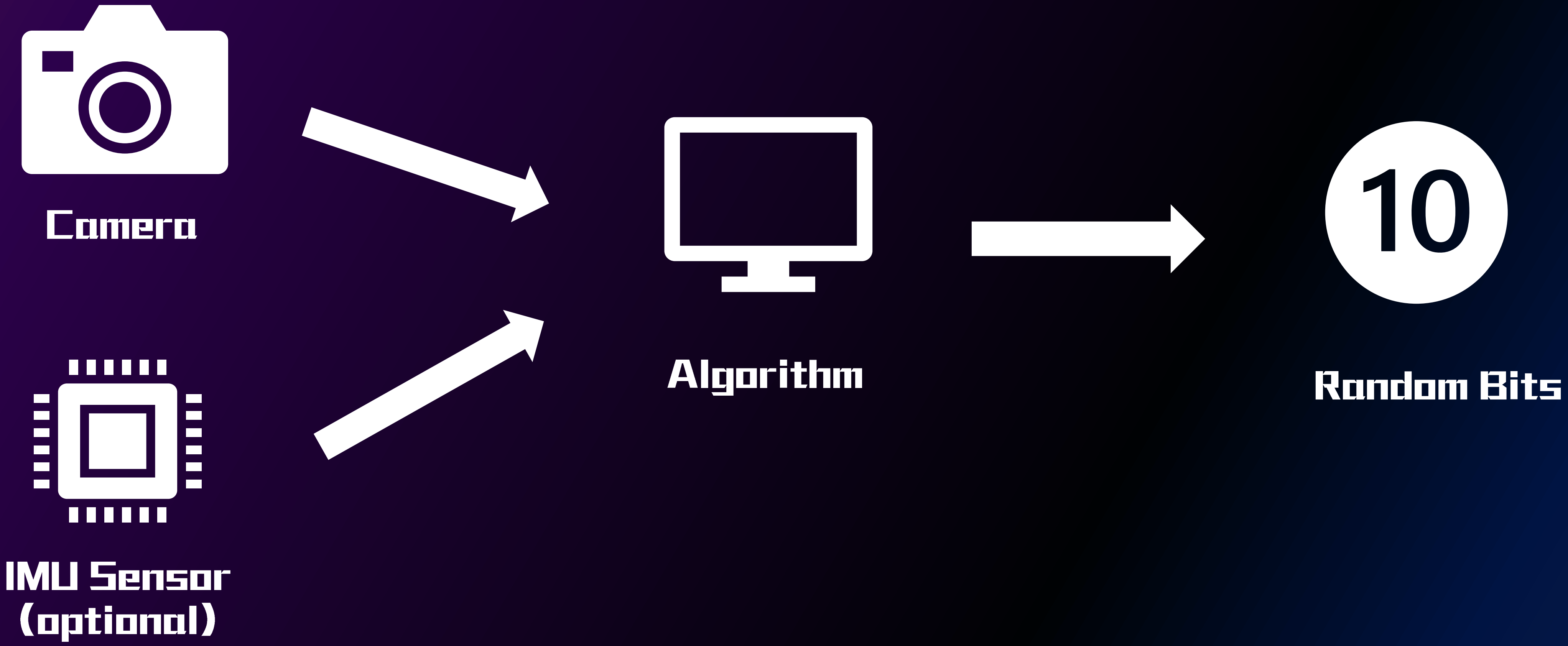
Reliance on image sensors continues to increase.

Noise Sources from Realworld

- Environmental changes
- Human appearance
- Light and shadow noise
- Resolution changes
- Lens distortion
- Encoding format

DESIGN
架構設計

ARCHITECTURE



Camera

IMU Sensor
(optional)

Algorithm

Random Bits

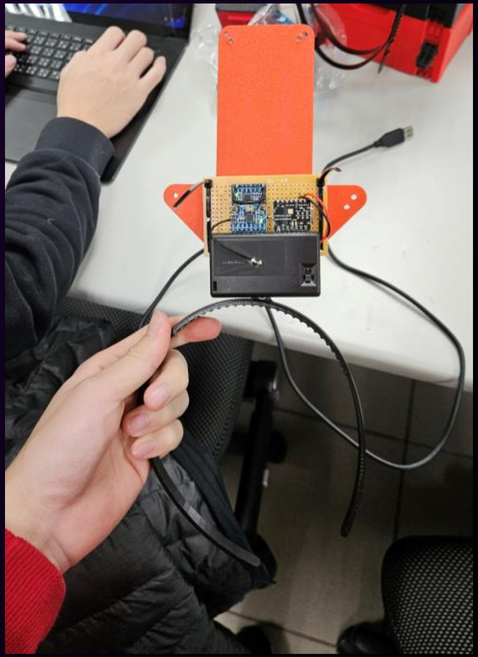
IMPLEMENTATION
亂數實作

Videos record
[Images input]

Image frames

IMU input

Value
Remapping



1010
1010

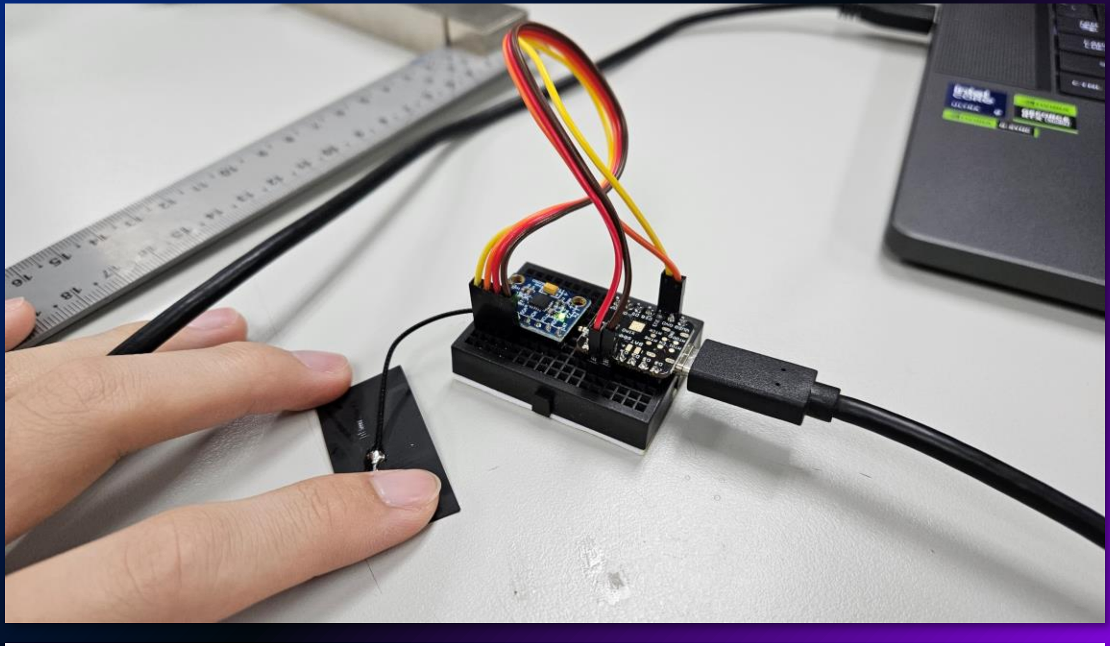
Image
+
IMU bits

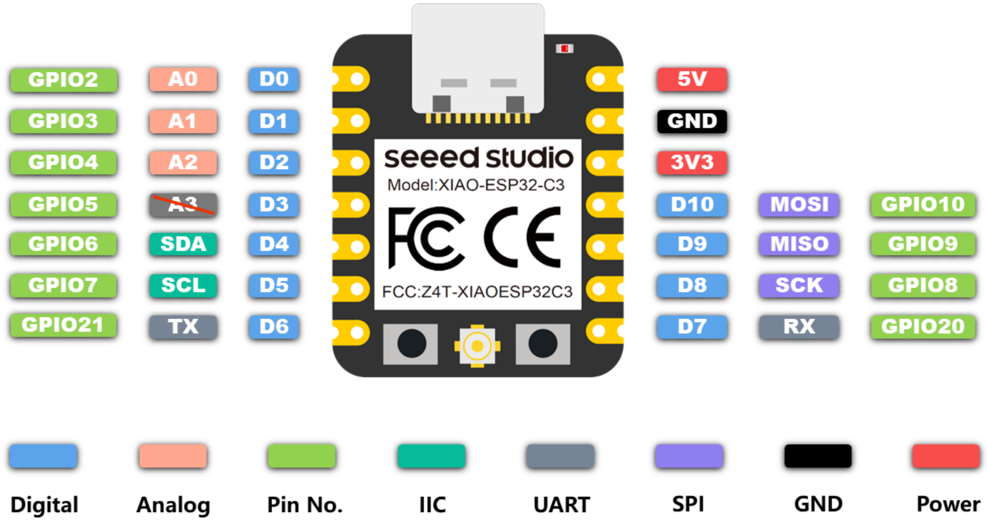
1010
1010

Hashed bits
(SHA256)

SELECT MCU

Choosing MCU that has a **higher clock speed**, includes wireless capabilities like **Wi-Fi** and **Bluetooth**, and is compact in size.

