SensorID

Sensor Calibration Fingerprinting for Smartphones

CVE-2019-8541

Stan (Jiexin) Zhang, Alastair Beresford

{jz448, arb33}@cl.cam.ac.uk

University of Cambridge

Ian Sheret

ian.sheret@polymathinsight.co.uk

Polymath Insight Limited

Device Fingerprinting

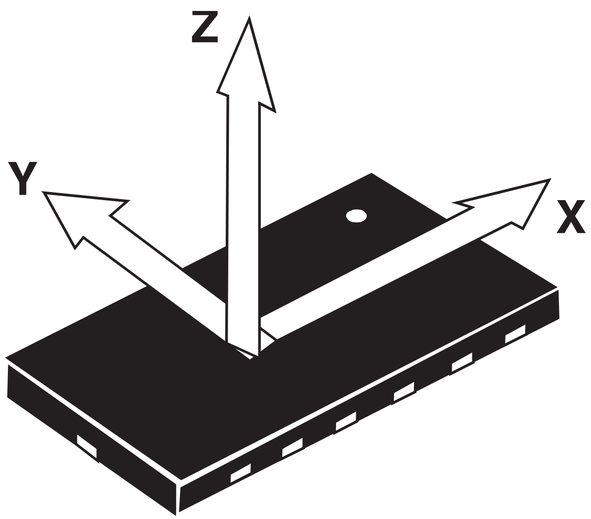
Device fingerprinting aims to generate a distinctive signature, or fingerprint, that uniquely identifies a specific computing device.

With a reliable device fingerprint, advertisers can track users online and offline, study their behaviour, deliver tailored content, etc.

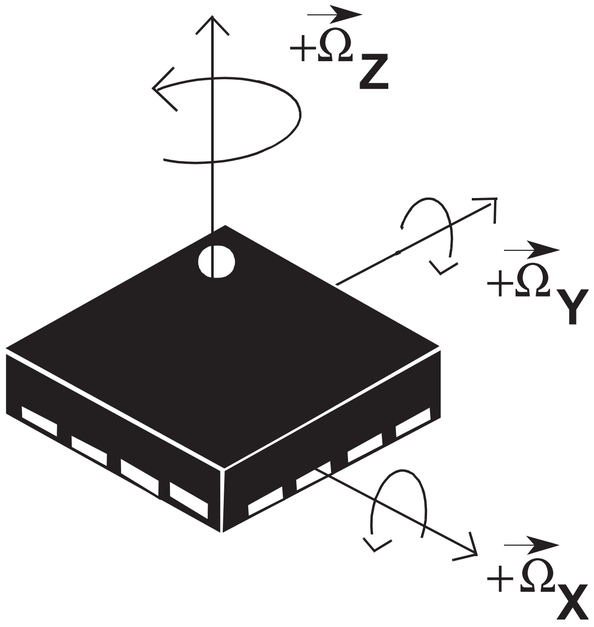
To protect user privacy, both Android and iOS have applied a variety of measures to prevent device fingerprinting.

Motion Sensors in Smartphones

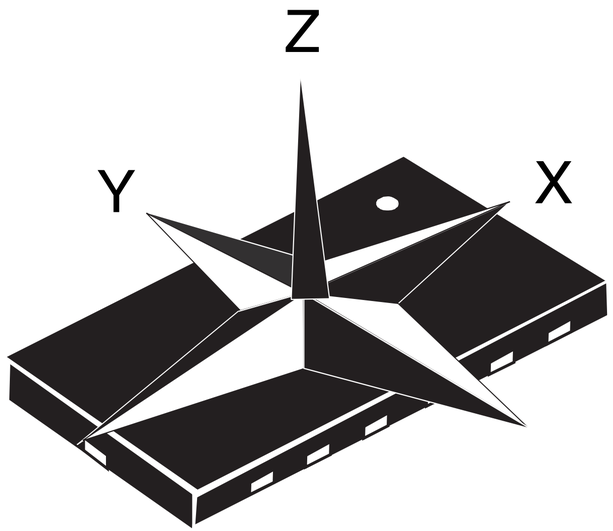
Accelerometer



Gyroscope



Magnetometer



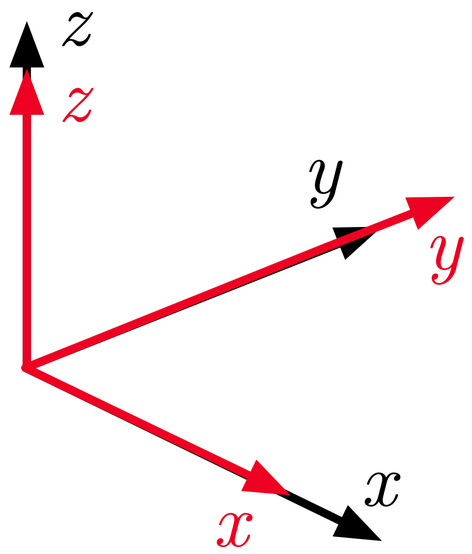
A ***calibration fingerprinting attack*** infers the per-device factory calibration data from a device by careful analysis of the sensor output alone.

