# A Data Hiding Approach for Sensitive Smartphone Data

Chu Luo, Angelos Fylakis, Juha Partala, Simon Klakegg,
Jorge Goncalves, Kaitai Liang, Tapio Seppänen, Vassilis Kostakos

Center for Ubiquitous Computing & Center for Machine Vision and Signal Analysis
University of Oulu & Aalto University, Finland
http://ubicomp.oulu.fi/

UNIVERSITY of OULU
OULUN YLIOPISTO

# Data Sources of Smartphone


# Sensitive Data

# Motivation: Data Sharing

# Data Needs Imperceptibility

# Approach: Data Hiding

- Hide a message in another
  - Different from cryptography
- Two important sub-disciplines:
  - Steganography
  - Watermarking

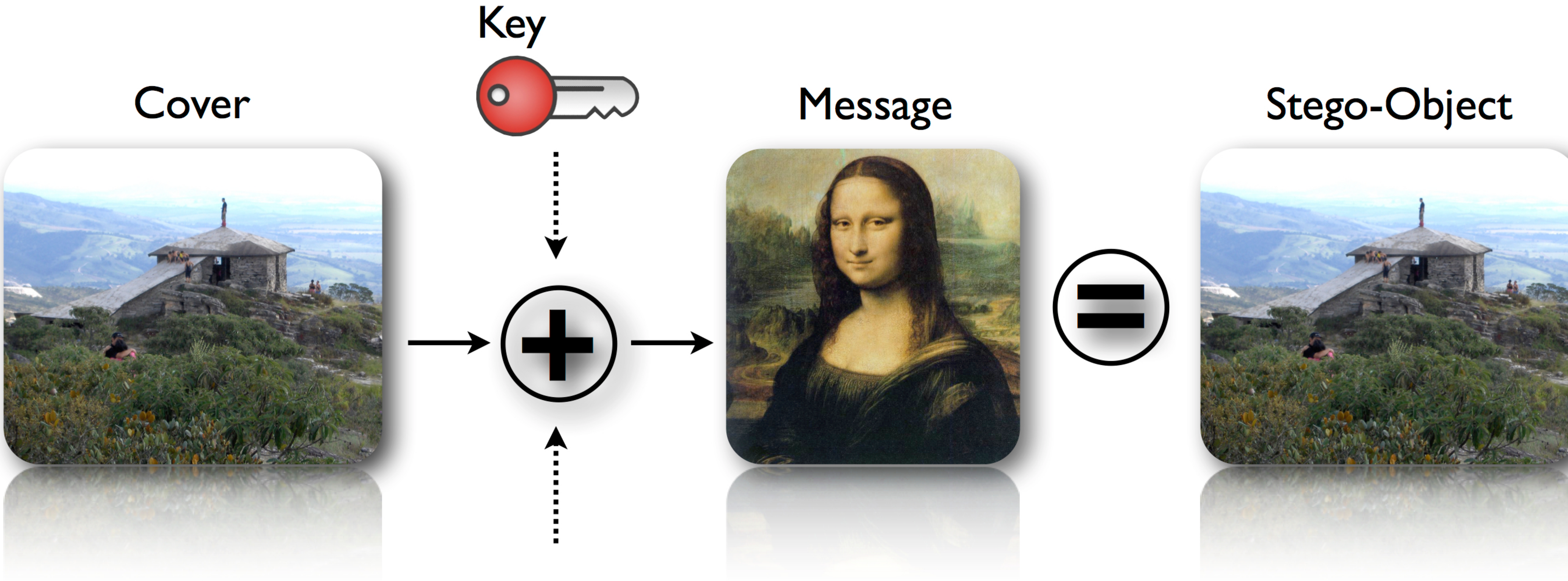
# Steganography

- An example:

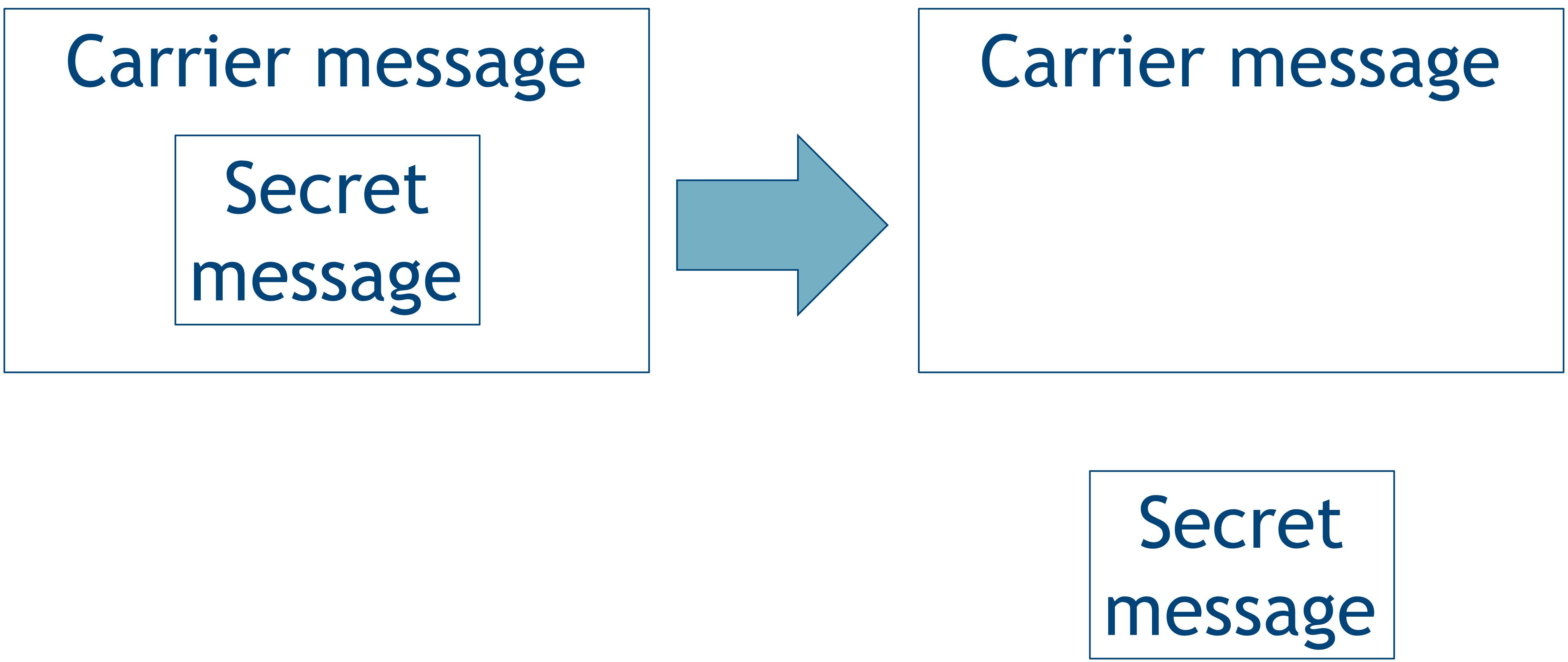
Unmarried Boys In China Overburden Moms Permanently.