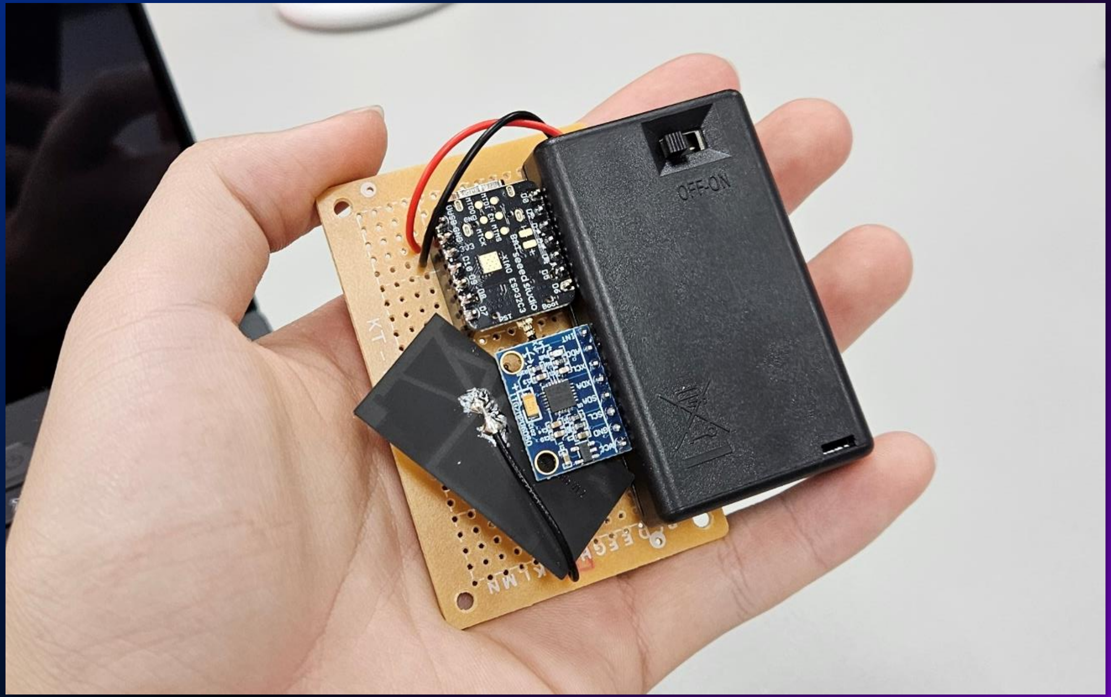


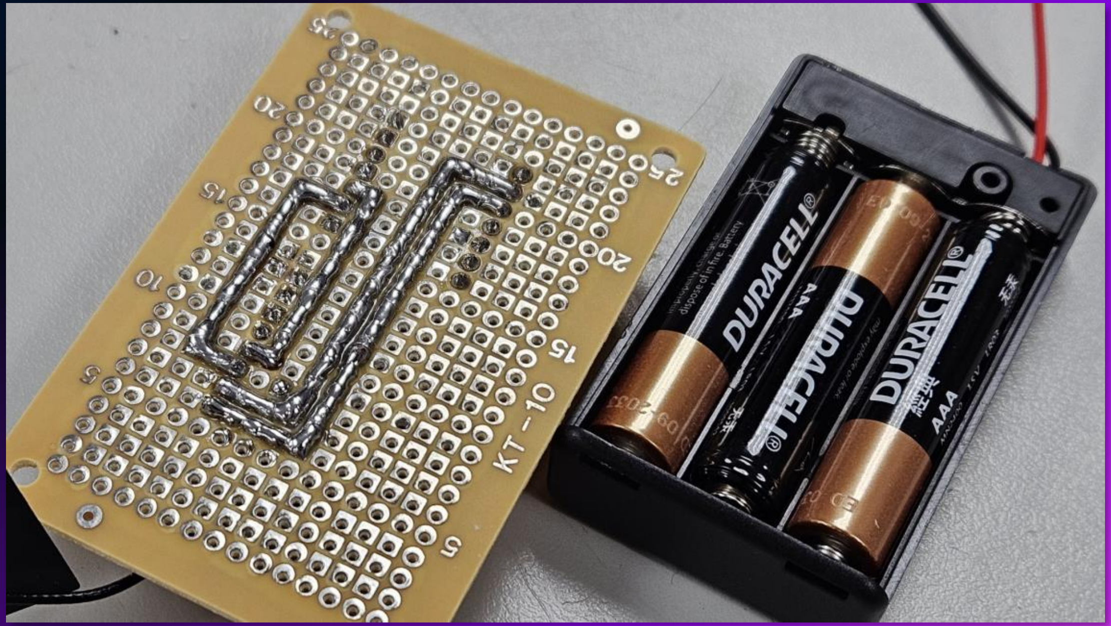


**A3(GPIO5) - Uses ADC2, which may become inoperative due to false sampling signals. For reliable analog reads, use ADC1 instead. Refer to the ESP32-C3 datasheet.*

SIMPLE SOLDERING

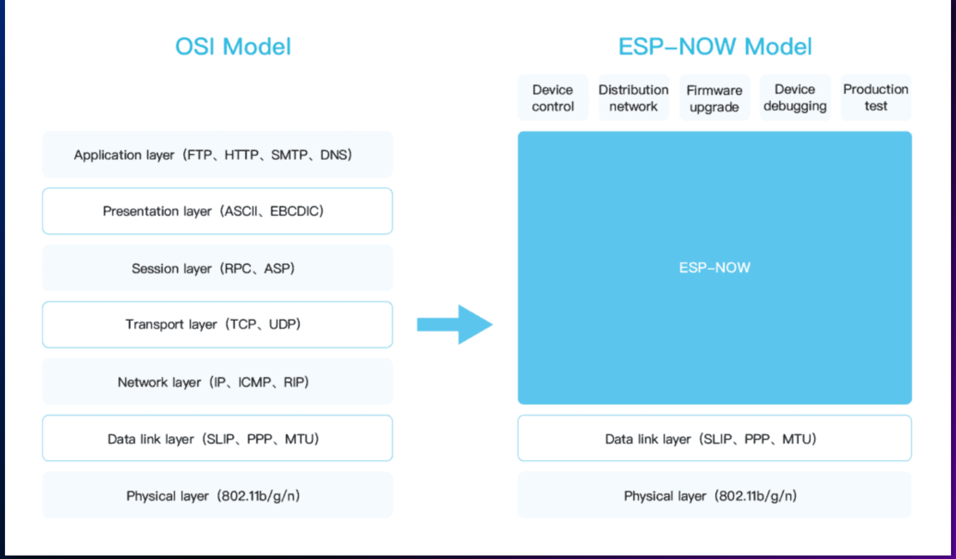
Solder them onto the circuit board, ensuring stable connections, and add a battery so it can be **portable**.





ESP-NOW

- Fast Response
- Low Power Consumption
- Good Compatibility (MESH)
- Long Distance Communication



OSI Model

Application layer（FTP、HTTP、SMTP、DNS）

Presentation layer（ASCII、EBCDIC）

Session layer（RPC、ASP）

Transport layer（TCP、UDP）

Network layer（IP、ICMP、RIP）

Data link layer（SLIP、PPP、MTU）

Physical layer（802.11b/g/n）

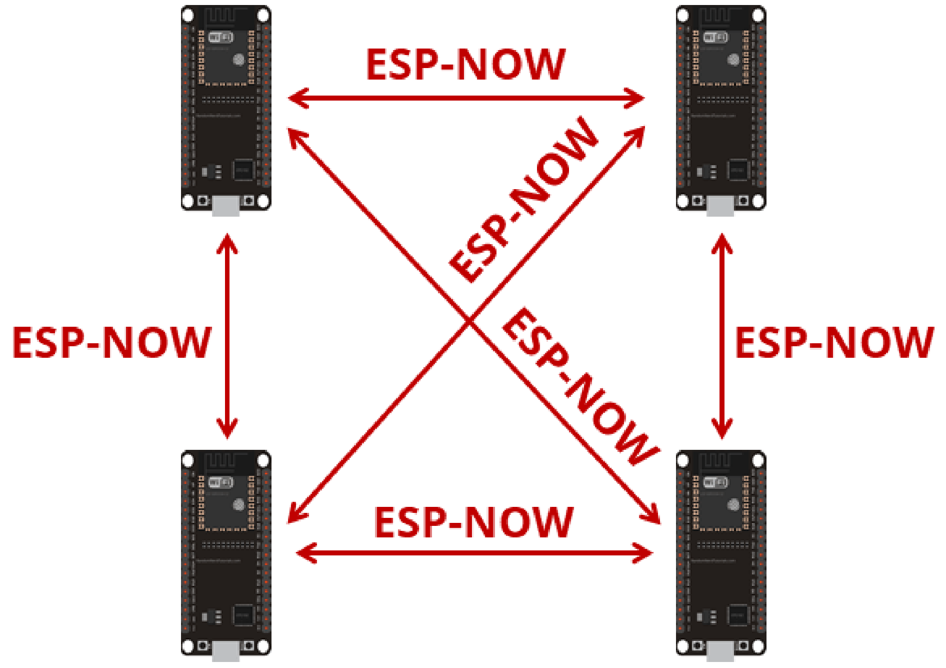
ESP–NOW Model

Device control | Distribution network | Firmware upgrade | Device debugging | Production test