- attack takes less than 1 second
- requires no permission or interaction from the user
- can be launched from both a mobile website and an mobile app
- can generate a globally unique and consistent fingerprint

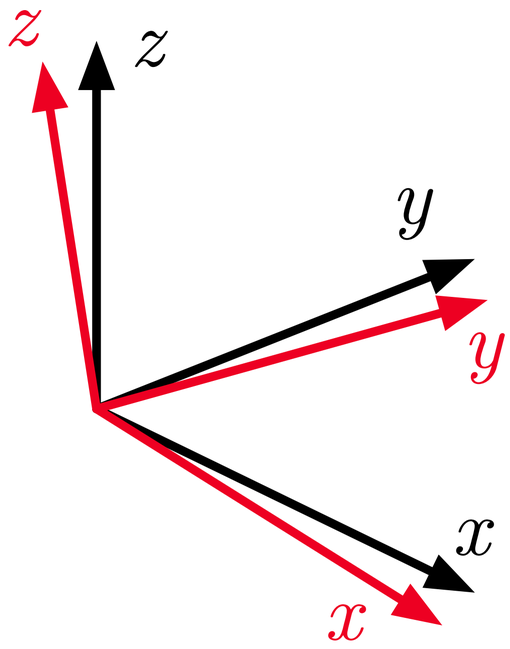

13:44
General
About
Name
iPhone
Songs
0
Videos
0
Photos
0
Applications
9
Capacity
256 GB
Available
244.77 GB
Version
12.0.1 (16A405)
Model
MT9H2B/A
Serial Number
G0NXM2Q6KPG4
Wi-Fi Address
6C:E8:5C:DC:78:90
Bluetooth
6C:E8:5C:C6:2B:43
1.00.08
SEID
13:44
General
About
Name
Test's iPhone
Songs
0
Videos
0
Photos
5
Applications
4
Capacity
64 GB
Available
57.69 GB
Version
12.1.1 (16C50)
Model
MT9E2B/A
Serial Number
G0NXHAWLKPG1
Wi-Fi Address
F8:38:80:78:BD:6D
Bluetooth
F8:38:80:7C:A9:5E
Modem Firmware
1.02.18
SEID
EID
Two iPhone XS devices
with different storage size

Deterministic Errors in Motion Sensors

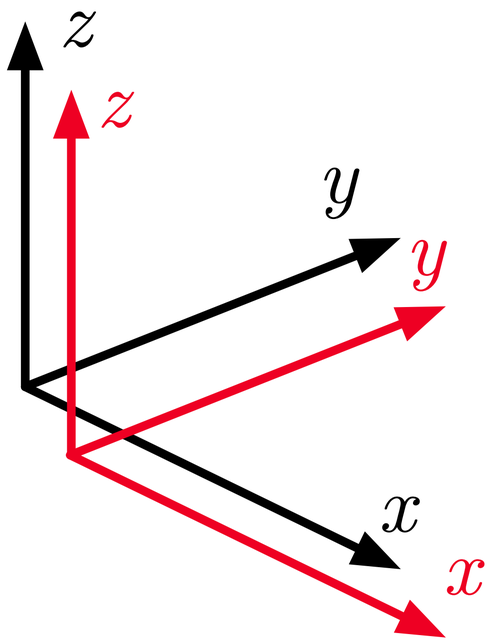
Scale Error



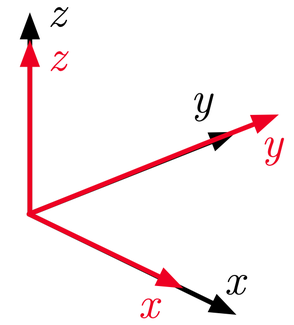
Non-orthogonality



Bias

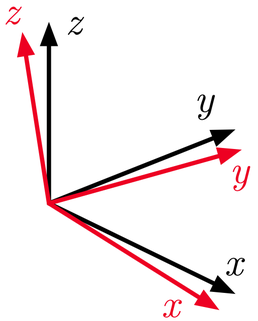


Motion Sensor Calibration



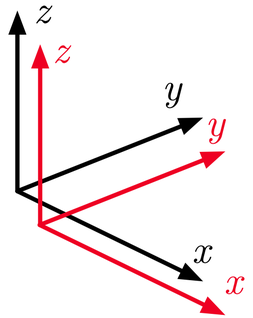
Scale Error

$$\mathbf{S} = \begin{bmatrix} S_x & 0 & 0 \\ 0 & S_y & 0 \\ 0 & 0 & S_z \end{bmatrix}$$



Non-orthogonality

$$\mathbf{N} = \begin{bmatrix} N_{xx} & N_{xy} & N_{xz} \\ N_{yx} & N_{yy} & N_{yz} \\ N_{zx} & N_{zy} & N_{zz} \end{bmatrix}$$



Bias

$$\mathbf{B} = \begin{bmatrix} B_x \\ B_y \\ B_z \end{bmatrix}$$

Motion Sensor Calibration

Sensor Output = Scale * Non-orthogonality * ADC output + Bias

$$\begin{bmatrix} O_x \\ O_y \\ O_z \end{bmatrix} = \begin{bmatrix} S_x & 0 & 0 \\ 0 & S_y & 0 \\ 0 & 0 & S_z \end{bmatrix} \begin{bmatrix} N_{xx} & N_{xy} & N_{xz} \\ N_{yx} & N_{yy} & N_{yz} \\ N_{zx} & N_{zy} & N_{zz} \end{bmatrix} \begin{bmatrix} A_x \\ A_y \\ A_z \end{bmatrix} + \begin{bmatrix} B_x \\ B_y \\ B_z \end{bmatrix}$$

