Cross Body Signal Pairing ($CBSP_{CR}$): A Key Generation Protocol for Pairing Wearable Devices with Cardiac and Respiratory Sensors

Jafar Pourbemany (Cleveland State University)

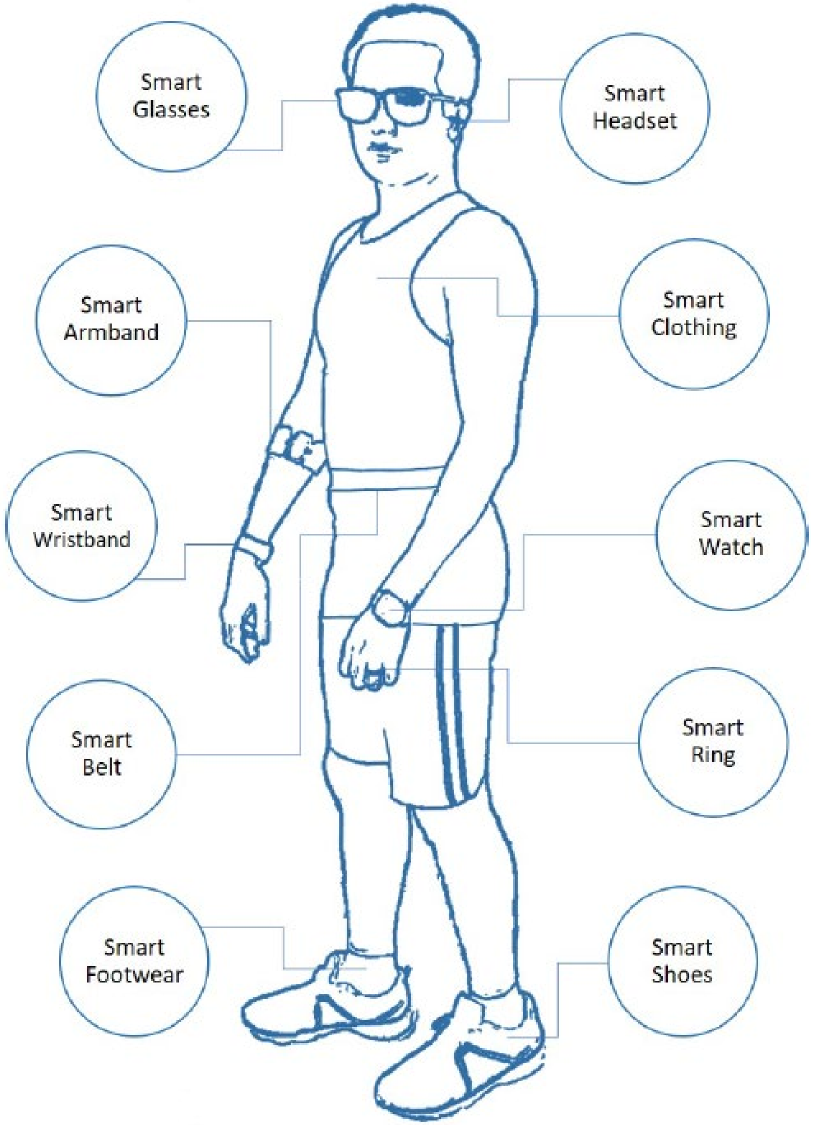
Co-Author:

Ye Zhu (Cleveland State University)

