Published: 04 March 2025



RESEARCH-ARTICLE

# MagKey: Empowering Wearables with Ballistocardiography-based Key Generation through Magnetic Field Vibration Sensing

JUNYING HUANG, Zhejiang University, Hangzhou, Zhejiang, China

XIUZHEN GUO, Zhejiang University, Hangzhou, Zhejiang, China

CHAOJIE GU, Zhejiang University, Hangzhou, Zhejiang, China

YUCHEN MIAO, Zhejiang University, Hangzhou, Zhejiang, China

SHIBO HE, Zhejiang University, Hangzhou, Zhejiang, China

YUANCHAO SHU, Zhejiang University, Hangzhou, Zhejiang, China

View all




https://doi.org/10.1145/3712272
EISSN: 2474-9567

# MagKey: Empowering Wearables with Ballistocardiography-based Key Generation through Magnetic Field Vibration Sensing

JUNYING HUANG, Zhejiang University, China
XIUZHEN GUO, Zhejiang University, China
CHAOJIE GU, Zhejiang University, China
YUCHEN MIAO, Zhejiang University, China
SHIBO HE, Zhejiang University, China
YUANCHAO SHU, Zhejiang University, China
JIMING CHEN, Zhejiang University, China

Symmetric key generation based on biometrics has emerged as a promising solution for wearables pairing. Among various biometrics, heartbeats offer significant potential owing to their inherent randomness and spontaneity. Ballistocardiography (BCG), in particular, stands out for its accessibility and inclusivity, as it measures the body's recoil forces in response to cardiac blood ejection into the vasculature. However, traditional approaches to BCG suffer from challenges in sensing on wearables and limited key generation rates. To this end, this paper presents MagKey, a system that enables wearables with BCG-based key generation. MagKey overcomes the difficulties in effective BCG sensing by translating skin vibration caused by recoil forces into magnetic field vibration (MFV). Moreover, MagKey demonstrates that the peak-to-peak trend (PPT) of MFV signals can reliably extract keys, and thus improve the key generation rate. To mitigate the impact of noise and motion artifacts on key generation, MagKey employs analog filters and a peak screening method for signal processing. We implement MagKey on a one-layer flexible printed circuit (FPC) and a two-layer printed circuit board (PCB). Extensive experiments show the usability and effectiveness of MagKey. Furthermore, our security analyses illustrate the scheme's resilience against potential attacks.

CCS Concepts: • **Human-centered computing → Ubiquitous and mobile computing systems and tools**; • **Security and privacy → Authentication**; • **Computer systems organization → Embedded and cyber-physical systems**.

Additional Key Words and Phrases: Key generation, GMR sensor, magnetic field vibration, heartbeat signal.

**ACM Reference Format:**
Junying Huang, Xiuzhen Guo, Chaojie Gu, Yuchen Miao, Shibo He, Yuanchao Shu, and Jiming Chen. 2025. MagKey: Empowering Wearables with Ballistocardiography-based Key Generation through Magnetic Field Vibration Sensing. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 9, 1, Article 6 (March 2025), 28 pages. https://doi.org/10.1145/3712272

## 1 INTRODUCTION

The ever-developing Internet of Things (IoT) brings the prosperity of wearables and actuation applications [1, 2]. The global wearable electronics market size was valued at $81.40 billion in 2020, and is expected to reach $459.58

Authors' addresses: Junying Huang, Zhejiang University, Hangzhou, China, hjy23@zju.edu.cn; Xiuzhen Guo, Zhejiang University, Hangzhou, China, guoxz@zju.edu.cn; Chaojie Gu, Zhejiang University, Hangzhou, China, gucj@zju.edu.cn; Yuchen Miao, Zhejiang University, Hangzhou, China, miaoyc@zju.edu.cn; Shibo He, Zhejiang University, Hangzhou, China, s18he@zju.edu.cn; Yuanchao Shu, Zhejiang University, Hangzhou, China, ycshu@zju.edu.cn; Jiming Chen, Zhejiang University, Hangzhou, China, cjm@zju.edu.cn.


ACM 2474-9567/2025/3-ART6
https://doi.org/10.1145/3712272

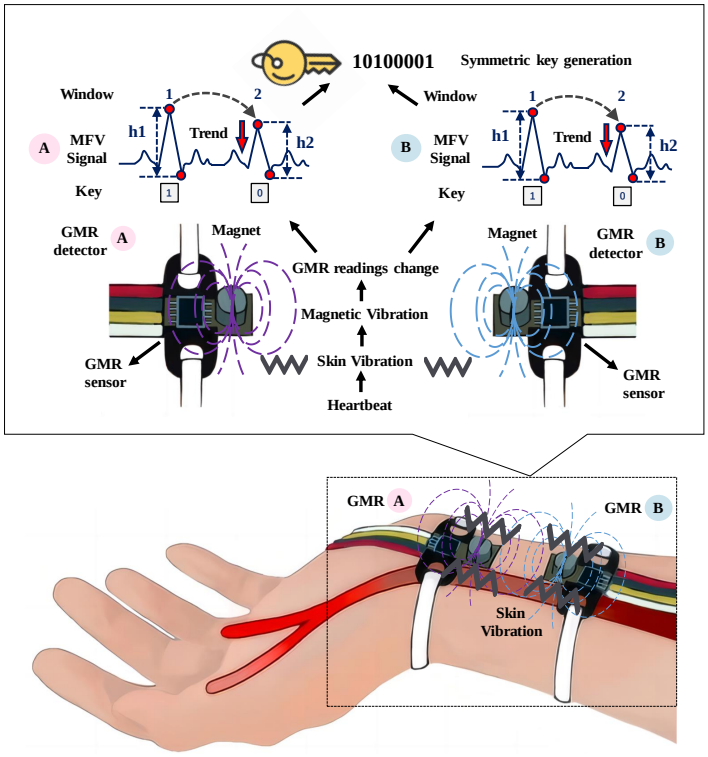



Fig. 1. An illustration of MagKey. The Skin vibration from the heartbeat leads to the vibration of the magnet attached to the skin. The magnetic vibration can be captured by the GMR sensor to generate symmetric keys.