**UBICOMP**

# Watermarking

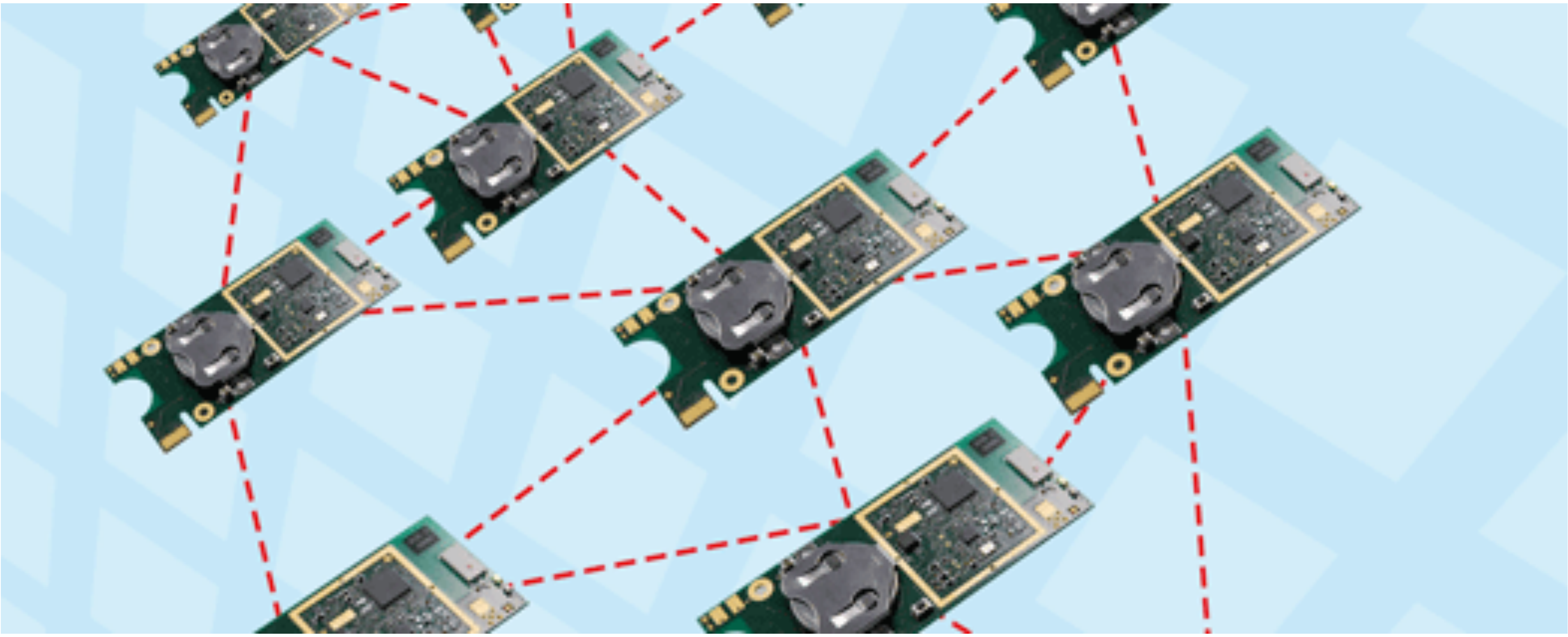


# Data Hiding Process



# Related Work

- Data hiding is in many areas

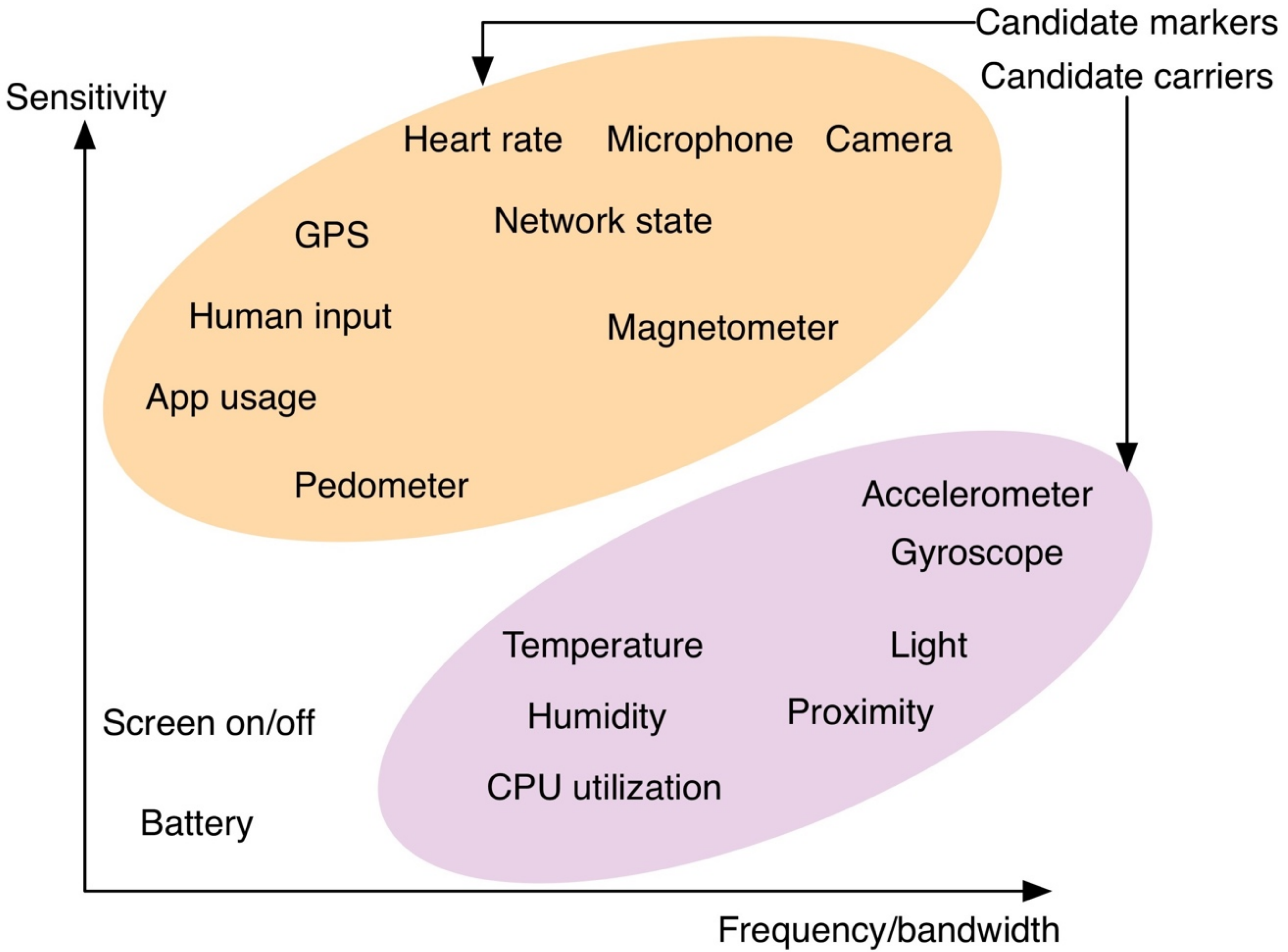


# Our Approach

- Data hiding for smartphone

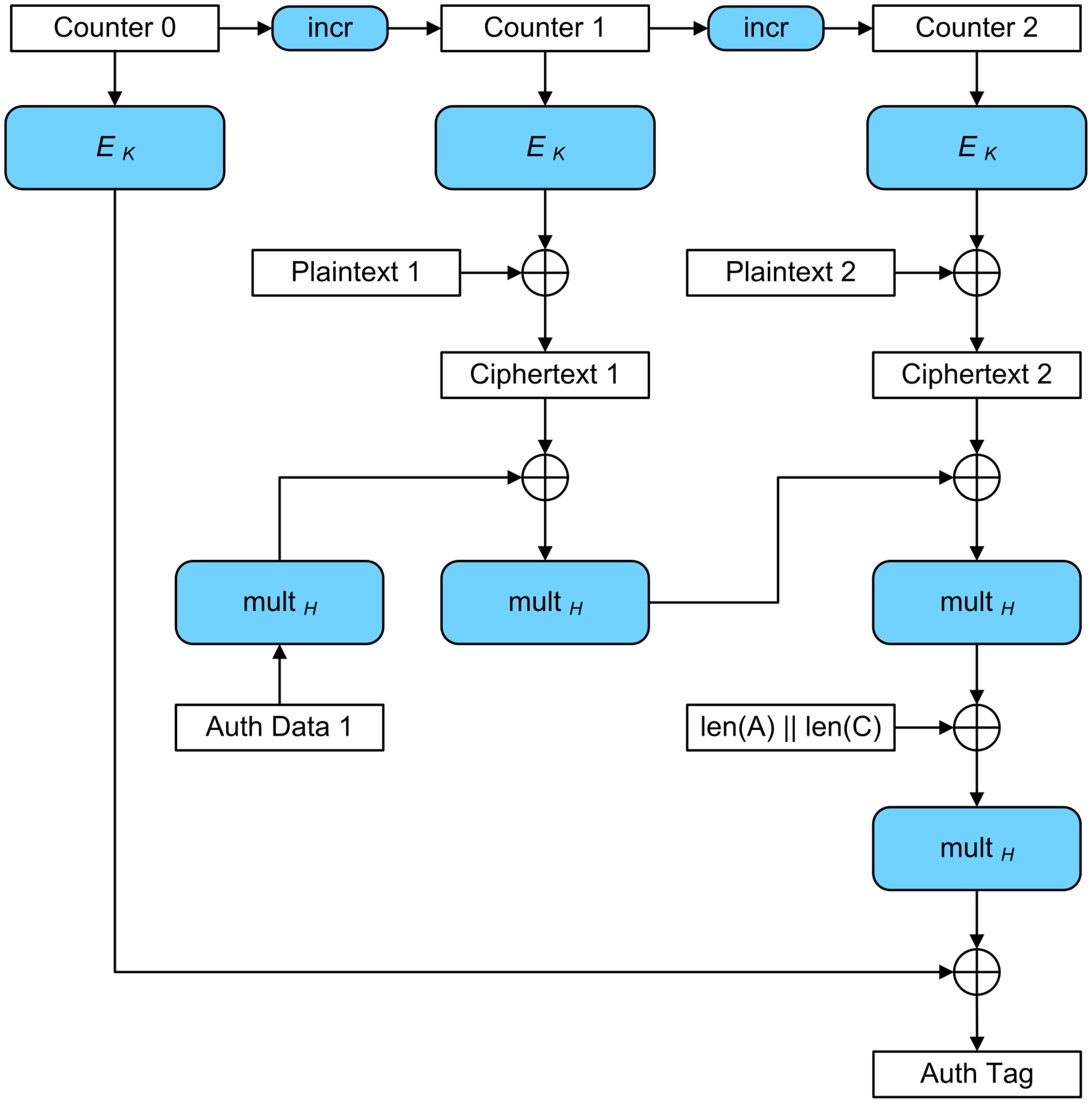
# Step 1: Find Carrier

- Classify data sources


Candidate markers
Candidate carriers
Sensitivity
Heart rate
Microphone
Camera
GPS
Network state
Human input
Magnetometer
App usage
Pedometer
Accelerometer
Gyroscope
Temperature
Light
Screen on/off
Humidity
Proximity
CPU utilization
Battery
Frequency/bandwidth