Or

$$\mathbf{O} = \mathbf{GA} + \mathbf{B}$$

A = ADC output, **O** = sensor output, **G** = gain matrix

Sensor Calibration Fingerprinting

$$\mathbf{O}_1 = \mathbf{G}\mathbf{A}_1 + \mathbf{B}$$

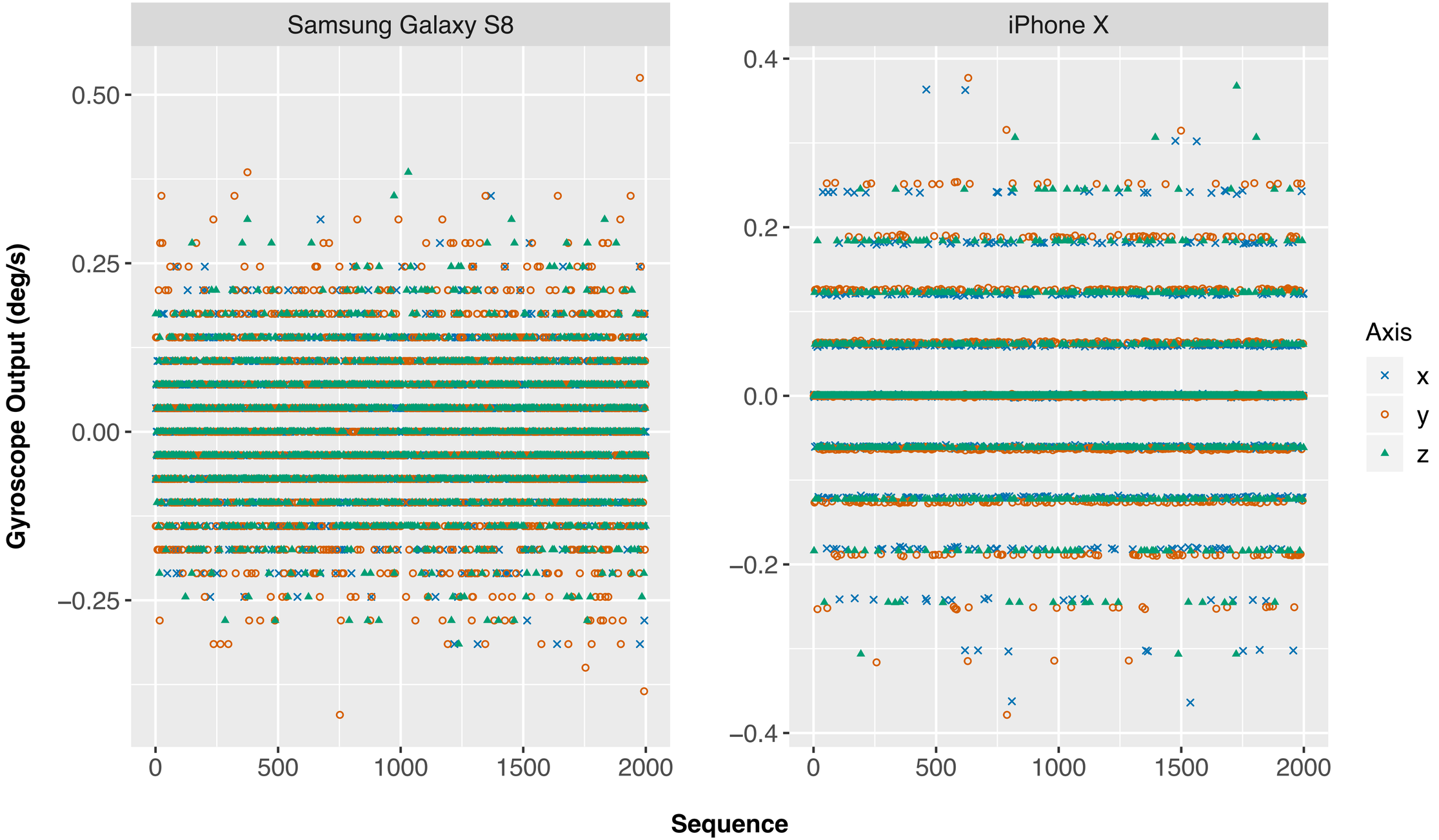
$$\mathbf{O}_2 = \mathbf{G}\mathbf{A}_2 + \mathbf{B}$$