ESP–NOW

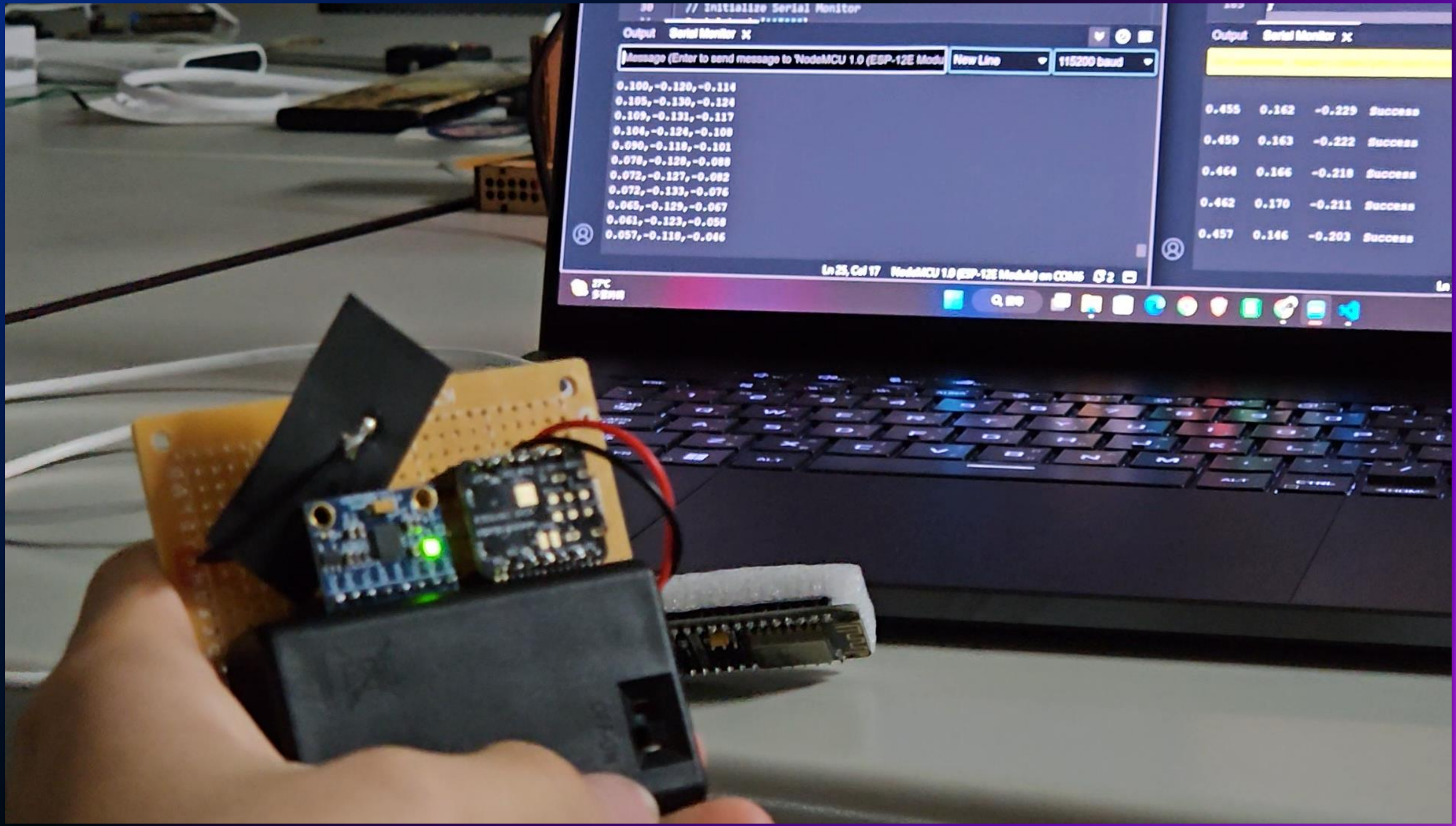
Data link layer（SLIP、PPP、MTU）

Physical layer（802.11b/g/n）



FIRST TRY

ESP32C3 → ESP8266 → PC

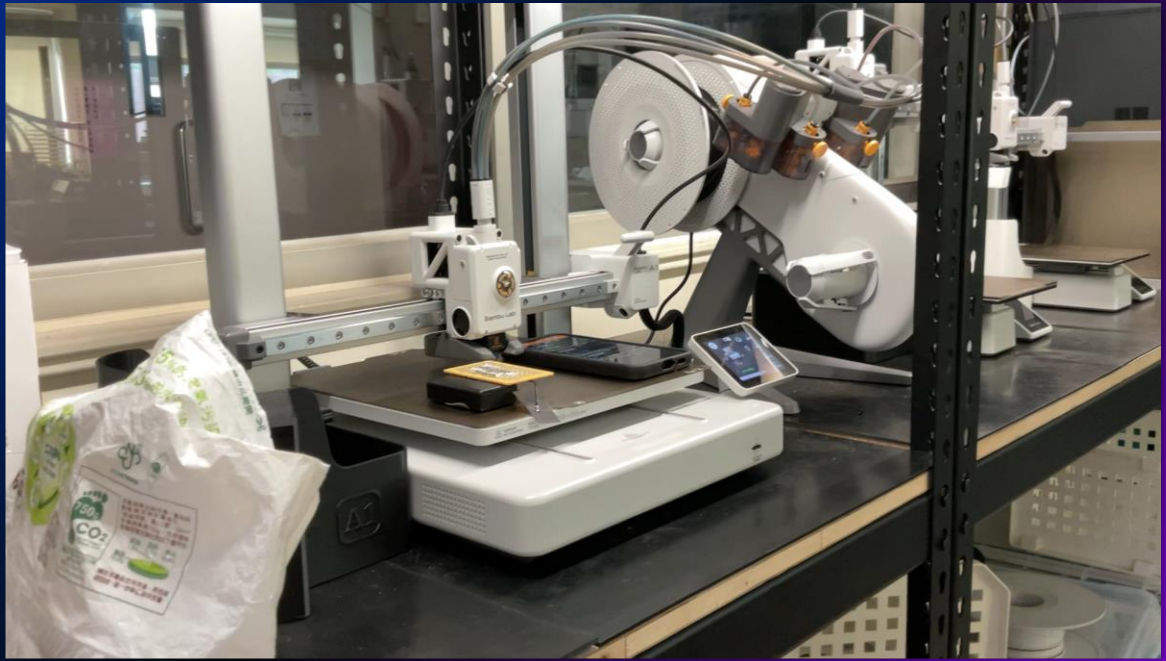

// Initialize Serial Monitor
Output
Serial Monitor
Message (Enter to send message to 'NodeMCU 1.0 (ESP-12E Modu
New Line
115200 baud
Ln 25, Col 17
NodeMCU 1.0 (ESP-12E Module) on COM5

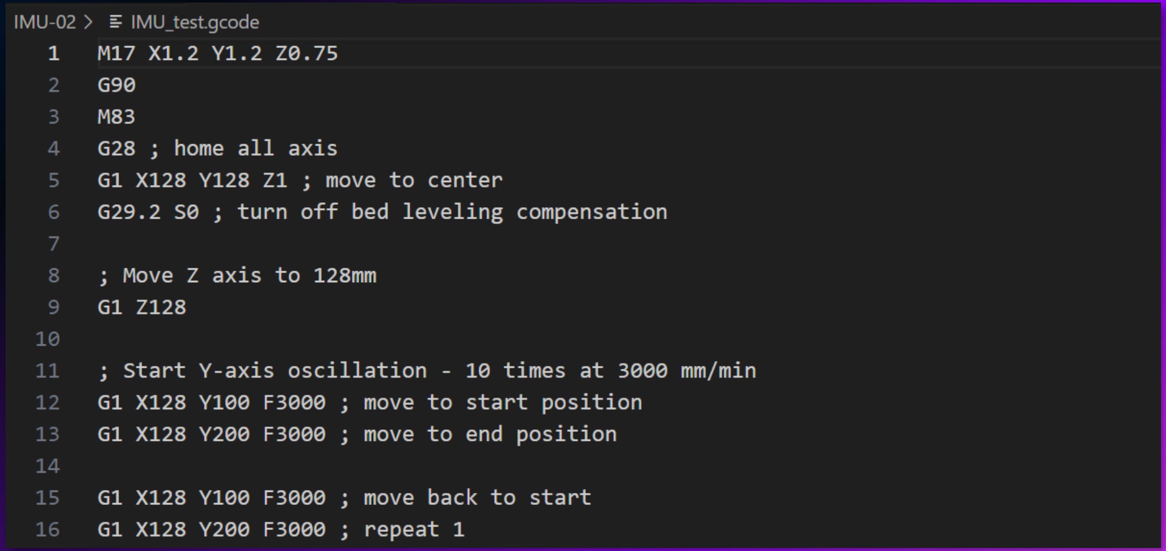
```
0.100,-0.120,-0.114
0.105,-0.130,-0.124
0.109,-0.131,-0.117
0.104,-0.124,-0.108
0.090,-0.118,-0.101
0.078,-0.128,-0.088
0.072,-0.127,-0.082
0.072,-0.133,-0.076
0.065,-0.129,-0.067
0.061,-0.123,-0.058
0.057,-0.118,-0.046
```

```
0.455   0.162   -0.229  Success
0.459   0.163   -0.222  Success
0.464   0.166   -0.218  Success
0.462   0.170   -0.211  Success
0.457   0.146   -0.203  Success
```

BUILD A TESTING PLATFORM

Compare the noise levels of **different** sensors, such as mobile phone sensors and IMU modules.

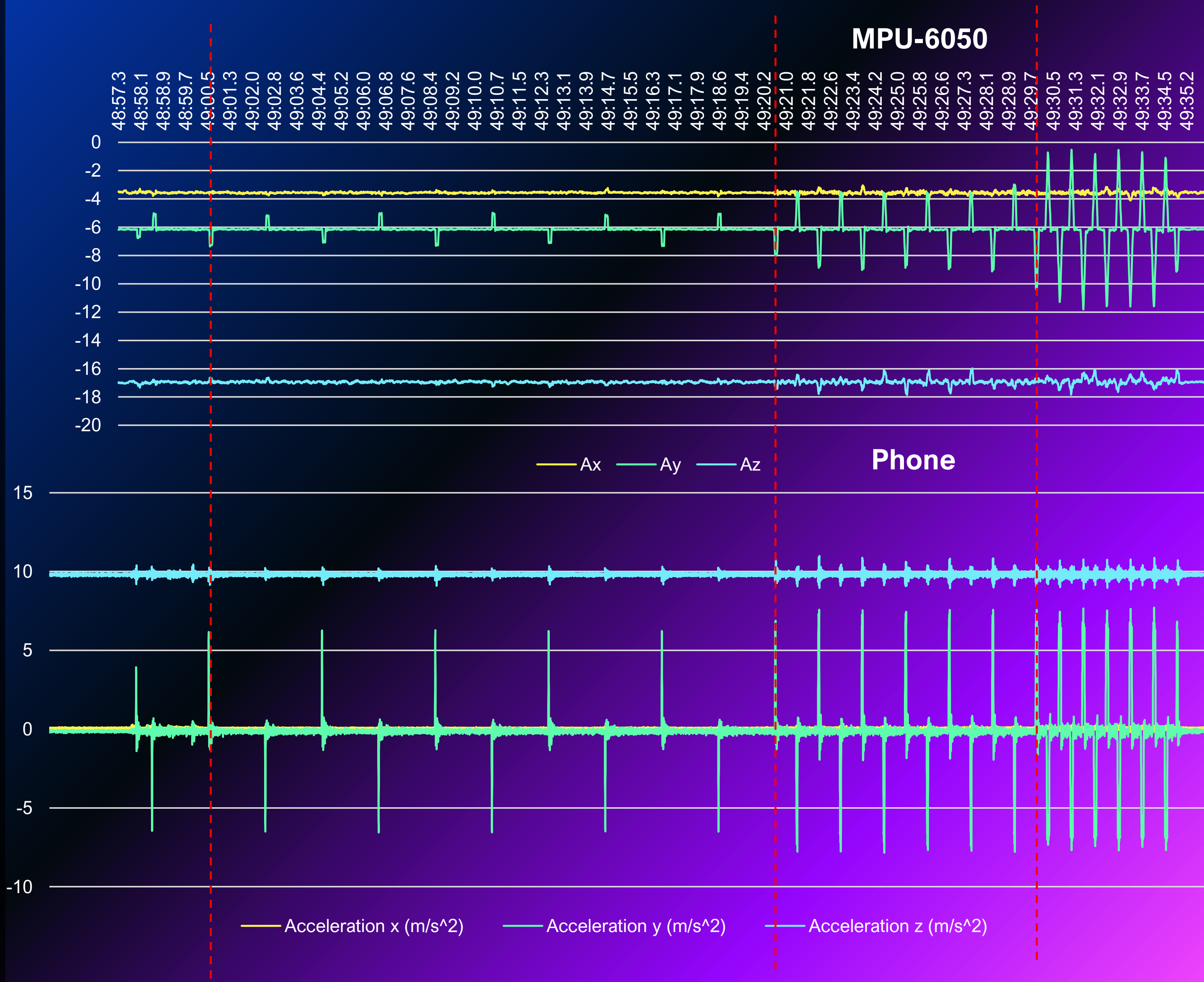




```
M17 X1.2 Y1.2 Z0.75
G90
M83
G28 ; home all axis
G1 X128 Y128 Z1 ; move to center
G29.2 S0 ; turn off bed leveling compensation

; Move Z axis to 128mm
G1 Z128

; Start Y-axis oscillation - 10 times at 3000 mm/min
G1 X128 Y100 F3000 ; move to start position
G1 X128 Y200 F3000 ; move to end position

G1 X128 Y100 F3000 ; move back to start
G1 X128 Y200 F3000 ; repeat 1
```