ACSAC 2023

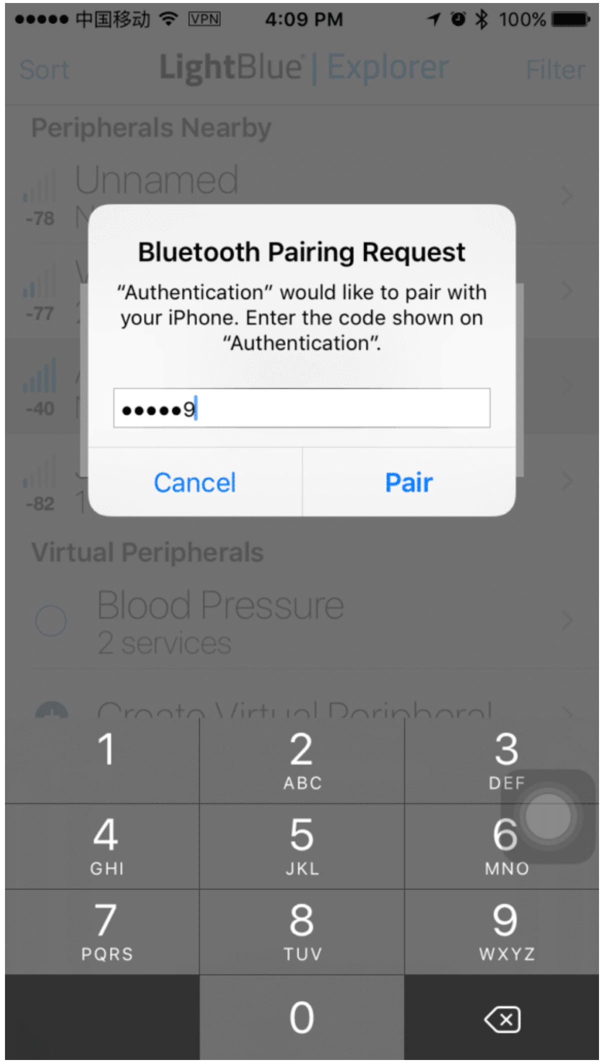
Pairing

- Why pairing?
  - To generate a common key to secure the communication



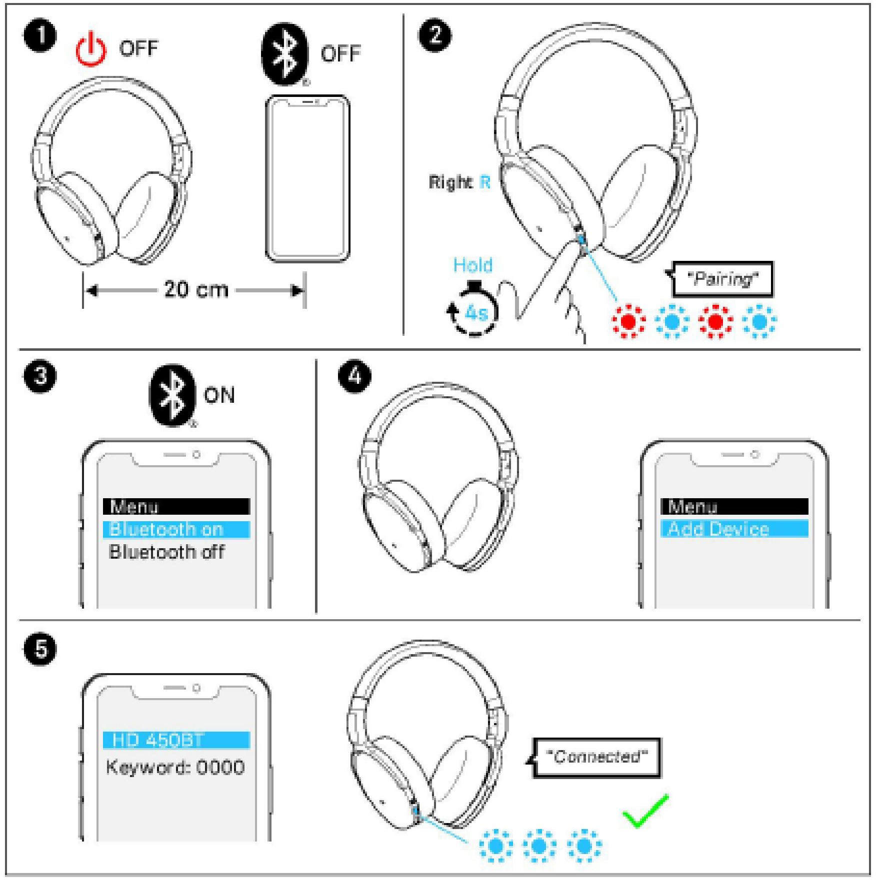
Traditional Approaches

- Traditional pairing approach
  - Bluetooth pairing (using a PIN code or password)



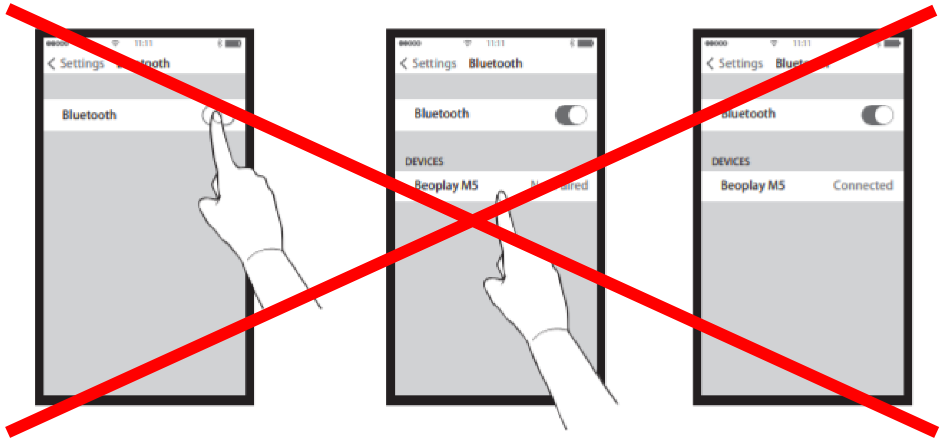
Traditional Approaches Drawback

- It needs user interaction.
  - Pairing is hard when you have lots of devices



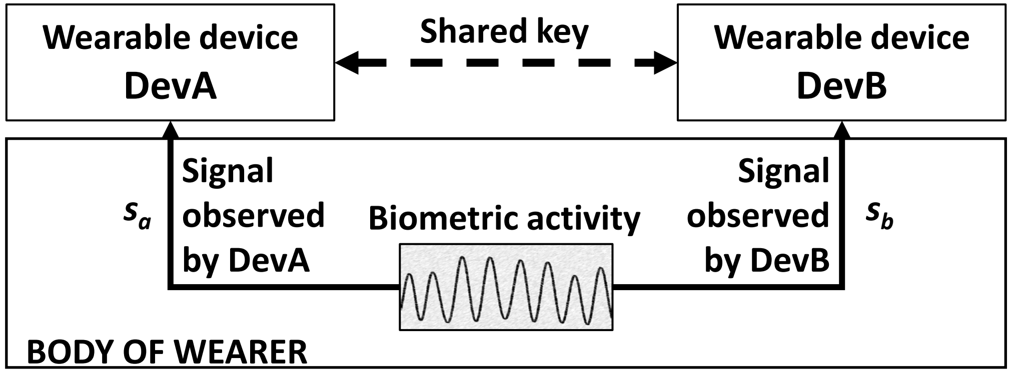
Traditional Approaches Drawback

- Most wearable devices do not have a user interface
  - e.g., keyboard and display