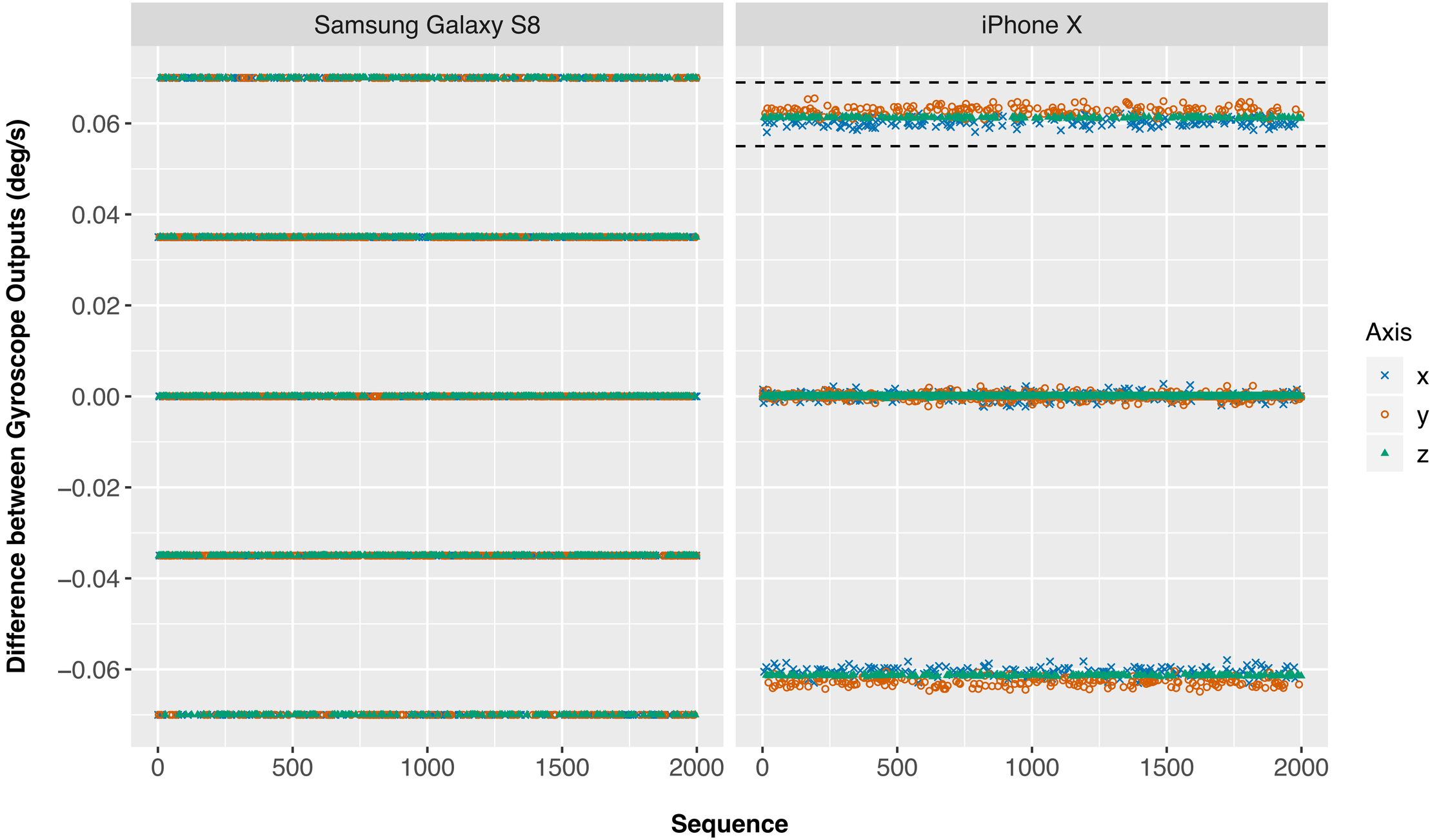
$$\mathbf{O}_2 - \mathbf{O}_1 = \mathbf{G}(\mathbf{A}_2 - \mathbf{A}_1)$$

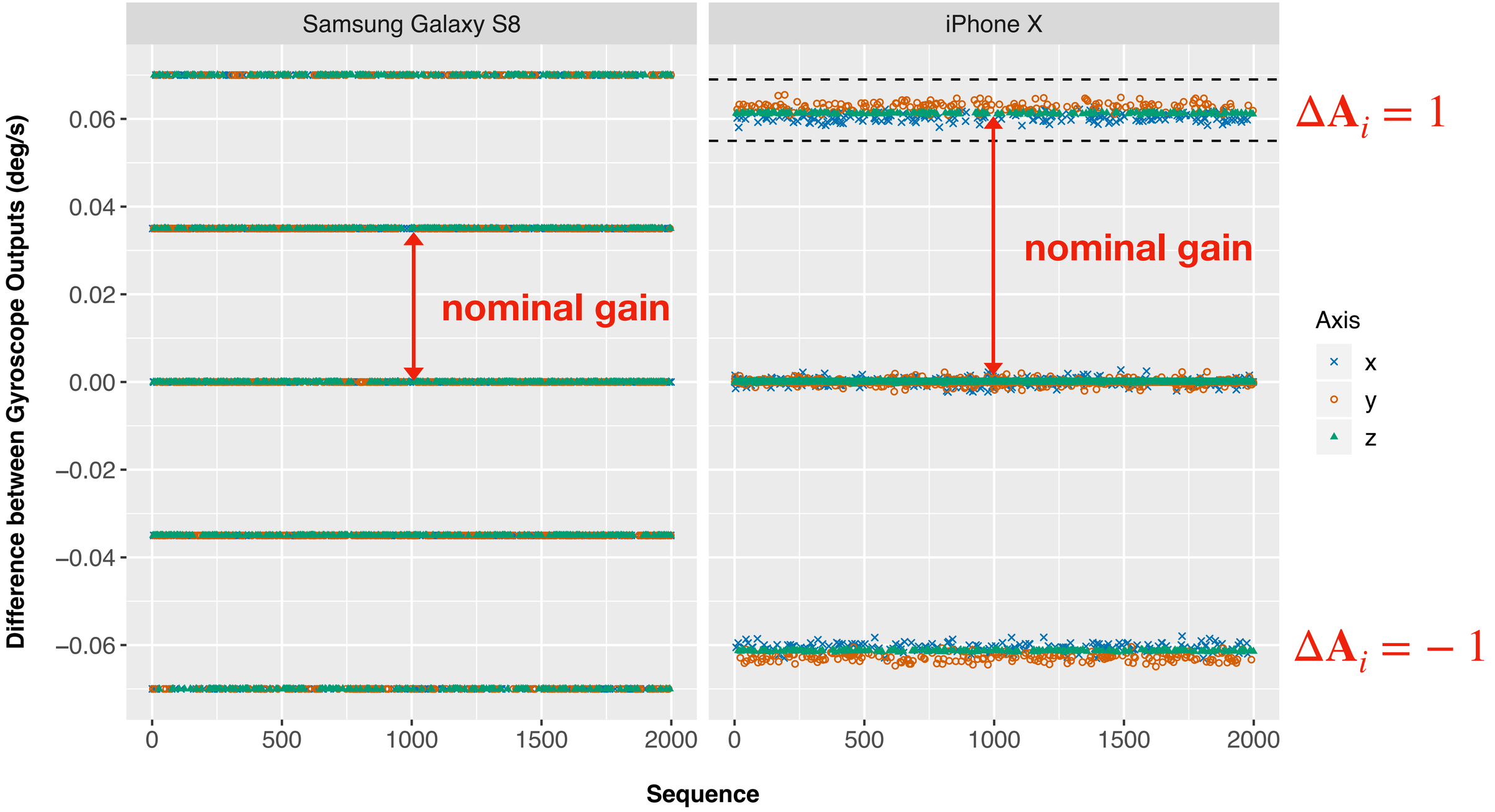
$$[\mathbf{O}_2 - \mathbf{O}_1, \cdots, \mathbf{O}_n - \mathbf{O}_{n-1}] = \mathbf{G}[\mathbf{A}_2 - \mathbf{A}_1, \cdots, \mathbf{A}_n - \mathbf{A}_{n-1}]$$