DIFF NOISE

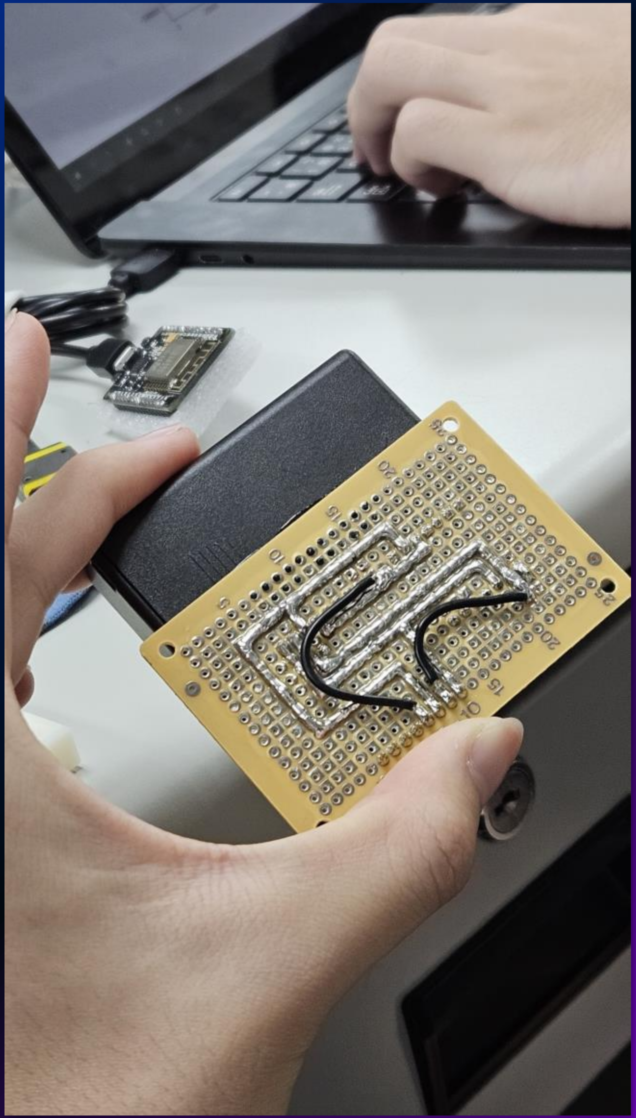
It can be observed from the graph that the noise produced by different sensors **varies significantly** without processing, and IMU sensors are also affected by **temperature and humidity**…

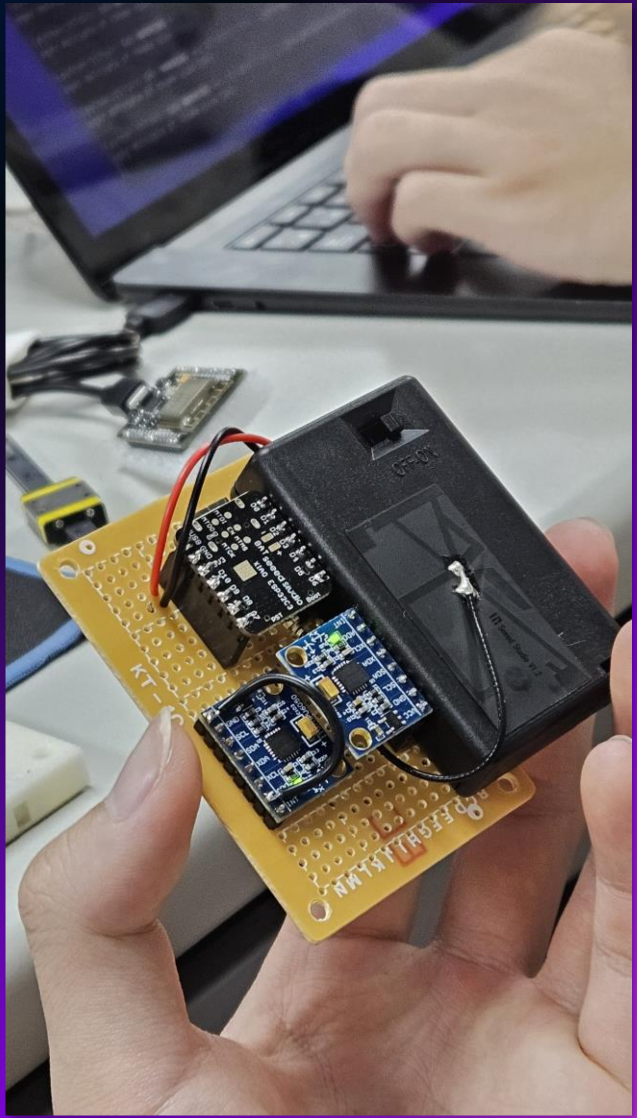


DOUBLE IT?

軟體不夠硬體來湊

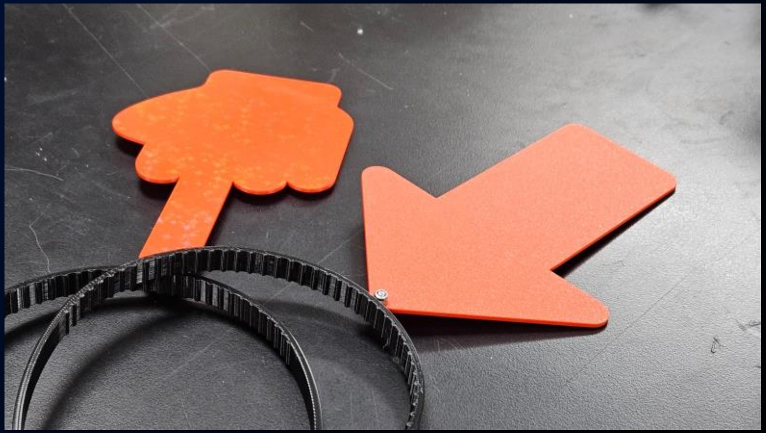
Some devices are equipped with more than one IMU, allowing us to append two random numbers within the **same frame**.