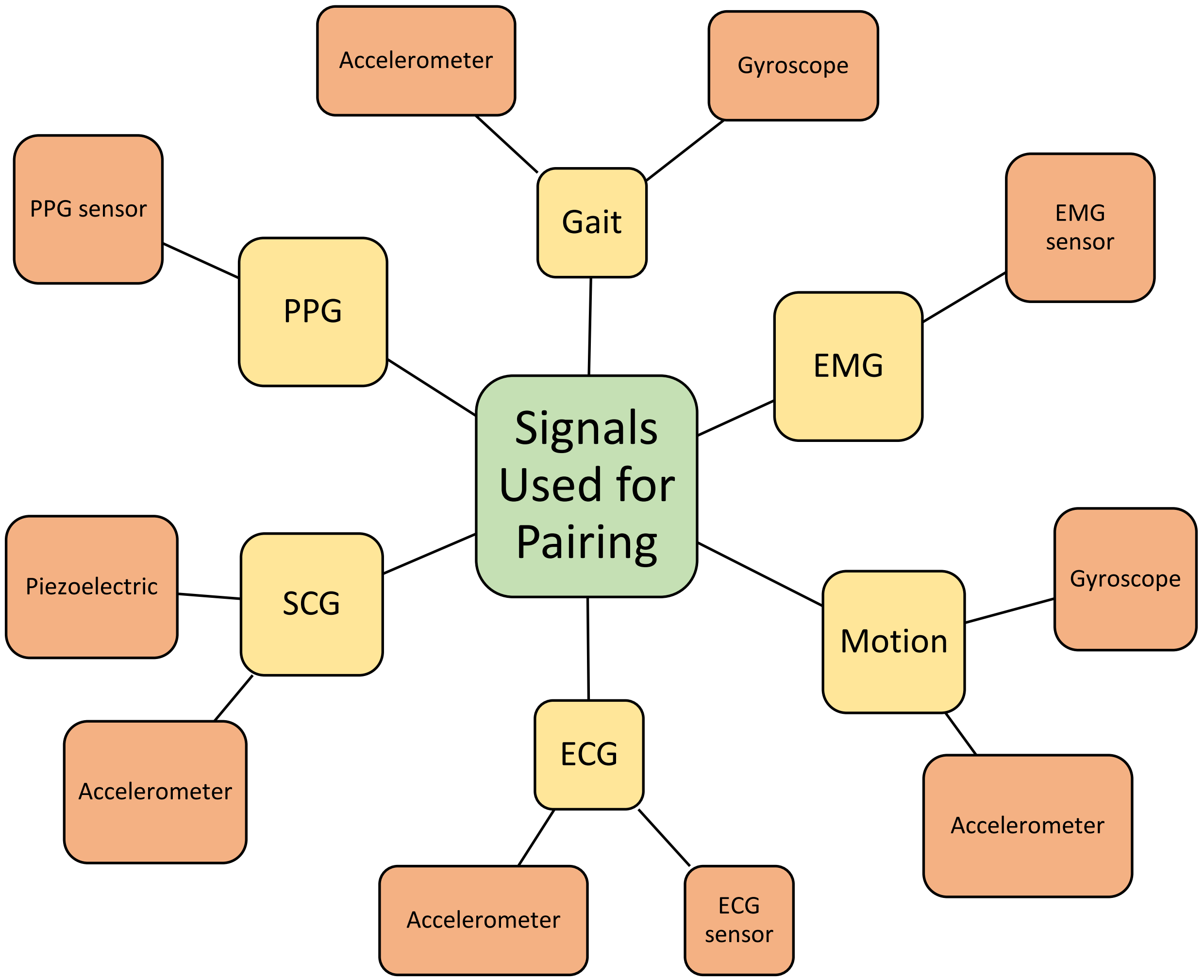
Pairing Based on Body Signals

- **Input**: observation of common dynamics
- **Output**: shared symmetric key
- **Example**: two wearables detecting user's heart beats