$$\Delta\mathbf{O} = \mathbf{G}\Delta\mathbf{A}$$

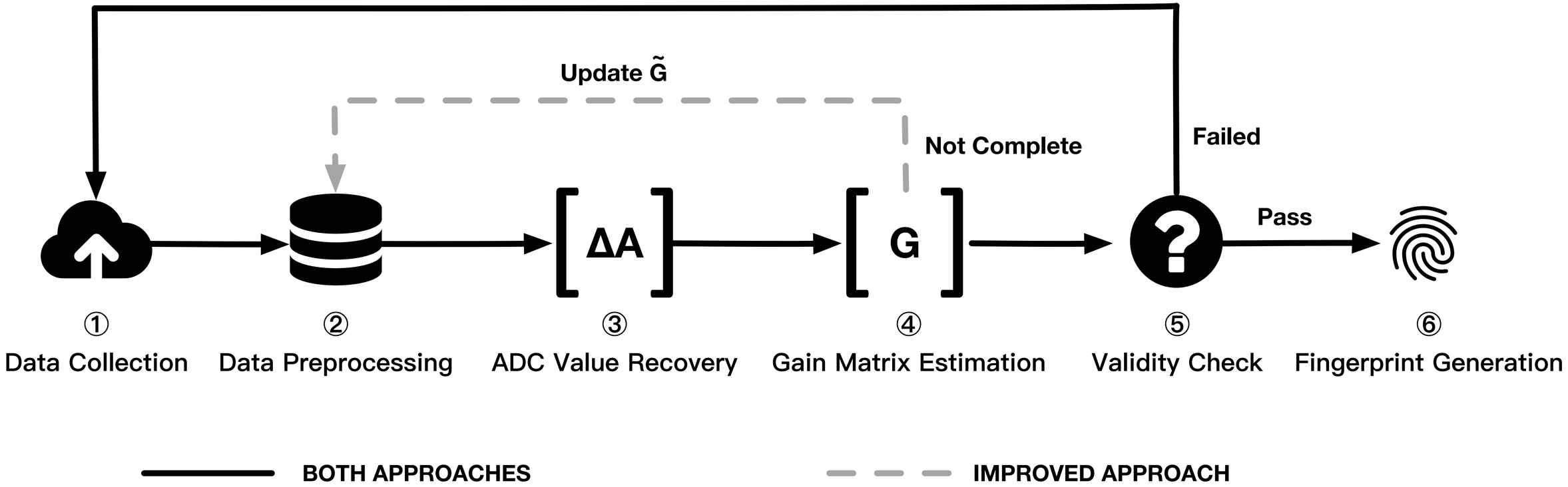
ΔA: all values are integers

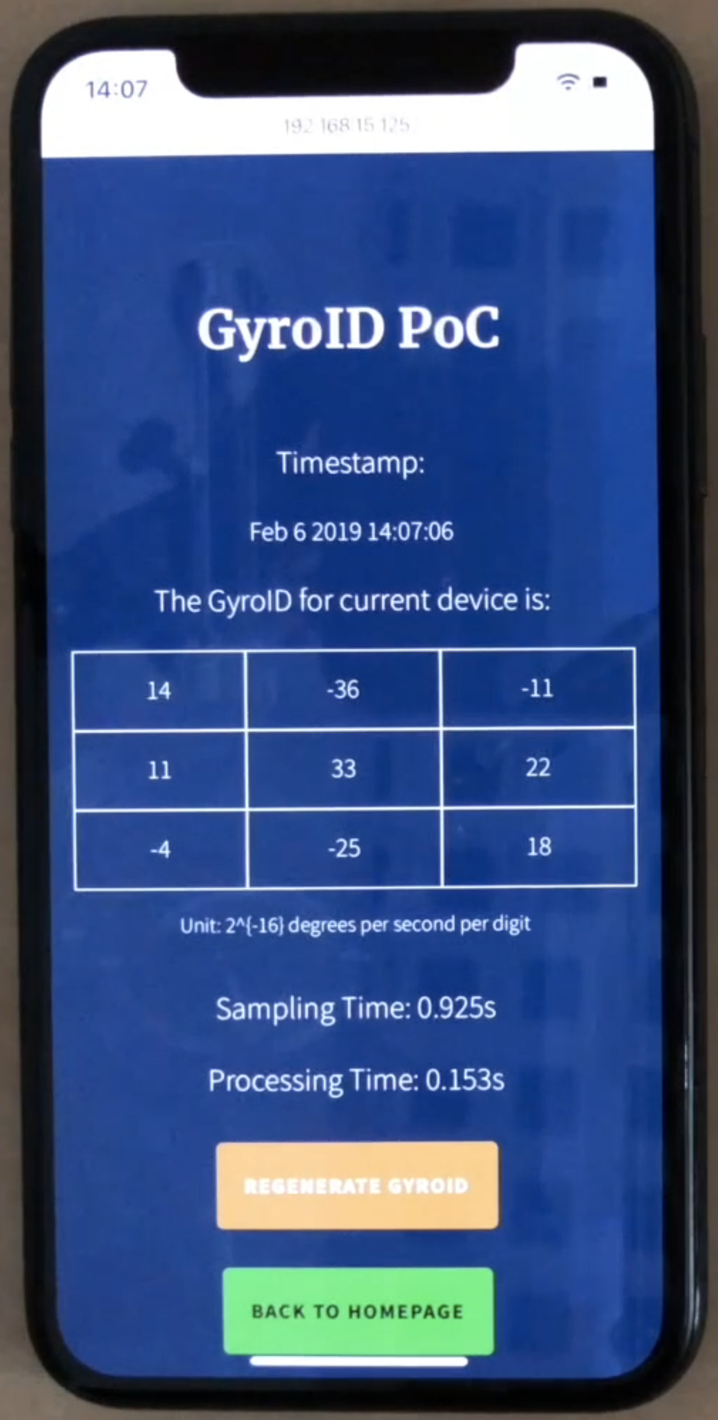

Samsung Galaxy S8
iPhone X
Gyroscope Output (deg/s)
0.50
0.25
0.00
−0.25
0.4
0.2
0.0
−0.2
−0.4
0
500
1000
1500
2000
Sequence
Axis
x
y
z

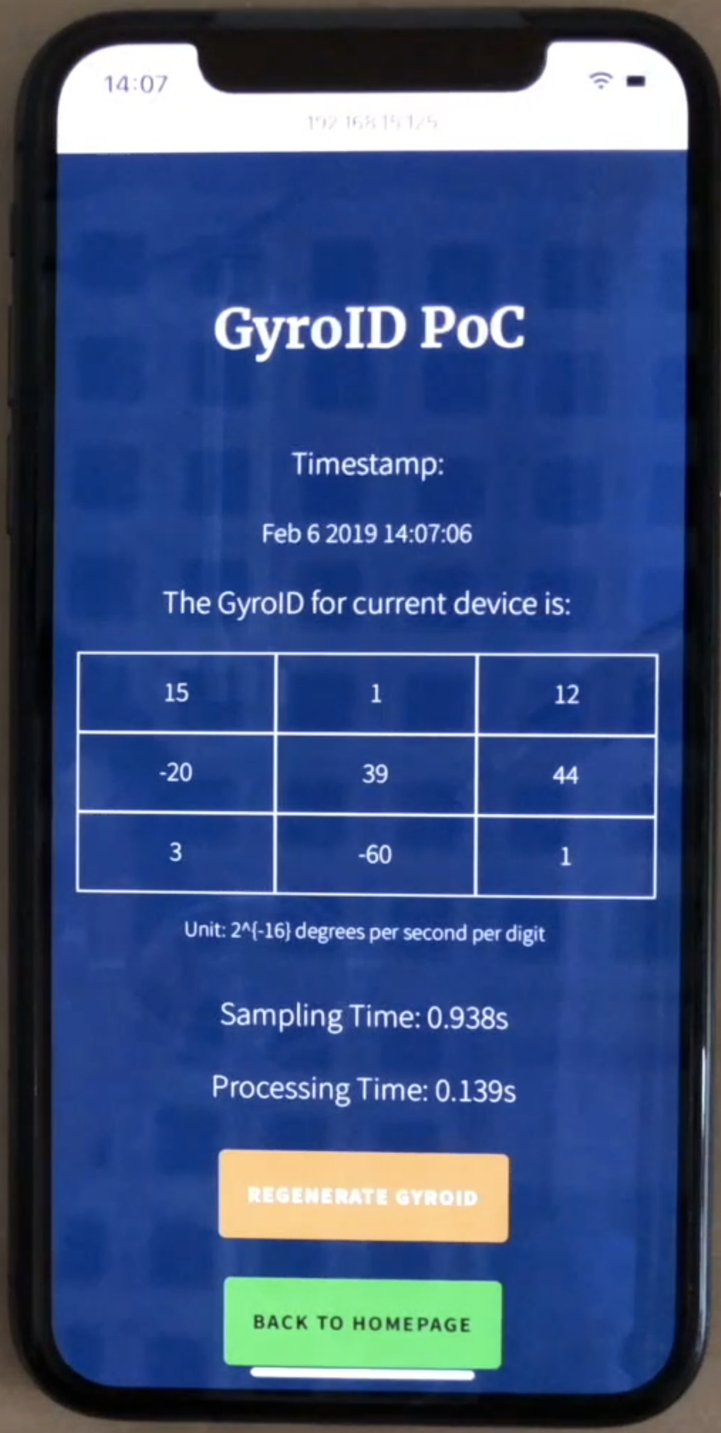

Samsung Galaxy S8
iPhone X
Difference between Gyroscope Outputs (deg/s)
0.06
0.04
0.02
0.00
−0.02
−0.04
−0.06
0
500
1000
1500
2000
Sequence
Axis
x
y
z


Samsung Galaxy S8
iPhone X
Difference between Gyroscope Outputs (deg/s)
0.06
0.04
0.02
0.00
−0.02
−0.04
−0.06
nominal gain
nominal gain
0
500
1000
1500
2000
Sequence
Axis
x
y
z
$\Delta A_i = 1$
$\Delta A_i = -1$