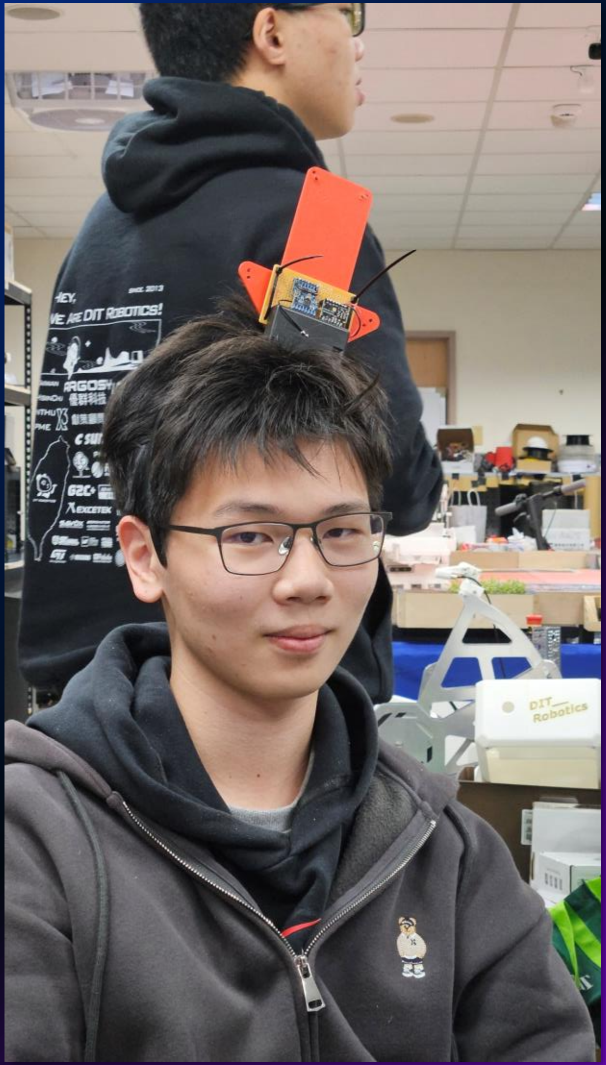


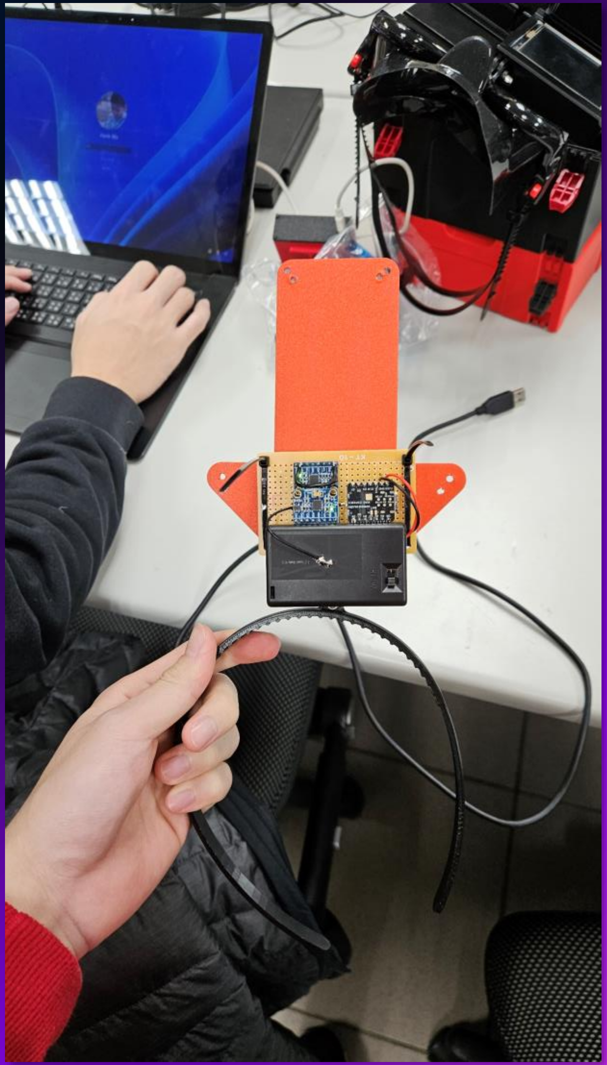


DATA COLLECTION SETUP

A 3D-printed headband is used to secure our IMU.

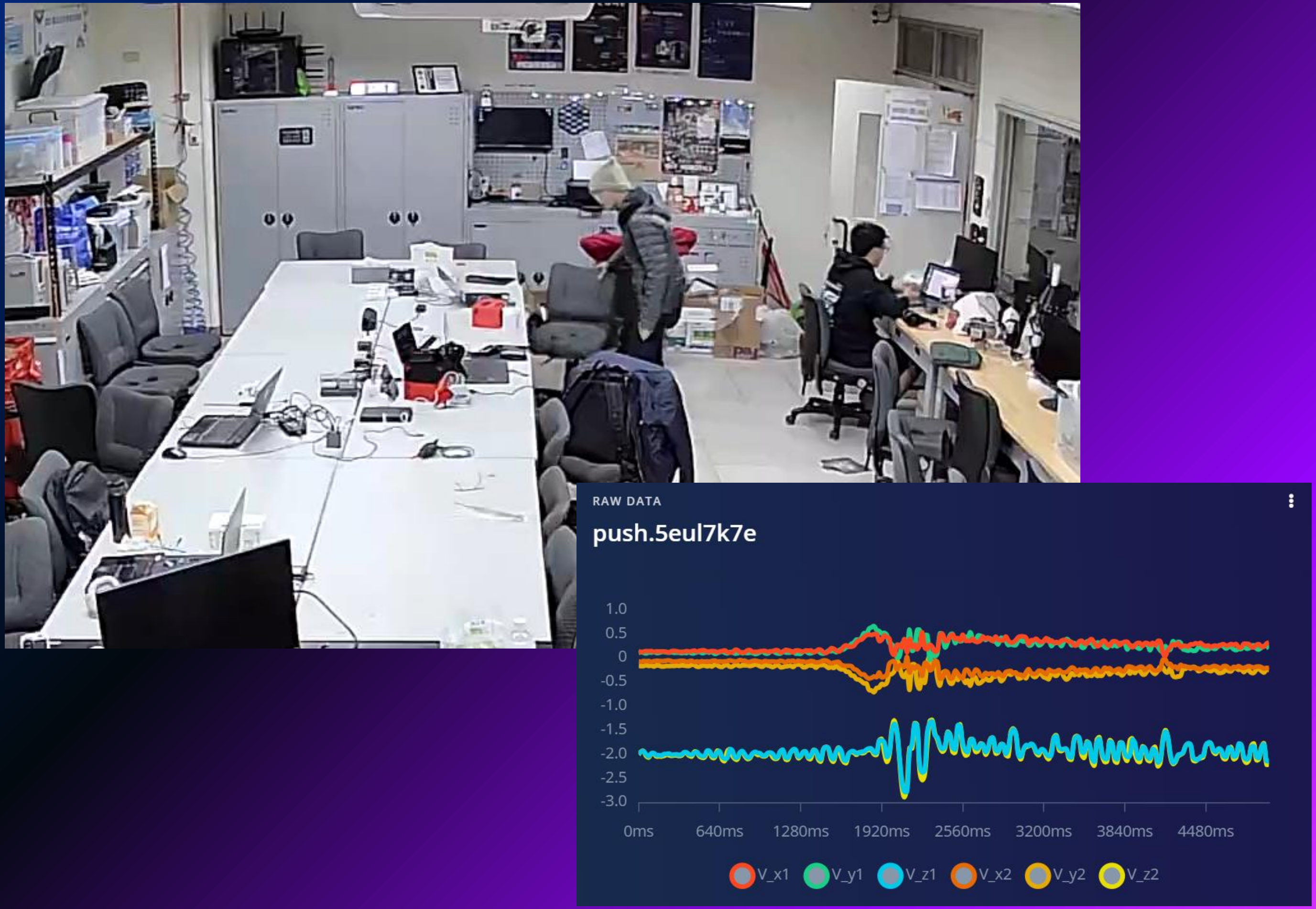






DATA COLLECTION

You can see six acceleration data lines in the graph.



Frame 1 bits → 68B84F...

Frame 2 bits → E58ADF...

⋮

Frame N bits → 243C4C...

Concatenate output hash values

Output → 68b84f...e58adf...243c4c...

Output value length < 1,000,000 bits?

Original value = 68b84f...e58adf...243c4c...

→ hash of original value = 66f76d...

Concatenate hash to original value

→ 68b84f...e58adf...243c4c...66f76d...

Repeat until >= 1,000,000 bits

(pad original ~200 sha256 values to ~3988 sha256 values)

[3988 * 256 = 1,020,928]

Why add SHA-256

- **Avalanche effect**

  different image frames with little changes will output completely different hash values.

- **Fixed output size**

  despite different devices outputting different image sizes, SHA256 always produces a 256-bit output regardless of input size.

- **Uniform distribution**

  output bits are distributed uniformly in cases of common pixel values.

RESULT & ANALYSIS

結果分析

IID TEST 1

MEAN = 0.499859:

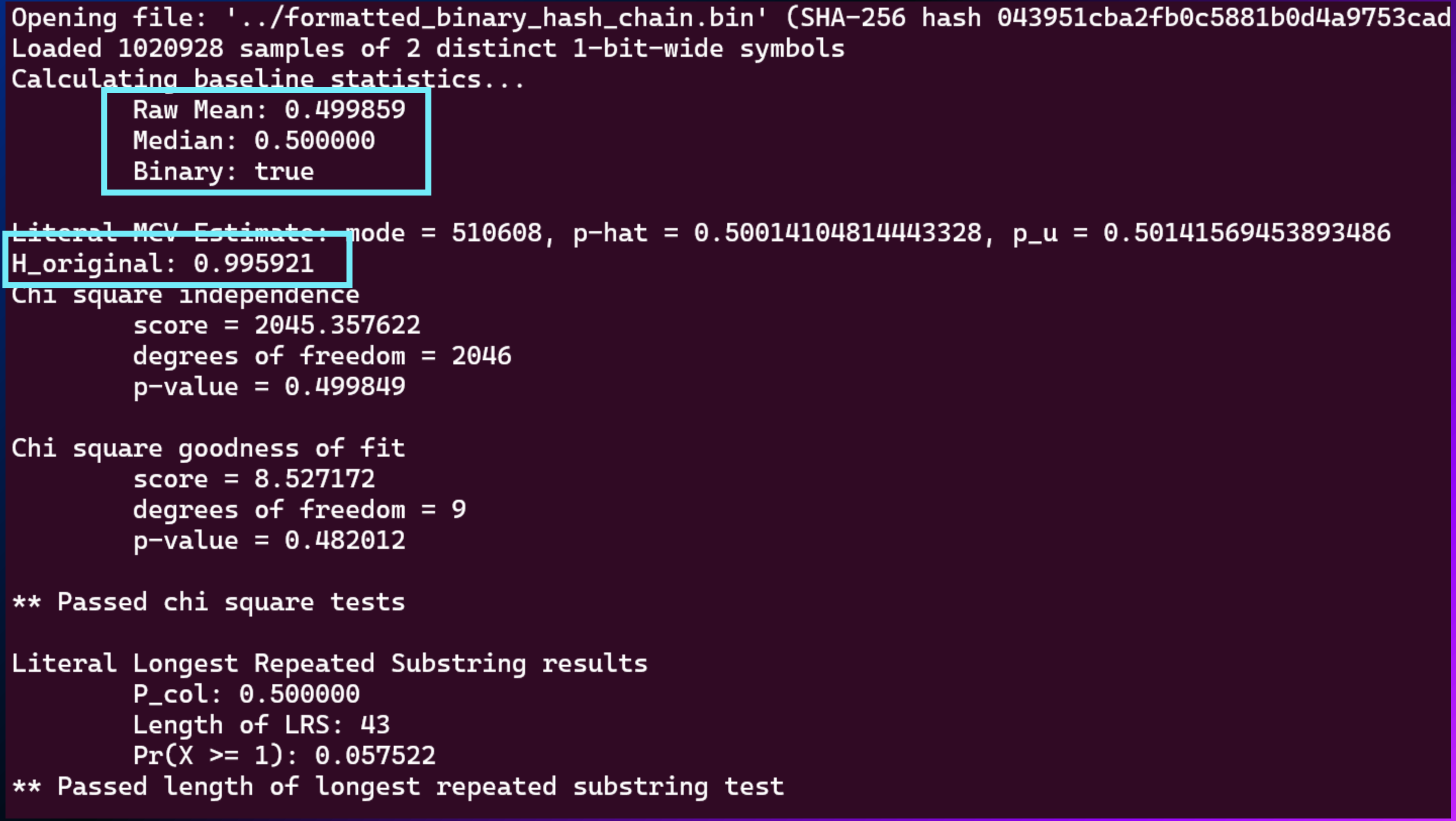
Close to 0.5, indicating that the data distribution is nearly balanced.