# Step 2: Encryption

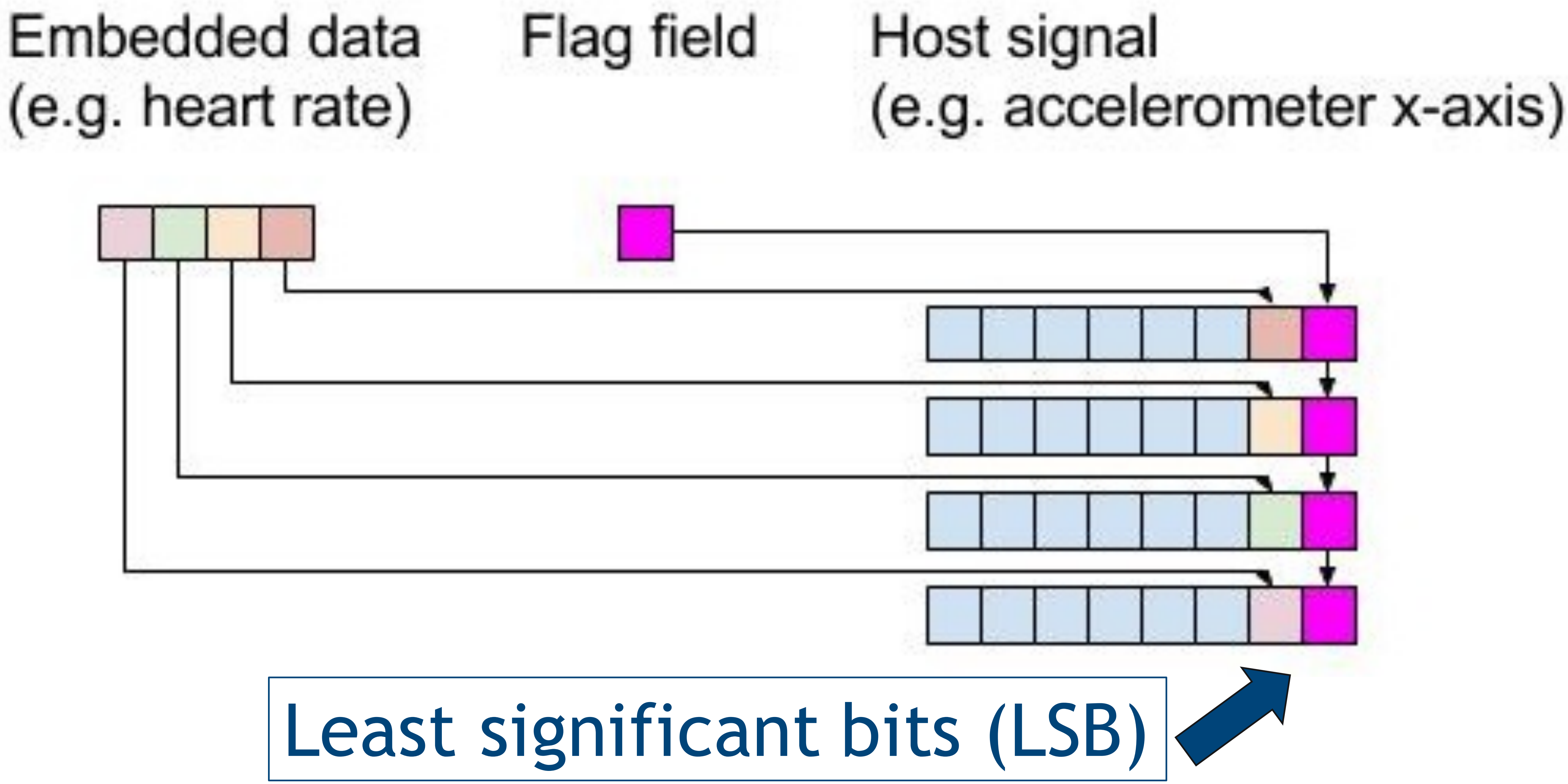
- Encrypt secret data
  - –Using AES/GCM



# AES/GCM

- Advanced Encryption Standard
- Galois/Counter Mode (GCM)
- Used in many protocols
- Using symmetric key
- Fast encryption/decryption and integrity check

# Step 3: Hiding



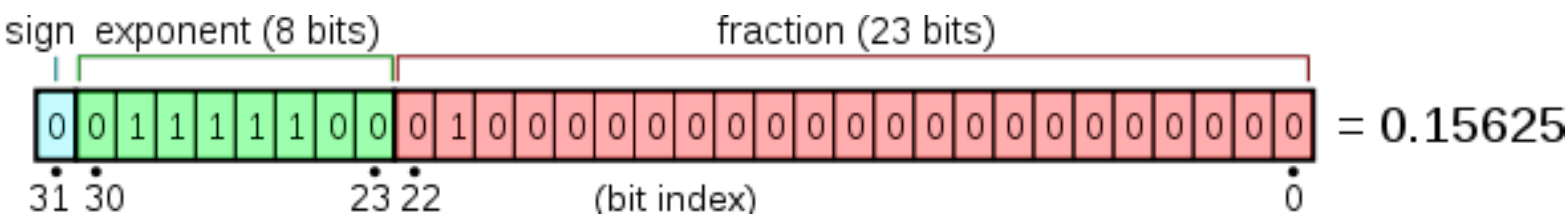
# Distortion in Carriers

- Depends on the data type and used bits
- For the integer/long type, using $n$ $(0<n<32)$ LSBs, error is $-(2^n-1)$ to $2^n-1$

# Distortion in Carriers

- For the double/floating type, more complex.
- A 32-bit floating representation:

$$f = (-1)^s \times c \times 2^q$$



# Distortion in Carriers

- Using $n$ ($0<n<23$) LSBs, error is also related to the exponent:

$$|E_{max}| = \sum_{i=1}^{n} 2^{i-24+q}$$

- Normally, $q$ is small, so error is small.

# Distortion in Carriers

- Example: gravity acceleration is $9.8 m/s^2$, so the approximation of float gives:

01000001000111001100110011001101 in 2

9.80000019073486328125 in 10

01000001000111001100110011001101 in 2

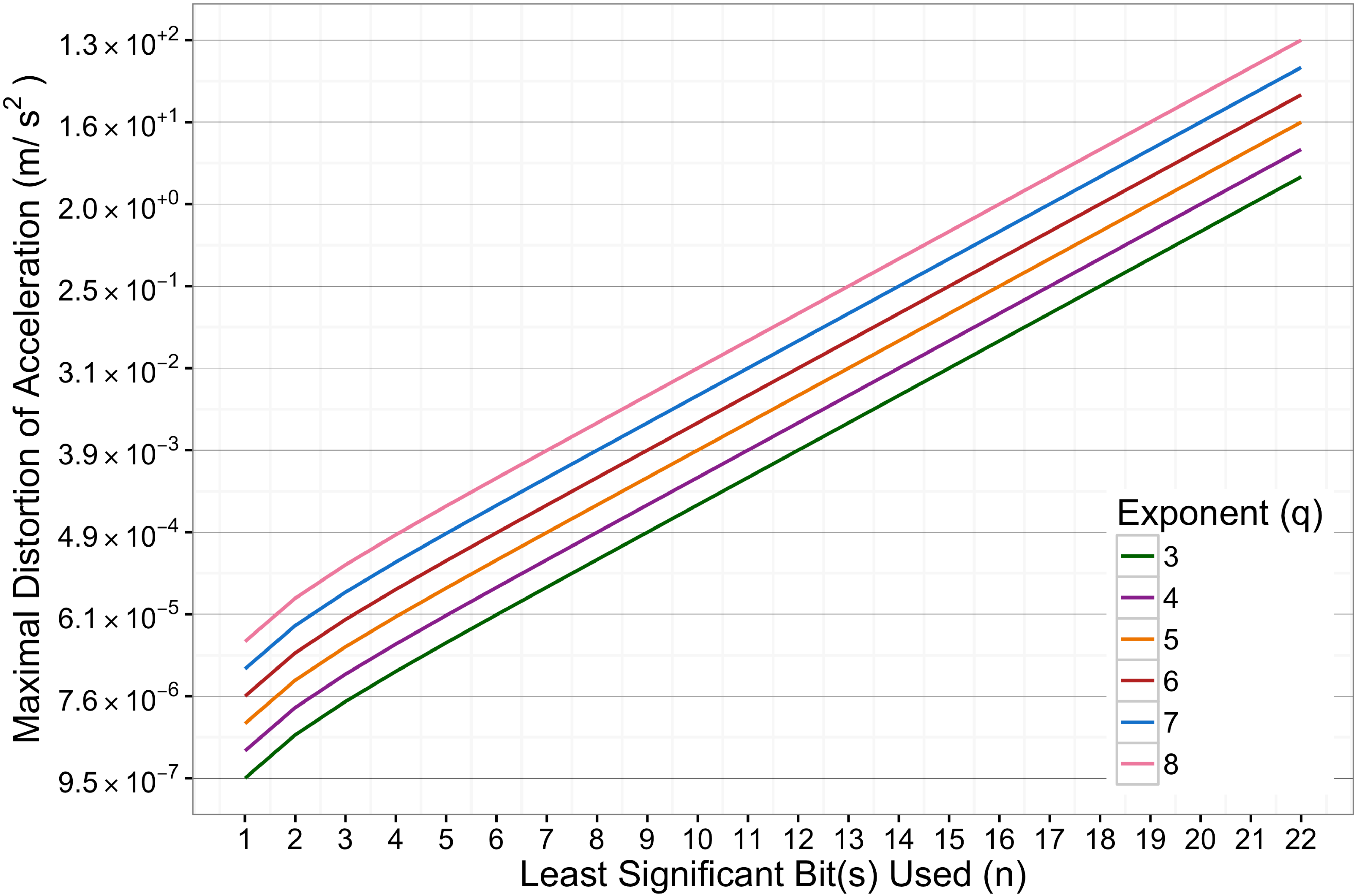
Flip the last bit in binary:

01000001000111001100110011001100 in 2

From 9.80000019073486328125 in 10

To 9.7999992370605546875 in 10

Difference 0.0000009536743 16 in 10



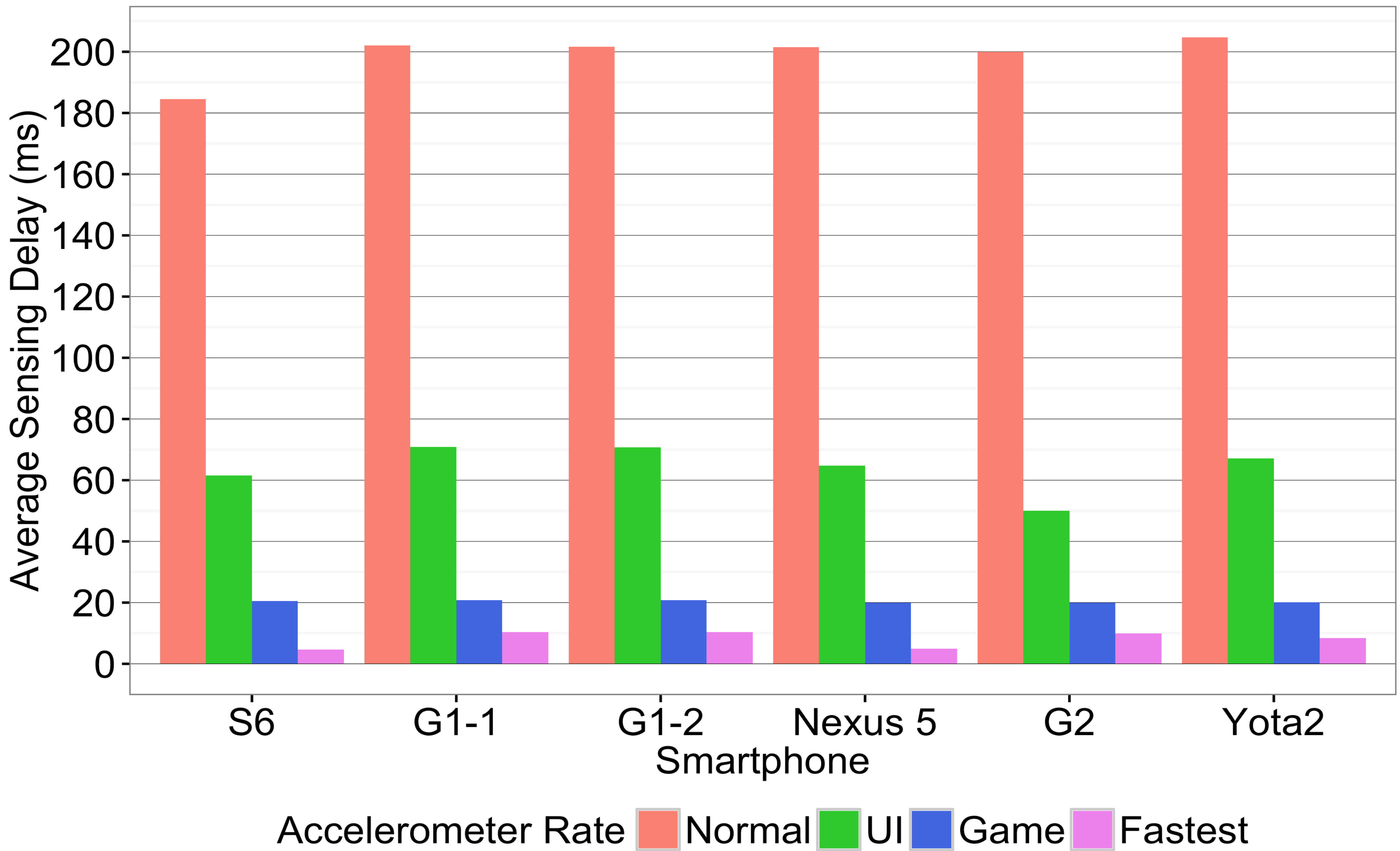
Maximal Distortion of Acceleration (m/ s^2 )
1.3 × 10^+2
1.6 × 10^+1
2.0 × 10^+0
2.5 × 10^−1
3.1 × 10^−2
3.9 × 10^−3
4.9 × 10^−4
6.1 × 10^−5
7.6 × 10^−6
9.5 × 10^−7
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
Least Significant Bit(s) Used (n)
Exponent (q)
3
4
5
6
7
8