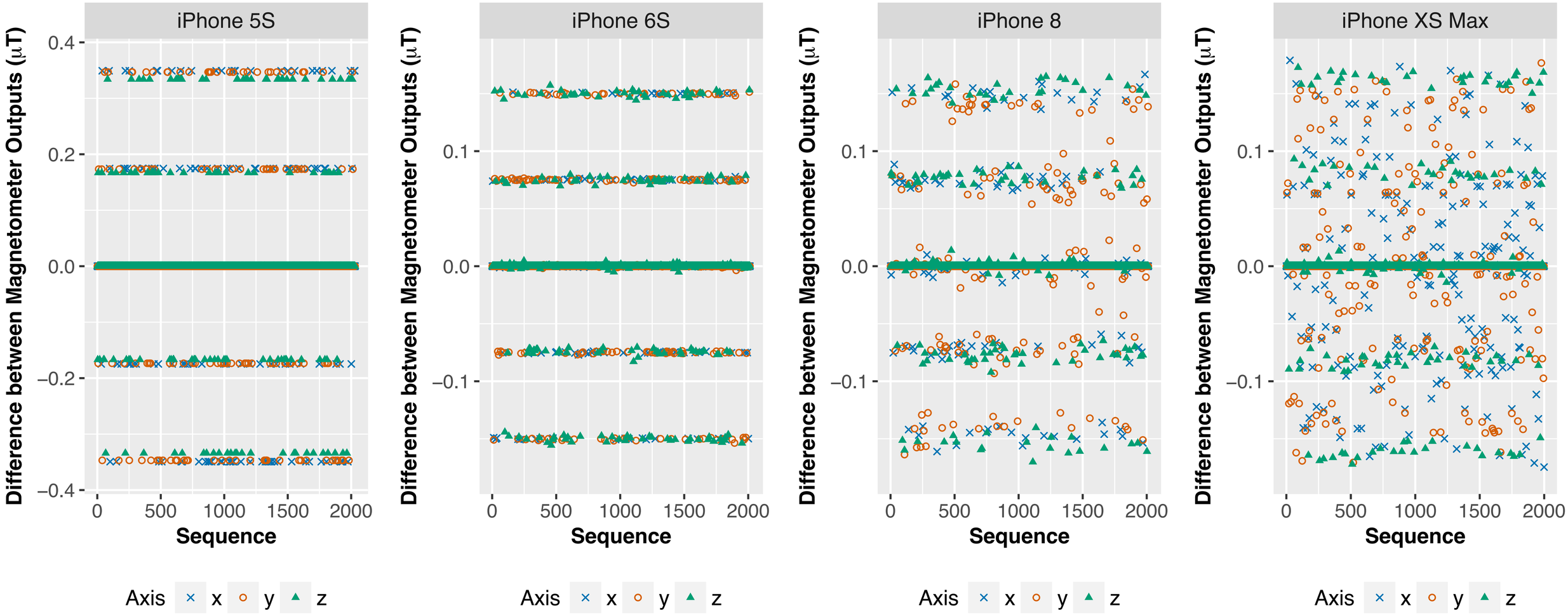
Generation of the Calibration Fingerprint




14:07
192.168.15.125
GyroID PoC
Timestamp:
Feb 6 2019 14:07:06
The GyroID for current device is:
14 -36 -11
11 33 22
-4 -25 18
Unit: 2^(-16) degrees per second per digit
Sampling Time: 0.925s
Processing Time: 0.153s
REGENERATE GYROID
BACK TO HOMEPAGE


14:07
192.168.15.125
GyroID PoC
Timestamp:
Feb 6 2019 14:07:06
The GyroID for current device is:
15 1 12
-20 39 44
3 -60 1
Unit: 2^(-16) degrees per second per digit
Sampling Time: 0.938s
Processing Time: 0.139s
REGENERATE GYROID
BACK TO HOMEPAGE

Calibration Fingerprint for Magnetometer



Definition of the SensorID

We refer to the collection of distinctive sensor calibration fingerprints as the ***SensorID***.

For iOS devices, the SensorID includes:

- GyroID (Gyroscope Fingerprint)
- MagID (Magnetometer Fingerprint)

For Google Pixel 2/3, the SensorID includes:

- AccID (Accelerometer Fingerprint)

Example

GyroID of an iPhone XS:

$$\text{GyroID} = \begin{bmatrix} 14 & -36 & -11 \\ 11 & 33 & 22 \\ -4 & -25 & 18 \end{bmatrix}$$

MagID of an iPhone XS:

$$\text{MagID} = \begin{bmatrix} 7 & 2 & -47 \\ -6 & 30 & 61 \\ 69 & 29 & 75 \end{bmatrix}$$

AccID of an Pixel 3:

$$\text{AccID} = \begin{bmatrix} 0.994785 & 0 & 0 \\ 0 & 1.004922 & 0 \\ 0 & 0 & 0.995183 \end{bmatrix}$$

SensorID Uniqueness Analysis

Fingerprint	GyroID	MagID		Fingerprintjs2																
# Devices	870	795		870																
Group Size	1	1	2	1	2	3	4	5	6	7	9	10	11	13	14	19	22	28	36	45
# Groups	870	775	10	391	43	22	12	2	4	2	1	1	2	2	1	1	1	1	1	1