MEDIAN = 0.5:

Matches the ideal value.

H_original = 0.995921:

The original entropy is close to the ideal value of 1, suggesting that the data has high randomness.



```
Opening file: '../formatted_binary_hash_chain.bin' (SHA-256 hash 043951cba2fb0c5881b0d4a9753cad
Loaded 1020928 samples of 2 distinct 1-bit-wide symbols
Calculating baseline statistics...
        Raw Mean: 0.499859
        Median: 0.500000
        Binary: true

Literal MCV Estimate: mode = 510608, p-hat = 0.50014104814443328, p_u = 0.50141569453893486
H_original: 0.995921
Chi square independence
        score = 2045.357622
        degrees of freedom = 2046
        p-value = 0.499849

Chi square goodness of fit
        score = 8.527172
        degrees of freedom = 9
        p-value = 0.482012

** Passed chi square tests

Literal Longest Repeated Substring results
        P_col: 0.500000
        Length of LRS: 43
        Pr(X >= 1): 0.057522
** Passed length of longest repeated substring test
```

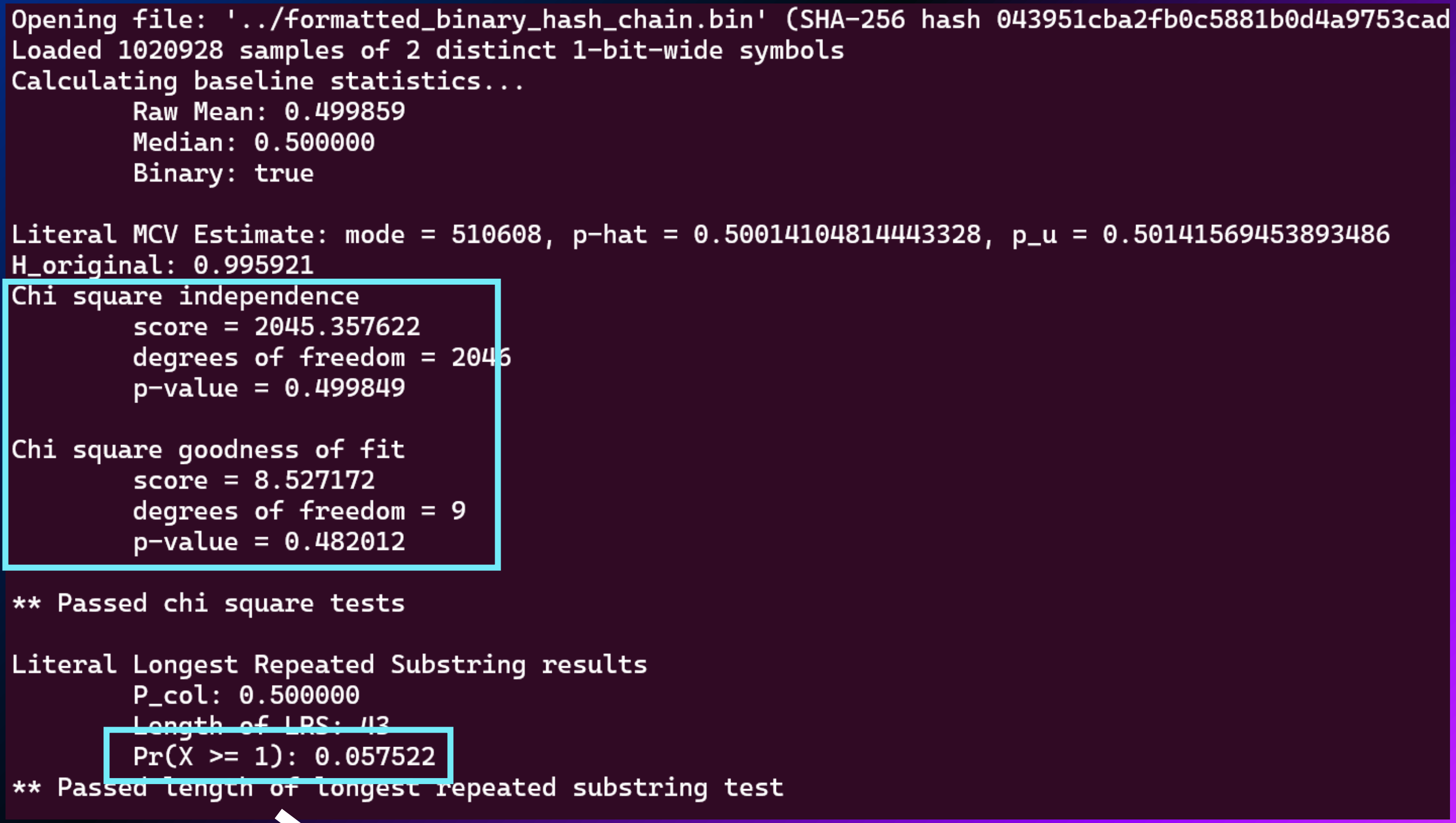
IID TEST 2

獨立性檢驗 (Chi-Square Independence):

A p-value greater than 0.05 indicates no significant evidence that the data is not independent.

適配度檢驗 (Chi-Square Goodness of Fit):

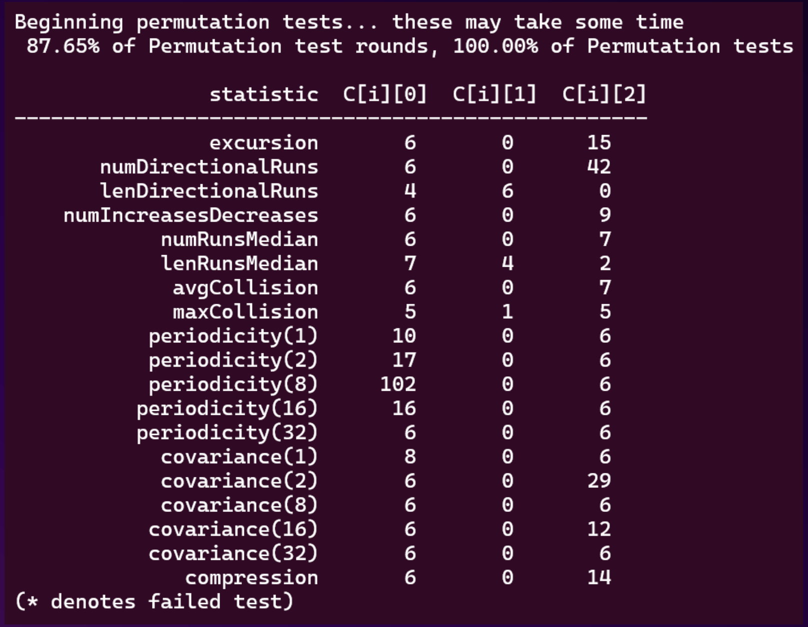
A p-value greater than 0.05 suggests that the data fits well with the theoretical distribution.



```
Opening file: '../formatted_binary_hash_chain.bin' (SHA-256 hash 043951cba2fb0c5881b0d4a9753cad
Loaded 1020928 samples of 2 distinct 1-bit-wide symbols
Calculating baseline statistics...
        Raw Mean: 0.499859
        Median: 0.500000
        Binary: true

Literal MCV Estimate: mode = 510608, p-hat = 0.50014104814443328, p_u = 0.50141569453893486
H_original: 0.995921
Chi square independence
        score = 2045.357622
        degrees of freedom = 2046
        p-value = 0.499849

Chi square goodness of fit
        score = 8.527172
        degrees of freedom = 9
        p-value = 0.482012

** Passed chi square tests

Literal Longest Repeated Substring results
        P_col: 0.500000
        Length of LRS: 43
        Pr(X >= 1): 0.057522
** Passed length of longest repeated substring test
```

最長重複子串測試 Pr(X >= 1) = 0.057522：表明出現長重複子串的概率較低，符合隨機性預期。

IID TEST 3



```
Beginning permutation tests... these may take some time
 87.65% of Permutation test rounds, 100.00% of Permutation tests

                statistic  C[i][0]  C[i][1]  C[i][2]
----------------------------------------------------
                excursion        6        0       15
       numDirectionalRuns        6        0       42
       lenDirectionalRuns        4        6        0
  numIncreasesDecreases          6        0        9
            numRunsMedian        6        0        7
            lenRunsMedian        7        4        2
             avgCollision        6        0        7
             maxCollision        5        1        5
           periodicity(1)       10        0        6
           periodicity(2)       17        0        6
           periodicity(8)      102        0        6
          periodicity(16)       16        0        6
          periodicity(32)        6        0        6
            covariance(1)        8        0        6
            covariance(2)        6        0       29
            covariance(8)        6        0        6
           covariance(16)        6        0       12
           covariance(32)        6        0        6
              compression        6        0       14
(* denotes failed test)
```

- Testing success rate: passed 87.65% testcases
- **Testing results:**

  C[i][0] : Passed count, C[I][1]: Undefined count, C[i][2]: Failed count

- Notable passed items:

  lenDirectionalRuns, periodicity, covariance having low failed counts

- **Caveats**

periodicity(8):

meaning the bias or deviation in the periodic patterns at 8-bit intervals.
(Limited to only 8'b00000000 or 8'b00000001)