# Performance on Real Phone

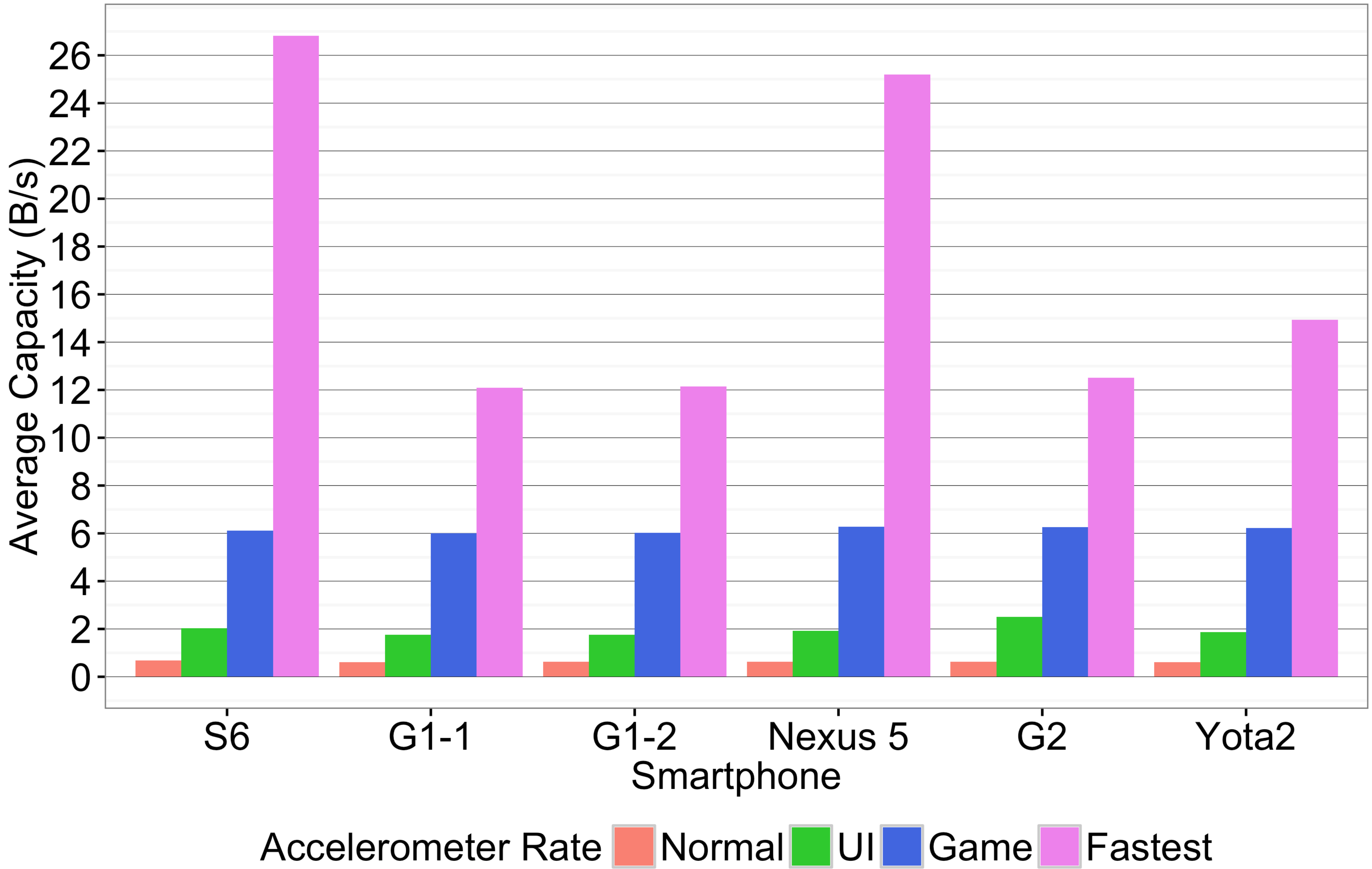
- We conducted experiments on Android phones to investigate:
- 1. Capacity
- 2. Difference between Phones
- 3. Computational Cost

| Experiment | Device | Marker | Carrier | LSBs |
|---|---|---|---|---|
| E1 | All | Magnetometer (3 x 32-bit float) (normal, UI, game, fastest) | Accelerometer (3 x 32-bit float) (normal, UI, game, fastest) | 2 |
| E2 | S6 | Magnetometer (3 x 32-bit float) (normal, UI, game, fastest) | Accelerometer (3 x 32-bit float) (normal, UI, game, fastest) | 3 |
| E3 | S6 | Heart rate sensor (32-bit int) (normal, UI, game, fastest) | Accelerometer (1 x 32-bit float) (normal, UI, game, fastest) | 2 |
| E4 | S6 | GPS (3 x 64-bit double) (0.1, 0.2, 1, 10 Hz) | Accelerometer (3 x 32-bit float) (normal, UI, game, fastest) | 2 |
| E5 | S6 | Human input (8-bit char) (1, 10, 100, 200 Hz) | Accelerometer (1 x 32-bit float) (normal, UI, game, fastest) | 2 |
| E6 | S6 | Device ID (16 x 8-bit char) | Accelerometer (1 x 32-bit float) (normal, UI, game, fastest) | 2 |