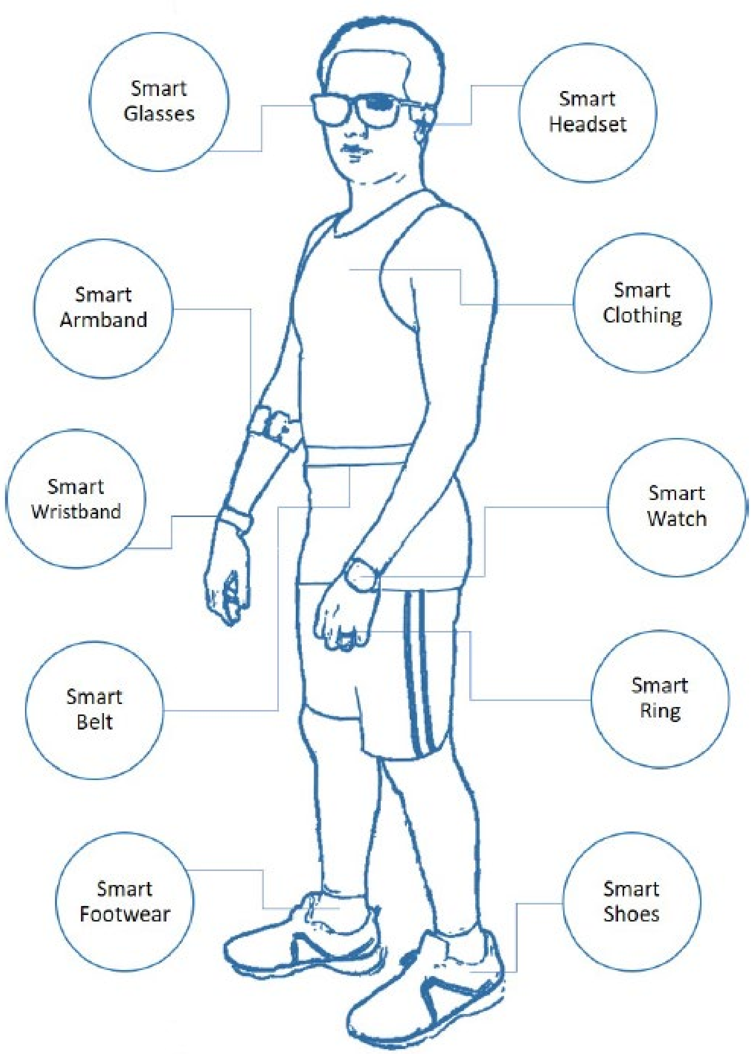
Prior Works

- Focus on the same type of sensors and signals



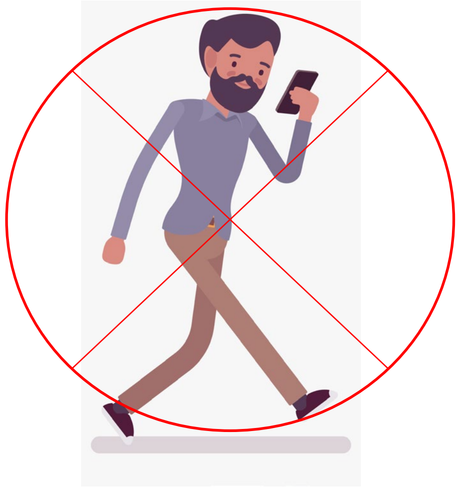
Motivating Question

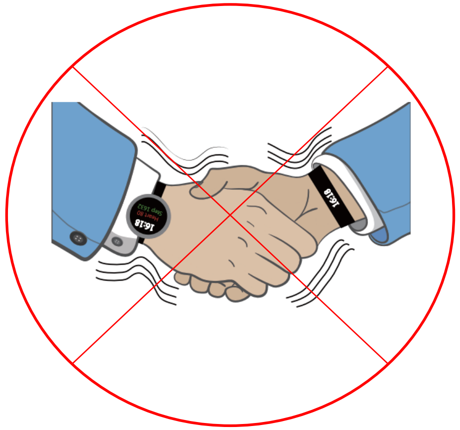
- How to pair smart wearables equipped with different sensors sensing different body signals?



Cross Body Signal Pairing

- Pairing based on the heartbeat and breathing patterns
  - Users do not need to do some special actions (e.g., walking or shaking)