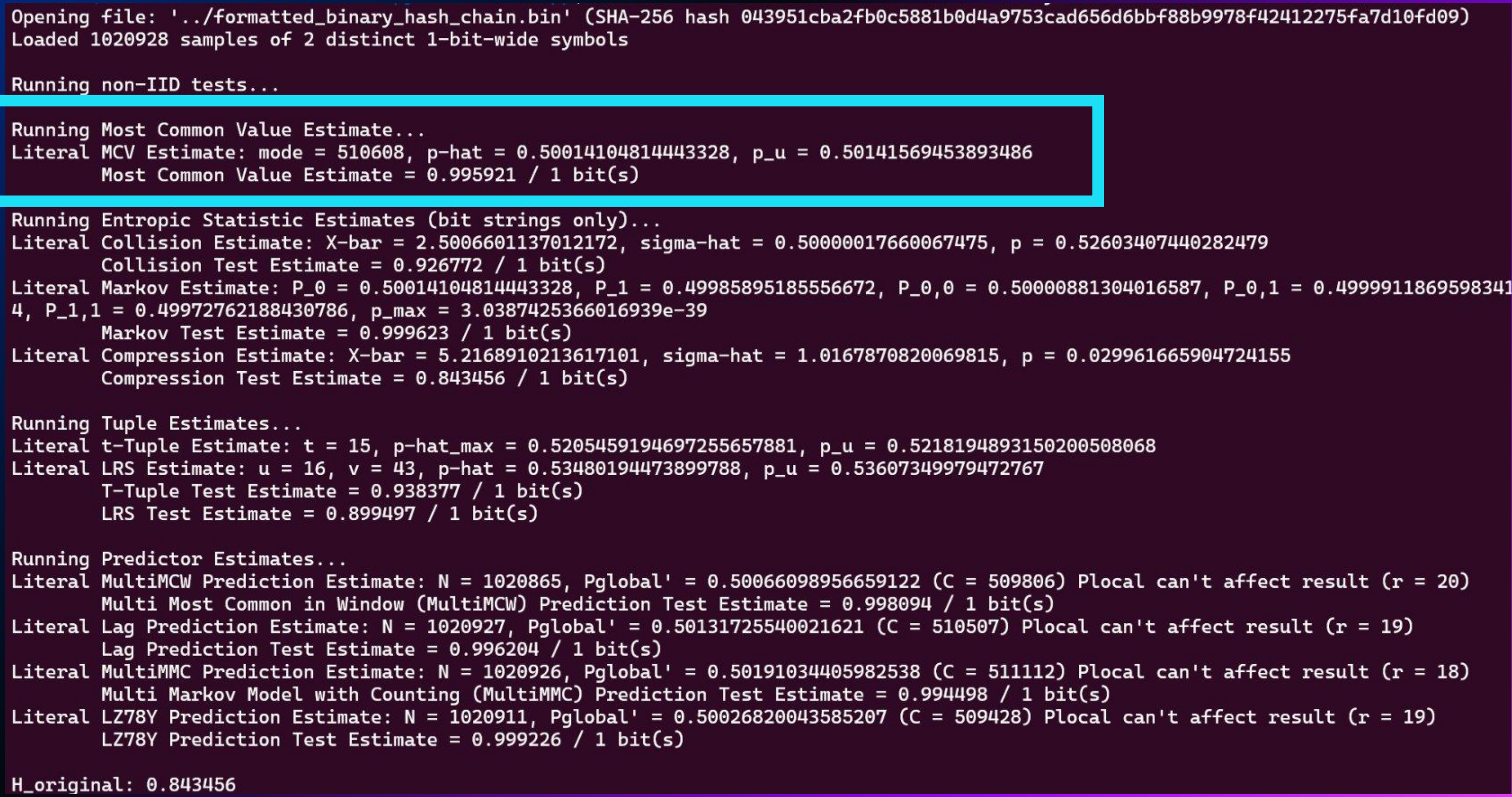
Covariance:

correlation in the data may be higher for lower periodic patterns
due to having many '0's in 8'b00000000 or 8'b00000001

NON IID TEST 1

Most Common Value (MCV) Estimate：

檢測數據流中最常見的值（例如0或1）的比例，p-hat ≈ 0.5001，代表數據中0和1的出現機率非常接近0.5，符合理論隨機分佈。



```
Opening file: '../formatted_binary_hash_chain.bin' (SHA-256 hash 043951cba2fb0c5881b0d4a9753cad656d6bbf88b9978f42412275fa7d10fd09)
Loaded 1020928 samples of 2 distinct 1-bit-wide symbols

Running non-IID tests...

Running Most Common Value Estimate...
Literal MCV Estimate: mode = 510608, p-hat = 0.50014104814443328, p_u = 0.50141569453893486
        Most Common Value Estimate = 0.995921 / 1 bit(s)

Running Entropic Statistic Estimates (bit strings only)...
Literal Collision Estimate: X-bar = 2.5006601137012172, sigma-hat = 0.50000017660067475, p = 0.52603407440282479
        Collision Test Estimate = 0.926772 / 1 bit(s)
Literal Markov Estimate: P_0 = 0.50014104814443328, P_1 = 0.49985895185556672, P_0,0 = 0.50000881304016587, P_0,1 = 0.4999911869598341
4, P_1,1 = 0.49972762188430786, p_max = 3.0387425366016939e-39
        Markov Test Estimate = 0.999623 / 1 bit(s)
Literal Compression Estimate: X-bar = 5.2168910213617101, sigma-hat = 1.0167870820069815, p = 0.029961665904724155
        Compression Test Estimate = 0.843456 / 1 bit(s)

Running Tuple Estimates...
Literal t-Tuple Estimate: t = 15, p-hat_max = 0.52054591946972557881, p_u = 0.5218194893150200508068
Literal LRS Estimate: u = 16, v = 43, p-hat = 0.53480194473899788, p_u = 0.53607349979472767
        T-Tuple Test Estimate = 0.938377 / 1 bit(s)
        LRS Test Estimate = 0.899497 / 1 bit(s)

Running Predictor Estimates...
Literal MultiMCW Prediction Estimate: N = 1020865, Pglobal' = 0.50066098956659122 (C = 509806) Plocal can't affect result (r = 20)
        Multi Most Common in Window (MultiMCW) Prediction Test Estimate = 0.998094 / 1 bit(s)
Literal Lag Prediction Estimate: N = 1020927, Pglobal' = 0.50131725540021621 (C = 510507) Plocal can't affect result (r = 19)
        Lag Prediction Test Estimate = 0.996204 / 1 bit(s)
Literal MultiMMC Prediction Estimate: N = 1020926, Pglobal' = 0.50191034405982538 (C = 511112) Plocal can't affect result (r = 18)
        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate = 0.994498 / 1 bit(s)
Literal LZ78Y Prediction Estimate: N = 1020911, Pglobal' = 0.50026820043585207 (C = 509428) Plocal can't affect result (r = 19)
        LZ78Y Prediction Test Estimate = 0.999226 / 1 bit(s)

H_original: 0.843456
```