# Sensing Delay in Millisecond



# Capacity in Byte per Second

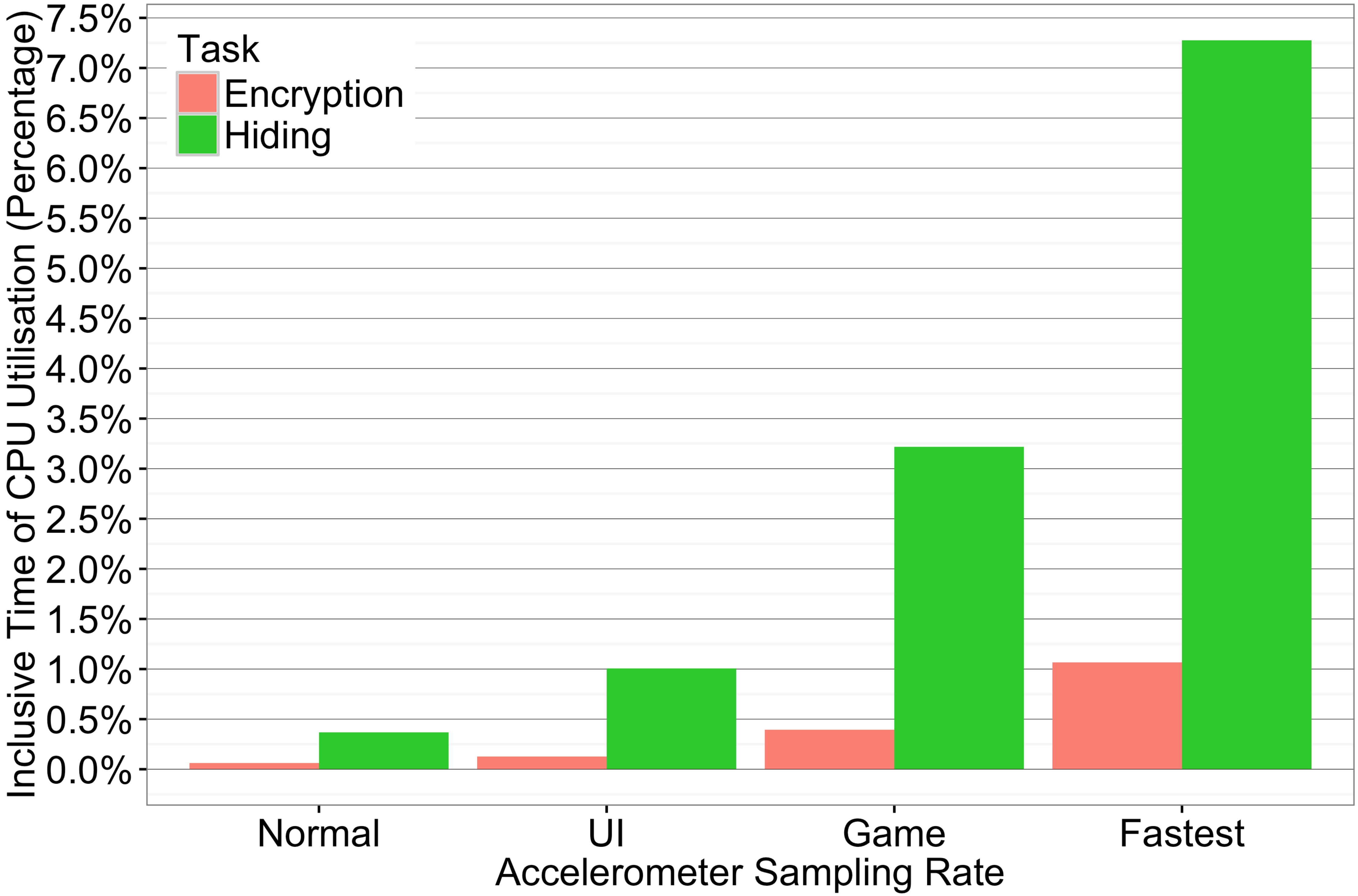


# Finding 1

- High capacity from high-frequency carriers, e.g., accelerometer:

  26 Bytes/s on 1 axis using 2LSBs

# CPU ratio: Per Task to Thread

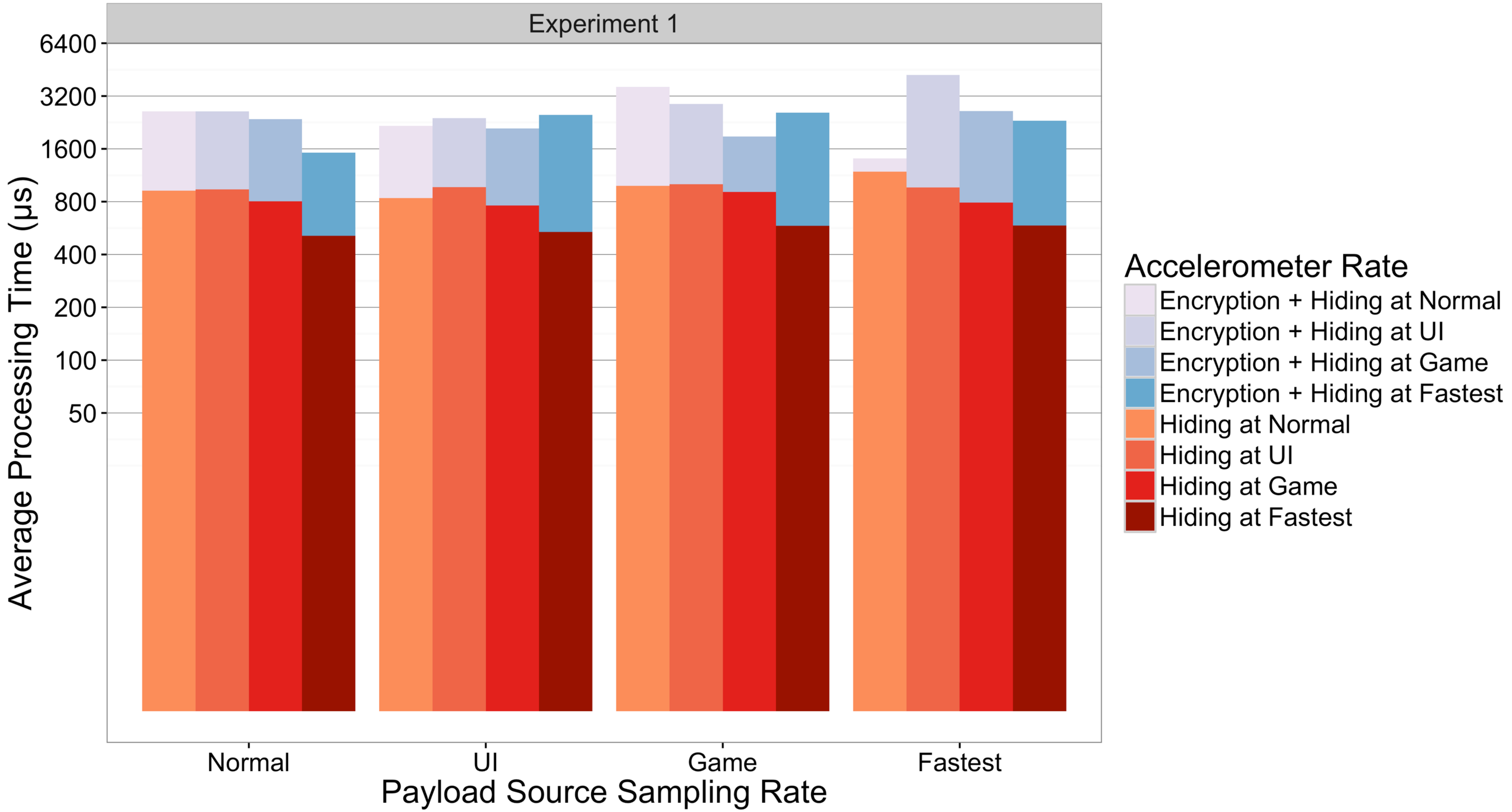


# Finding 2

- Low CPU Load on the thread:

  1% for normal speed, 8% for fastest

# Processing Time in Microsecond




UNIVERSITY of OULU
OULUN YLIOPISTO

# Finding 3

- Fast Computation.