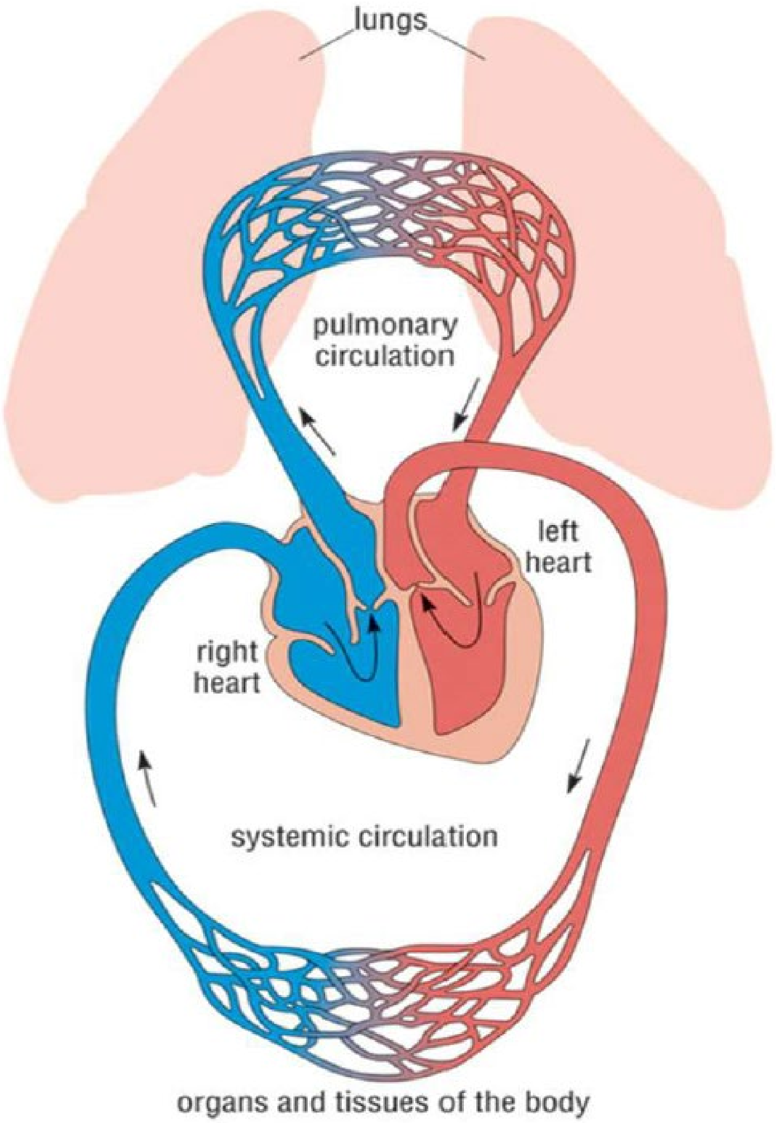




- Use wearables equipped with different types of sensors

Background

- The physiological connection between heart and lungs

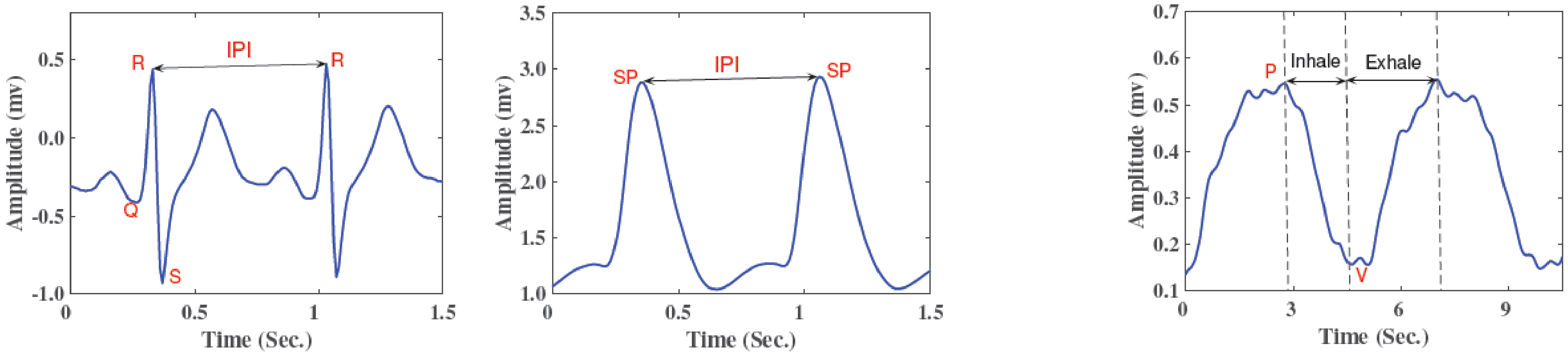


Circulation systems connecting heart and lungs [1]

[1] Anatomy and physiology of the heart. https://www.open.edu/

Background

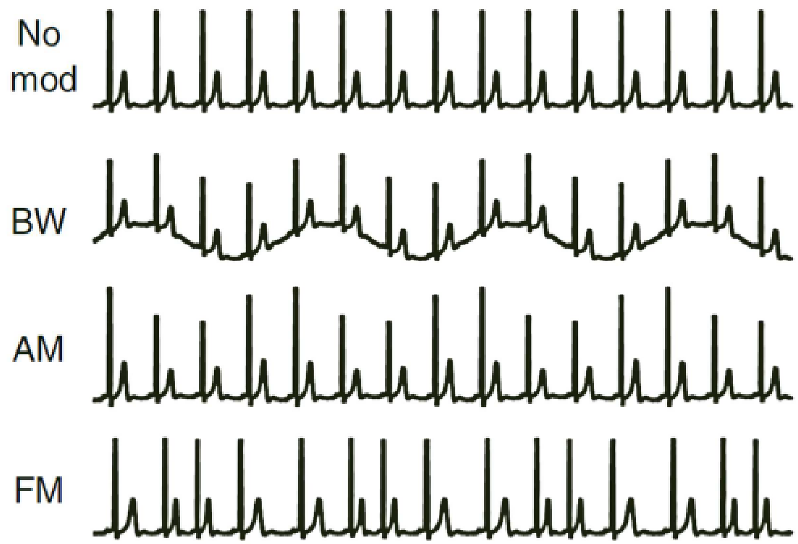
- The typical respiratory, ECG, and PPG signals



(a) ECG (b) PPG (c) Respiratory Signal

Background

- Relationship between cardiac and respiratory signals



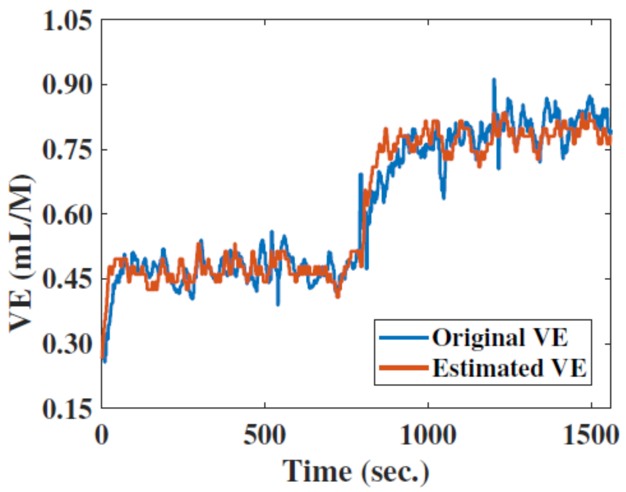
Idealized respiratory modulations of the ECG [2]

Equation	
Linear	$\overline{VE} = a + b_1 HR$
Quadratic	$\overline{VE} = a + b_1 HR + b_2 HR^2$
Exponential	$\overline{VE} = e^{a + b_1 HR}$