NON IID TEST 2

Collision Test：

測量數據中重複值的平均次數（碰撞）

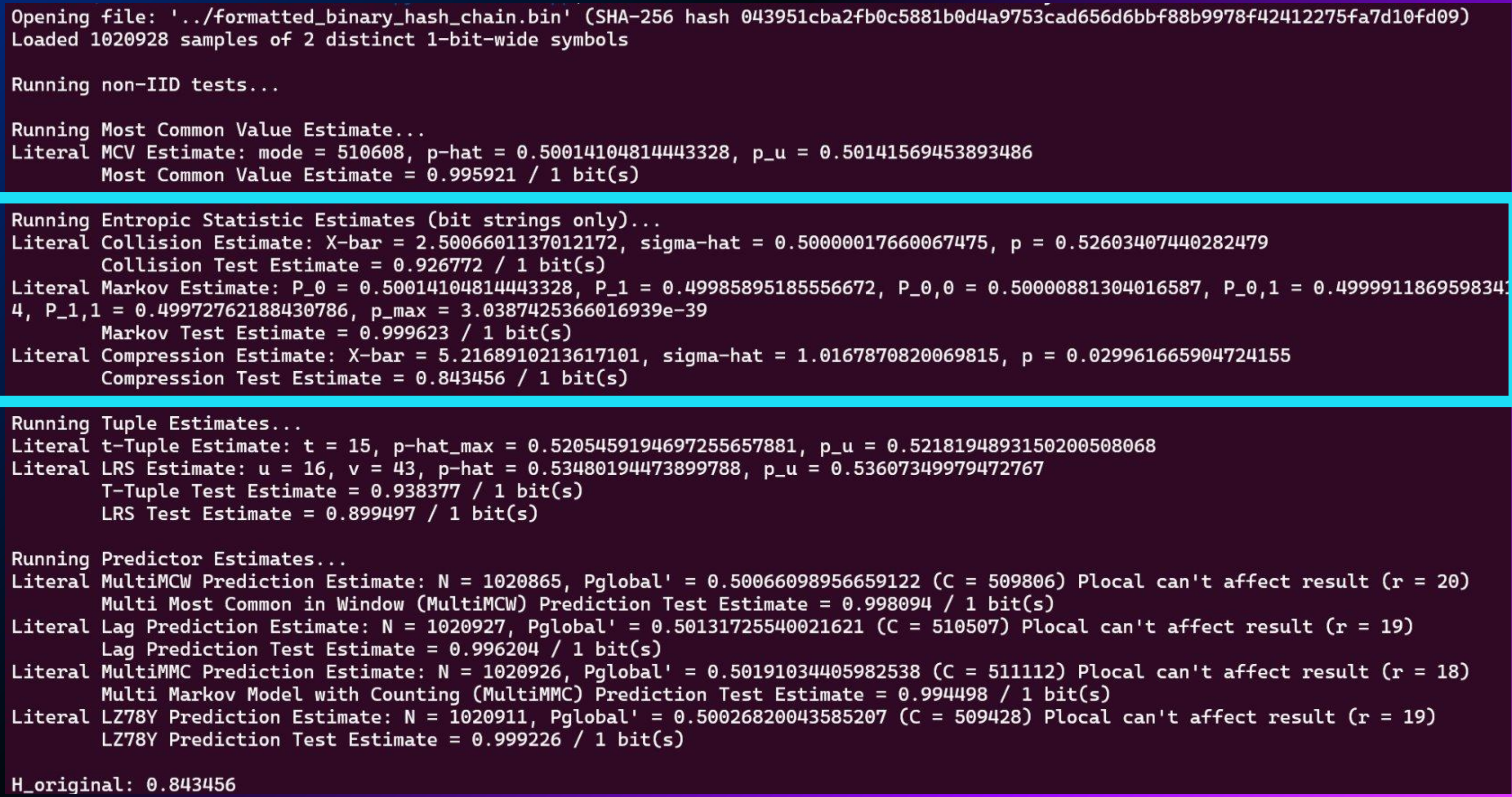
X-bar = 2.5000660113：碰撞的平均值。

Markov Test：

檢查數據的馬可夫性

【即是否存在**相鄰位間的依賴性**】

P_0,0和 P_0,1：表示從0轉移到0或1的機率

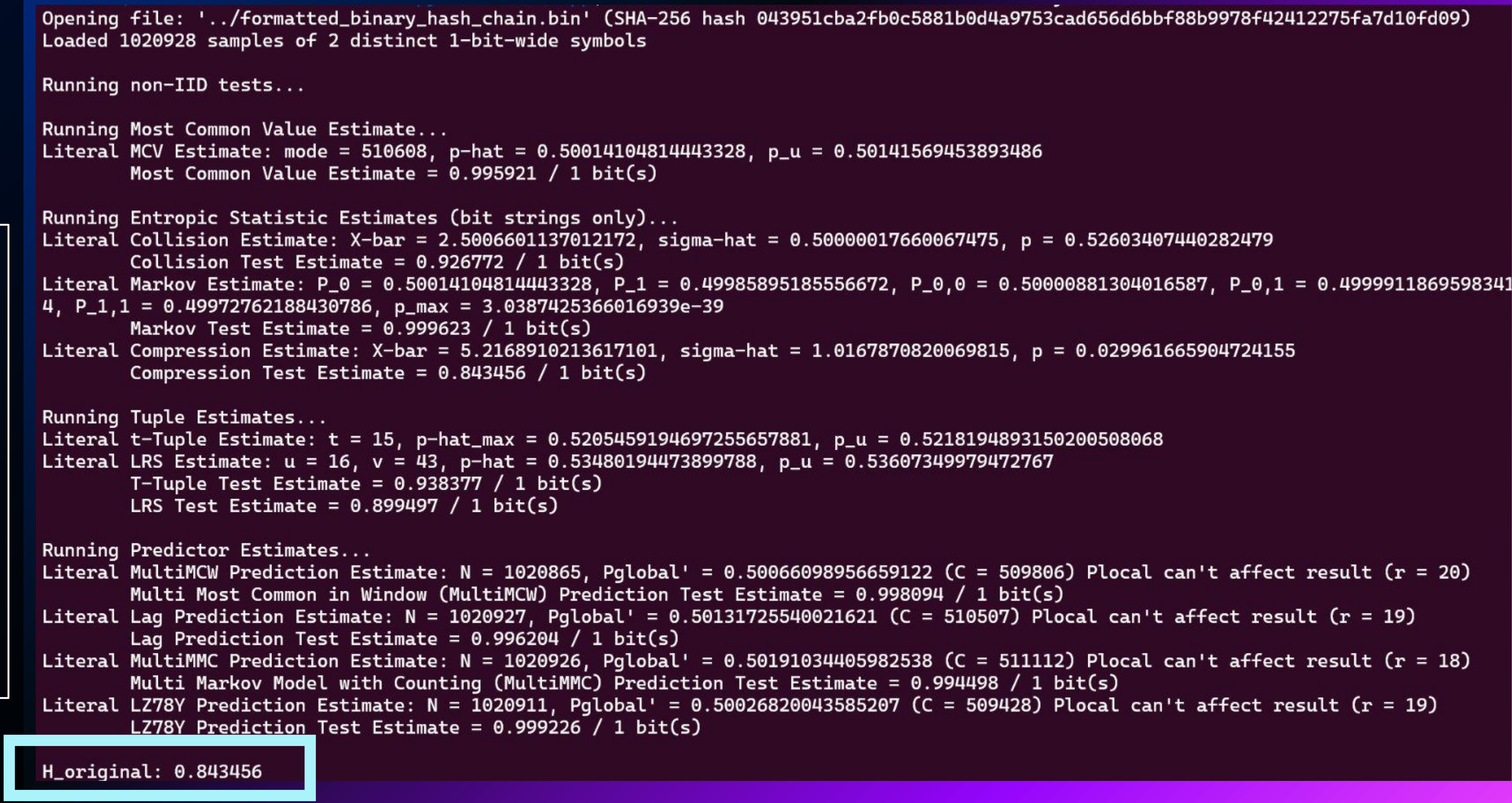


```
Opening file: '../formatted_binary_hash_chain.bin' (SHA-256 hash 043951cba2fb0c5881b0d4a9753cad656d6bbf88b9978f42412275fa7d10fd09)
Loaded 1020928 samples of 2 distinct 1-bit-wide symbols

Running non-IID tests...

Running Most Common Value Estimate...
Literal MCV Estimate: mode = 510608, p-hat = 0.50014104814443328, p_u = 0.50141569453893486
        Most Common Value Estimate = 0.995921 / 1 bit(s)

Running Entropic Statistic Estimates (bit strings only)...
Literal Collision Estimate: X-bar = 2.5006601137012172, sigma-hat = 0.50000017660067475, p = 0.52603407440282479
        Collision Test Estimate = 0.926772 / 1 bit(s)
Literal Markov Estimate: P_0 = 0.50014104814443328, P_1 = 0.49985895185556672, P_0,0 = 0.50000881304016587, P_0,1 = 0.499991186959834
4, P_1,1 = 0.49972762188430786, p_max = 3.0387425366016939e-39
        Markov Test Estimate = 0.999623 / 1 bit(s)
Literal Compression Estimate: X-bar = 5.2168910213617101, sigma-hat = 1.0167870820069815, p = 0.029961665904724155
        Compression Test Estimate = 0.843456 / 1 bit(s)

Running Tuple Estimates...
Literal t-Tuple Estimate: t = 15, p-hat_max = 0.5205459194697255657881, p_u = 0.5218194893150200508068
Literal LRS Estimate: u = 16, v = 43, p-hat = 0.53480194473899788, p_u = 0.53607349979472767
        T-Tuple Test Estimate = 0.938377 / 1 bit(s)
        LRS Test Estimate = 0.899497 / 1 bit(s)

Running Predictor Estimates...
Literal MultiMCW Prediction Estimate: N = 1020865, Pglobal' = 0.50066098956659122 (C = 509806) Plocal can't affect result (r = 20)
        Multi Most Common in Window (MultiMCW) Prediction Test Estimate = 0.998094 / 1 bit(s)
Literal Lag Prediction Estimate: N = 1020927, Pglobal' = 0.50131725540021621 (C = 510507) Plocal can't affect result (r = 19)
        Lag Prediction Test Estimate = 0.996204 / 1 bit(s)
Literal MultiMMC Prediction Estimate: N = 1020926, Pglobal' = 0.50191034405982538 (C = 511112) Plocal can't affect result (r = 18)
        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate = 0.994498 / 1 bit(s)
Literal LZ78Y Prediction Estimate: N = 1020911, Pglobal' = 0.50026820043585207 (C = 509428) Plocal can't affect result (r = 19)
        LZ78Y Prediction Test Estimate = 0.999226 / 1 bit(s)

H_original: 0.843456
```

NON IID TEST 3

MCV, Collision, Markov, Compression, Tuple, and Predictor tests show that the generated number have high randomness. **All the static result are close to theoretical value.**

H_original：0.84456. This indicate that the min-entropy of our data is **close to ideal value** 1.



```
Opening file: '../formatted_binary_hash_chain.bin' (SHA-256 hash 043951cba2fb0c5881b0d4a9753cad656d6bbf88b9978f42412275fa7d10fd09)
Loaded 1020928 samples of 2 distinct 1-bit-wide symbols

Running non-IID tests...

Running Most Common Value Estimate...
Literal MCV Estimate: mode = 510608, p-hat = 0.50014104814443328, p_u = 0.50141569453893486
        Most Common Value Estimate = 0.995921 / 1 bit(s)

Running Entropic Statistic Estimates (bit strings only)...
Literal Collision Estimate: X-bar = 2.5006601137012172, sigma-hat = 0.50000017660067475, p = 0.52603407440282479
        Collision Test Estimate = 0.926772 / 1 bit(s)
Literal Markov Estimate: P_0 = 0.50014104814443328, P_1 = 0.49985895185556672, P_0,0 = 0.50000881304016587, P_0,1 = 0.4999911869598341
4, P_1,1 = 0.49972762188430786, p_max = 3.0387425366016939e-39
        Markov Test Estimate = 0.999623 / 1 bit(s)
Literal Compression Estimate: X-bar = 5.2168910213617101, sigma-hat = 1.0167870820069815, p = 0.029961665904724155
        Compression Test Estimate = 0.843456 / 1 bit(s)

Running Tuple Estimates...
Literal t-Tuple Estimate: t = 15, p-hat_max = 0.52054591946972557881, p_u = 0.52181948931502005O8068
Literal LRS Estimate: u = 16, v = 43, p-hat = 0.53480194473899788, p_u = 0.53607349979472767
        T-Tuple Test Estimate = 0.938377 / 1 bit(s)
        LRS Test Estimate = 0.899497 / 1 bit(s)

Running Predictor Estimates...
Literal MultiMCW Prediction Estimate: N = 1020865, Pglobal' = 0.50066098956659122 (C = 509806) Plocal can't affect result (r = 20)
        Multi Most Common in Window (MultiMCW) Prediction Test Estimate = 0.998094 / 1 bit(s)
Literal Lag Prediction Estimate: N = 1020927, Pglobal' = 0.50131725540021621 (C = 510507) Plocal can't affect result (r = 19)
        Lag Prediction Test Estimate = 0.996204 / 1 bit(s)
Literal MultiMMC Prediction Estimate: N = 1020926, Pglobal' = 0.50191034405982538 (C = 511112) Plocal can't affect result (r = 18)
        Multi Markov Model with Counting (MultiMMC) Prediction Test Estimate = 0.994498 / 1 bit(s)
Literal LZ78Y Prediction Estimate: N = 1020911, Pglobal' = 0.50026820043585207 (C = 509428) Plocal can't affect result (r = 19)
        LZ78Y Prediction Test Estimate = 0.999226 / 1 bit(s)

H_original: 0.843456
```

你已被飛行荷蘭人的鬼船造訪
你的期末結果將會和鬼船一樣
過了！過了！過了！
隨便啦
過了…過了…過了…

Q&A

THANK YOU

111000225	111000212	111000178
張皓翔	吳承輸	連正文