SensorID Uniqueness Analysis

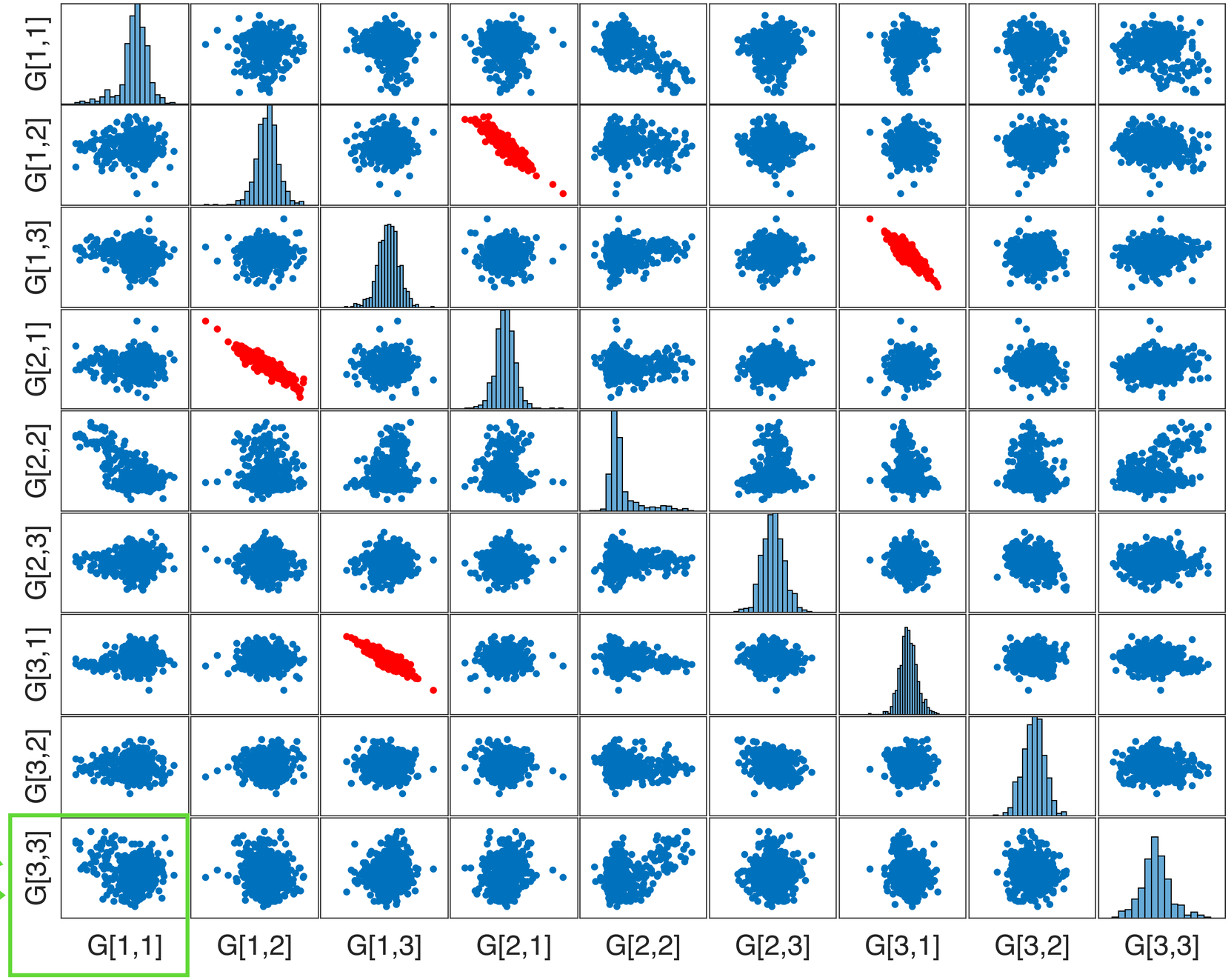
We collected motion sensor data from 870 iOS devices via crowdsourcing and estimated their SensorID.

We found there is a strong correlation between some values in the SensorID.

For the same device model, values in the SensorID follow normal distribution.

Fig: Scatter plot matrix of elements in the GyroID (693 iOS devices)

$$\text{GyroID} = \begin{bmatrix} G_{11} & G_{12} & G_{13} \\ G_{21} & G_{22} & G_{23} \\ G_{31} & G_{32} & G_{33} \end{bmatrix}$$



SensorID Uniqueness Analysis

For iPhone 6S, we estimate the GyroID has 42 bits of entropy and the MagID has 25 bits of entropy.

For 131M iPhone 6S devices, the chance of two iPhone 6S devices having the same SensorID is around 0.0058%.

Countermeasures

Option 1 - Adding noise:

$$\mathbf{O} = \mathbf{G}(\mathbf{A} + \epsilon) + \mathbf{B}$$

$$\epsilon_i \sim U(-0.5, 0.5)$$

Option 2 - Rounding the sensor outputs:

Manufacturers could round the factory calibrated sensor output to the nearest multiple of the nominal gain to prevent recovering the gain matrix.

Option 3 - Remove access to motion sensors

Results

- Calibration fingerprinting attack is easy to conduct by a website or an app in under 1 second, requires no special permissions, does not require user interaction.

- We collect motion sensor data from 870 iOS devices and show that our approach can generate a globally unique fingerprint (67 bits of entropy for the iPhone 6S).

- Apple adopted our suggestion of adding noise and removed sensor access by default in Mobile Safari on iOS 12.2 (CVE-2019-8541).

- Calibration fingerprinting attack is easy to conduct by a website or an app in under 1 second, requires no special permissions, does not require user interaction.
- We collect motion sensor data from 870 iOS devices and show that our approach can generate a globally unique identifier (67 bits of entropy for the iPhone 6S).
- Apple adopted our suggestion of adding noise and removed sensor access by default in Mobile Safari on iOS 12.2 (CVE-2019-8541).

For more details, visit:

https://sensorid.cl.cam.ac.uk

Stan Zhang

jz448@cl.cam.ac.uk