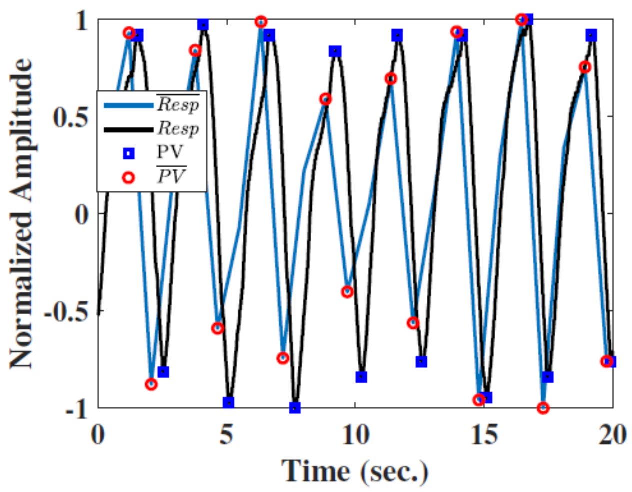
Models used for respiration estimation

[2] Peter H. Charlton, Timothy Bonnici, Lionel Tarassenko, David A. Clifton, Richard Beale, and Peter J. Watkinson. 2016. An assessment of algorithms to estimate respiratory rate from the electrocardiogram and photoplethysmogram. Physiological Measurement 37, 4 (2016), 610–626.

Feasibility Analysis



Actual VE signal and the estimated-VE signal in moderate and high-intensity exercises



Actual respiratory signal and the respiratory signal extracted from cardiac signal in resting phase

RMSPE	Rest	Moderate intensity	High intensity
Linear	0.1601	0.0707	0.0692
Quadratic	0.1650	0.0697	0.0677
Exponential	0.1663	0.0686	0.0656

RMSPE of equations in different intensity levels

Activity	Rest	Moderate intensity	High intensity
RMSPE	0.0522	0.0754	0.1593

RMSPE of respiratory signal extraction

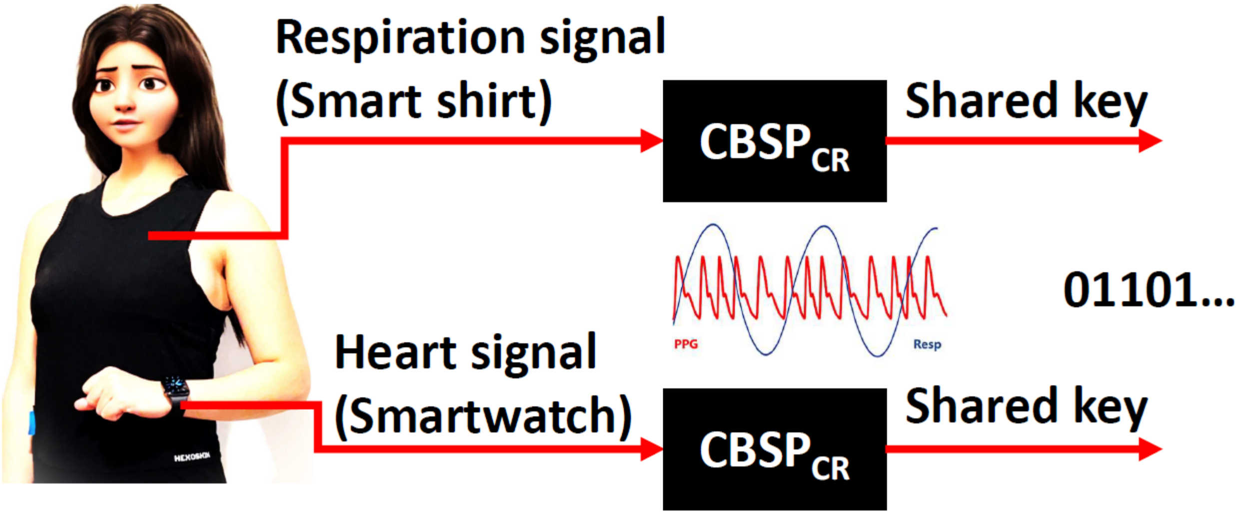
Challenges

1. Differing signals characteristics
   - Measuring unit, amplitude, frequency
   - Noise measurement

2. Activity intensity dependency
   - Varying RMSPE based on activity

Cross Body Signal Pairing (CBSP) Protocol

- **Goal:** Use cardiac and breathing patterns to generate shared keys in wearables equipped with different types of sensors by proving that devices are attached to the same body
- We use wearables equipped with ECG/PPG and/or RIP sensors