  Hiding = 1ms

  Hiding + Encryption = 3ms

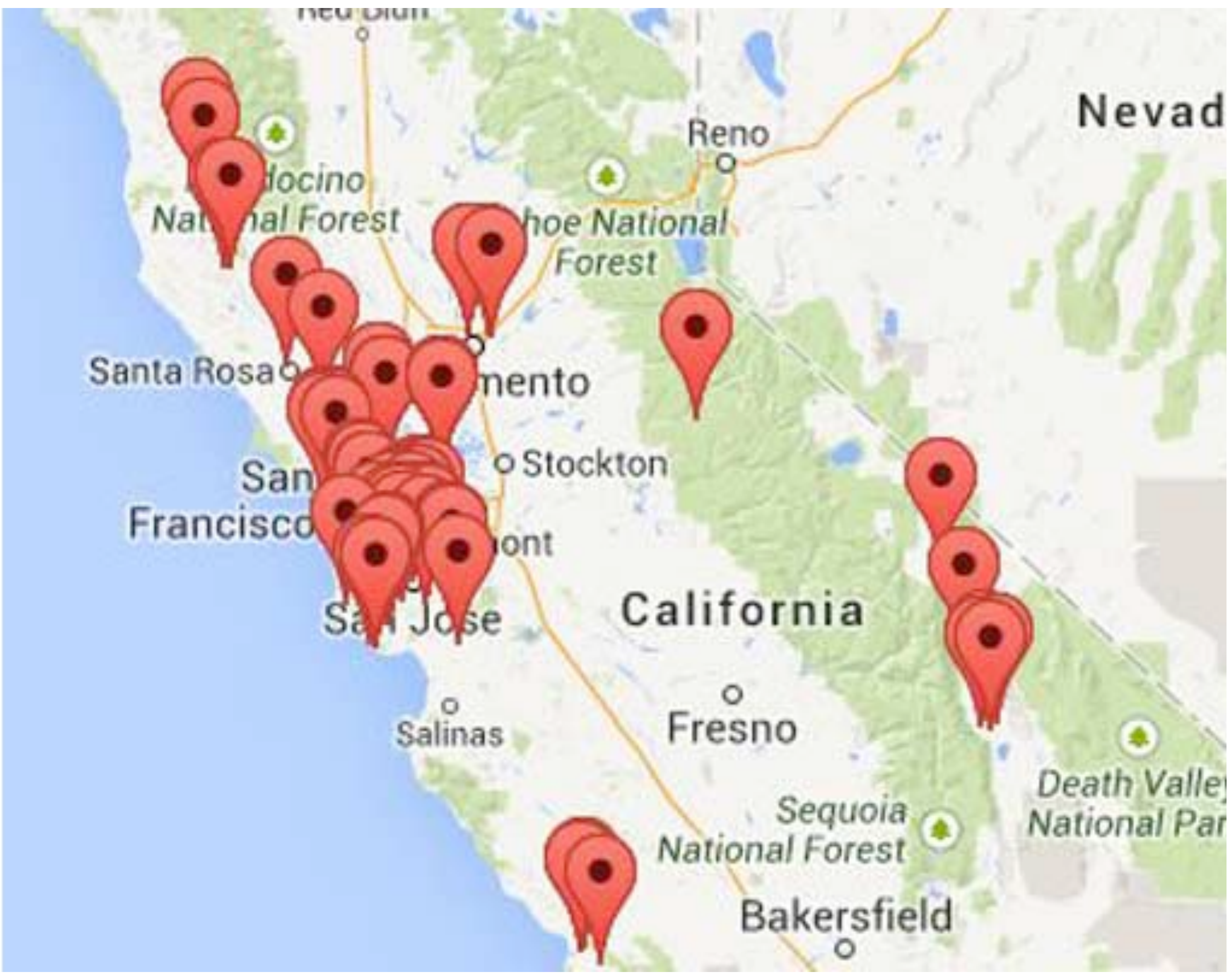
- Good for real-time apps.

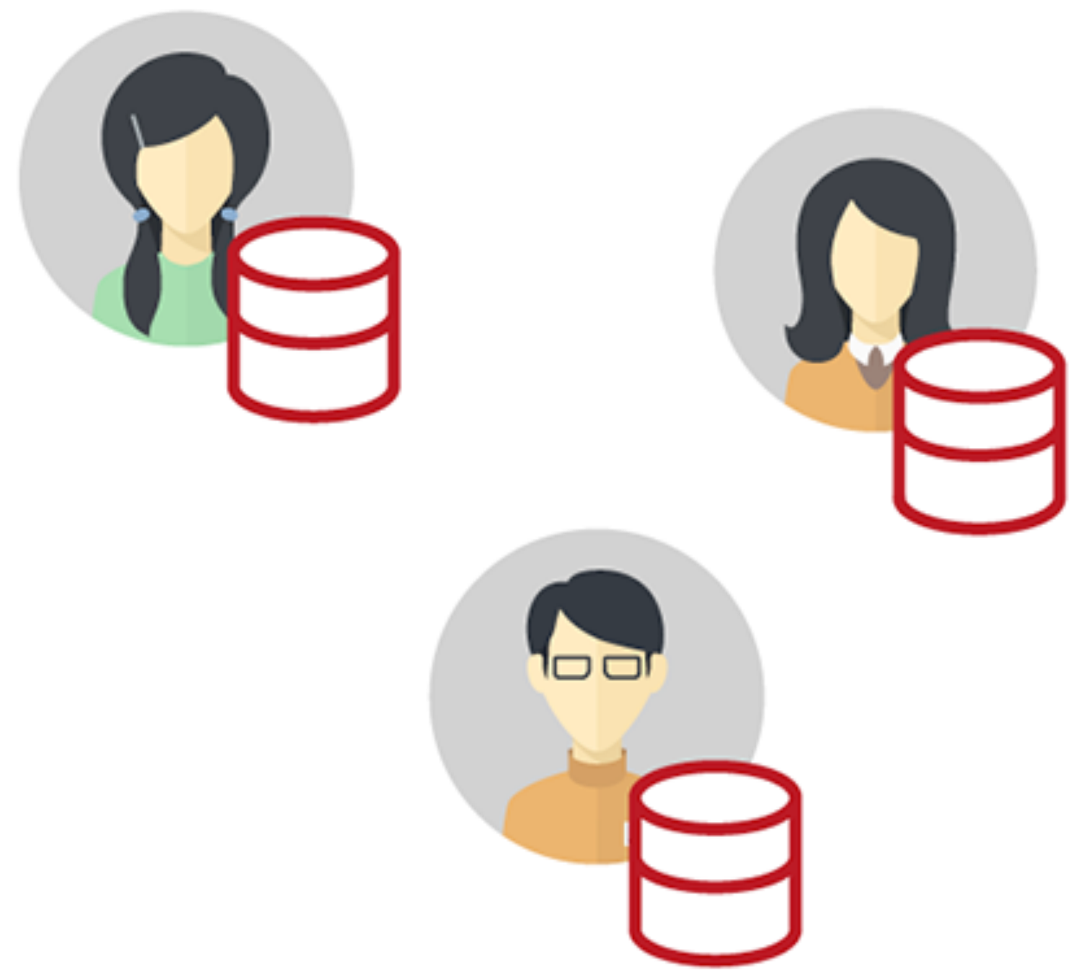
# Potential Applications

## Medical Apps: Higher-Level Privacy

# Potential Applications

## Crowdsensing: Authentication



# Take-away Points

- We propose a data hiding approach for smartphone:
  - –Imperceptibility
  - –High Capacity & Low Distortion
  - –Simple and Fast

# Thank you! Questions?

# A Data Hiding Approach for Sensitive Smartphone Data

Chu Luo, Angelos Fylakis, Juha Partala, Simon Klakegg,
Jorge Goncalves, Kaitai Liang, Tapio Seppänen, Vassilis Kostakos

Center for Ubiquitous Computing & Center for Machine Vision and Signal Analysis
University of Oulu & Aalto University, Finland
http://ubicomp.oulu.fi/