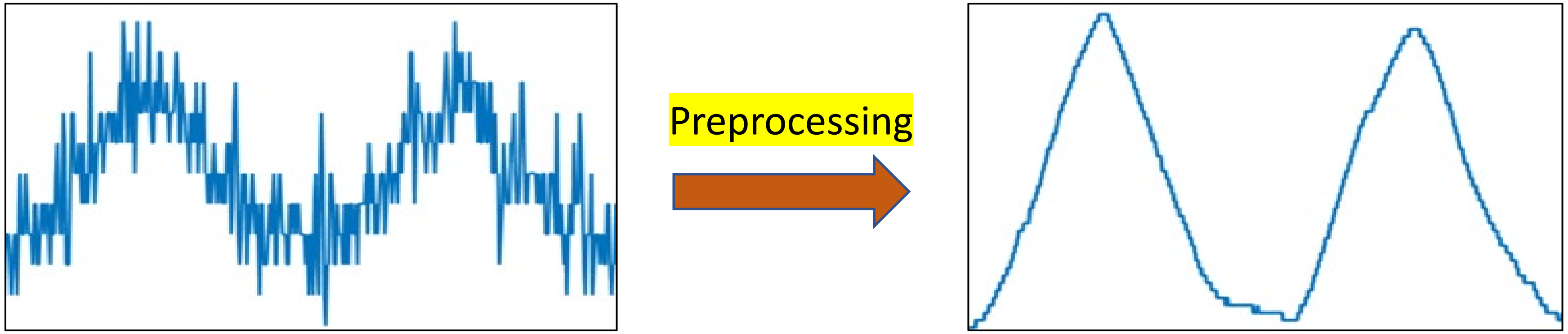


Cross Body Signal Pairing (CBSP) Protocol

- Threat Model
  - Third party's data
  - Historical data of user
  - Remote observation

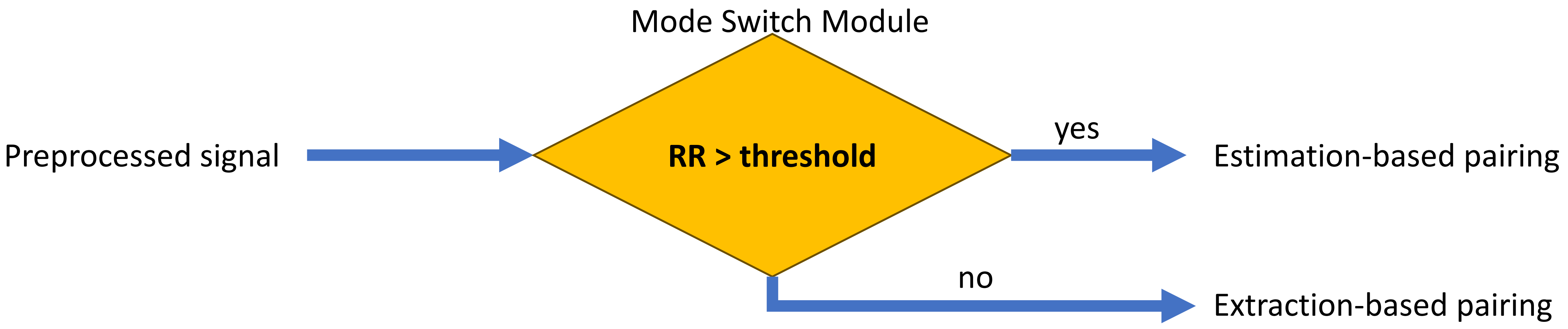
How do we address the challenges?

- Different signal characteristics
  - Preprocessing
    - Filtering
      - Cardiac Sensors: bandpass filter with cutoff frequencies of 0.5 Hz and 3 Hz
      - RIP Sensor: bandpass filter with cutoff frequencies of 0.1Hz and 1Hz
    - Normalization



How do we address the challenges?

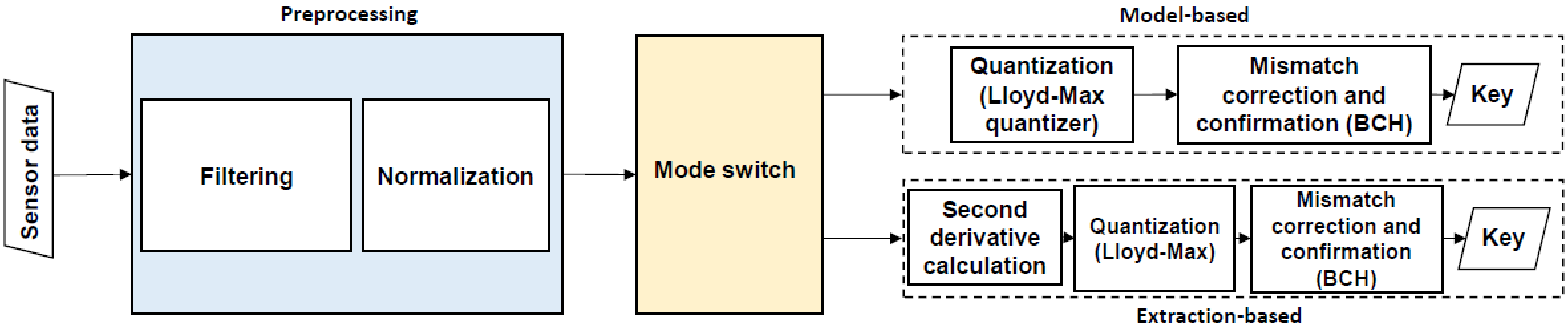
- Mode switching
  - Switching between estimation and extraction mode
    - Criterion: respiration rate
    - The respiration rate is calculated using IPIs
    - Switching buffer and threshold



Shared Key Generation

- How to generate 100% same bit string on both devices
  - Optimal quantization
    - Lloyd-Max
  - Effective error correction
    - BCH

CBSP Architecture



Evaluation

- Performance metrics
  - Key generation rate (KGR)
  - Entropy
  - Bit agreement rate
- Impact of various parameters
  - Quantization (number of bits per sample)
  - Error correction (BCH parameters)
  - Switching mode
  - Activity intensity level

Evaluation

- Experiment setup
  - Smart shirt (Hexoskin) and smartwatch (Samsung Galaxy Watch 3)
  - IRB approval
  - 30 participants (16 males and 14 females aged between 18 and 56)
  - Incremental exercises on stationary bike
    - Standardized in cardiorespiratory research
  - Record a video of the participant during the experiment for remote attack

Evaluation

- Result
  - Devices attached to the same body can generate a secure 128-bit key every 80 seconds.

Pairing mode	Extraction-based		Model-based	
Intensity level	KGR (key/sec)	Entropy	KGR (key/sec)	Entropy
Resting	0.0077	0.99	0.0052	0.97
Moderate intensity	0.0065	0.99	0.0113	0.99
High intensity	0.0046	0.98	0.0125	0.99

The results of CBSP in extraction- and model-based pairing

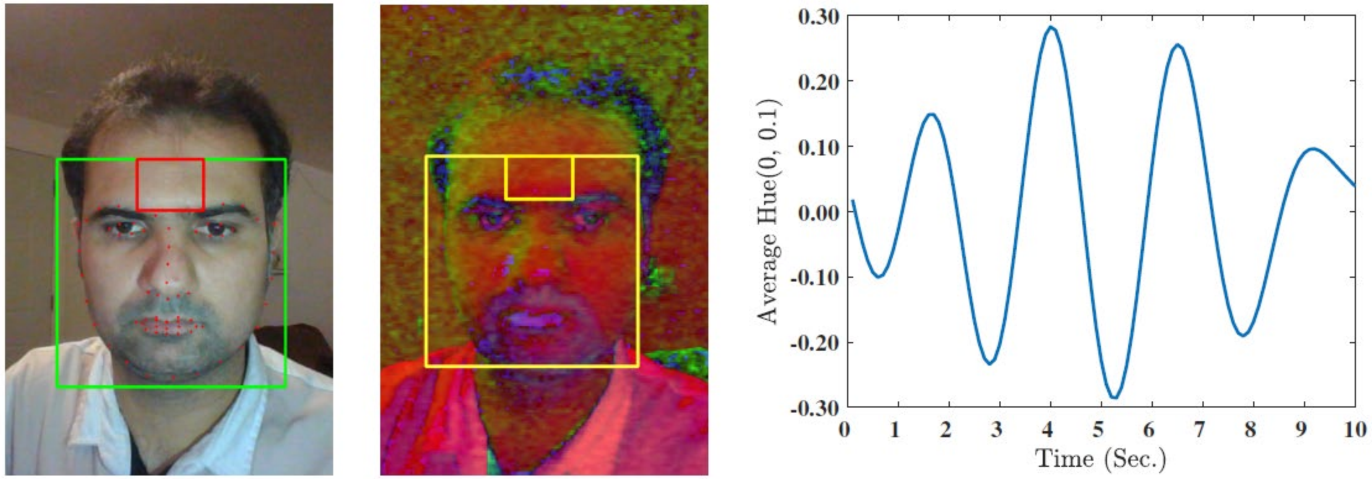
  - CBSP is robust against different types of attacks (low similarity of 68.1%)

Resistance to Attacks

- Impersonation attack with a third-party’s data
  - The attacker cannot achieve more than 68.1% match
- Impersonation attack with historical data
  - At most 73% match

Resistance to Attacks

- Video attack
  - Respiration extraction using Hue channel



- The attacker cannot achieve more than 78.6% match

Conclusion

- CBSP enables wearables pairing using cardiac and breathing signal
- CBSP demonstrates robustness against different types of attacks
- CBSP can generate a secure 128-bit key every 80 seconds

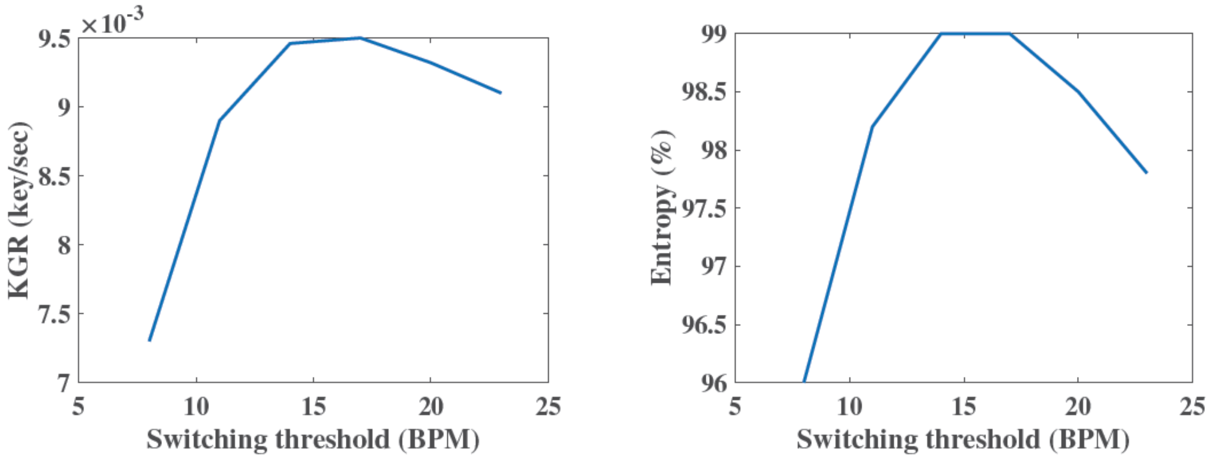
Thank You!

Jafar Pourbemany

pourbemany@ieee.org

Impact of parameters

- Switching threshold



- Error correction ratio