billion by 2030 [3]. The rapid advancement of wearables has given rise to a wide range of device-to-device (D2D) communication functions and applications, including social networking, health monitoring [4], and mobile payment. As a fundamental step of D2D communication, how to securely pair wearable devices has attracted increasing attention from academia and industry.

Recently, symmetric key generation based on biometric characteristics has emerged as a promising solution for wearables pairing. Wearables capitalize on ubiquitous body signals [5] or person-independent physical attributes as sources for random symmetric key generation [6, 7]. When two wearables independently generate identical keys, it implies that these devices are in proximity to the same individual. This method establishes mutual trust between wearables by harnessing the entropy of the random sources.

Heartbeats hold significant promise among all biometric-based symmetric key generation solutions due to their inherent randomness and spontaneity. The heartbeat signal is spontaneous and thus can be measured anytime and anywhere, making it a versatile and reliable source for symmetric key generation [8]. Existing approaches mainly utilize sensors to capture heartbeat representations, including electrocardiography (ECG) [9], photo-plethysmography (PPG) [10], Seismocardiography (SCG) [11], and Ballistocardiography (BCG) [12, 13]. Compared with ECG, PPG, and SCG, BCG offers greater accessibility by measuring the body's recoil forces in response to cardiac blood ejection into the vasculature. Additionally, the BCG demonstrates notable inclusivity. For example, PPG measurements can sometimes be affected by variations in skin tones because they rely on light

absorption and reflection. Thus, it could serve as a promising random signal source for symmetric key generation on wearables.

However, achieving BCG-based on-wearable symmetric key generation still faces several challenges.

• **Low-fidelity BCG signal sampling**. Current wearable BCG measurements rely on piezoelectric sensors [14–16]. When pressure is applied, it displaces the piezo film from its mechanical neutral axis, inducing high strain within the piezopolymer and generating high voltages [17]. However, the recoil force experienced by the wearable is typically weak, resulting in insufficient deflection of the piezopolymer. Consequently, piezoelectric sensors struggle to accurately measure the BCG. Furthermore, sensors placed at different locations experience varying recoil forces from the body, leading to inconsistent performance.

• **Limited key generation rate**. Current heartbeat-based schemes extract inter-pulse interval (IPI) information for key generation, leveraging its nature as a recognized random signal source [8, 18, 19]. However, the IPI has limited entropy. Even when employing an ECG sensor, the IPI signal can only yield approximately 3 bits of key per second. Consequently, given the typical heart rate range of 60 - 100 beats per minute [20], it necessitates approximately 40 seconds to generate a 128-bit key. Furthermore, employing piezoelectric sensors exacerbates this issue due to their inherently low signal-to-noise ratio (SNR) [8], further reducing the key generation rate.

To this end, in this paper, as shown in Figure 1, we propose MagKey, a symmetric key generation scheme that exploits BCG to achieve secure pairing on wearables. Specifically, MagKey addresses the aforementioned challenges with the following designs.

• **New BCG sensing modality and methodology**. Different from existing BCG sensing modalities, MagKey adopts the "Leverage Principle" to harness a tiny permanent magnet and a giant magnetoresistance (GMR) sensor to sense the subtle recoil force induced by the beating of the heart. Specifically, we embed a tiny permanent magnet on the wearable, coupled with a GMR sensor positioned nearby. During operation, the permanent magnet functions as a compact "load arm," vibrating in response to recoil forces, thereby inducing fluctuations in the magnetic field detected by the adjacent GMR sensor. Leveraging the exceptional sensitivity of the GMR sensor to magnetic field variations, it effectively extends the "lever arm." In this way, we can efficiently sense BCG using magnetic field vibration (MFV) signals.

• **New random feature for key generation**. To enhance the speed of key generation, we've identified a new random feature within the MFV signal. Specifically, we've discovered that the peak-to-peak trend (PPT) of the MFV signal demonstrates enough randomness, presenting an opportunity for its utilization as a reliable source for key generation. The PPT exhibits the following characteristics, which are instrumental for secure wearable pairing: (1) The PPTs of the MFV signals are similar and exhibit a strong correlation when measured by two GMR sensors placed on the same human body; (2) The PPTs of the MFV signals exhibit no obvious correlation when measured by two GMR sensors placed on different human bodies; (3) The PPT of the MFV signals have sufficient randomness to extract secure cryptographic keys. Note that the PPT does not require any collection effort, as it inherently exists within the MFV signal.

• **Robust signal processing pipeline**. The strength of the MFV signals is affected by the device placement, the individual differences, and the environment due to the hardware imperfections and the vital sign dynamics. We design a set of simple but effective signal processing algorithms for key generation, including peak-to-peak extraction, screening, and trend alignment methods. Moreover, to eliminate the remaining bit mismatch after signal processing and quantization, we utilize the fuzzy commitment scheme to remove inconsistent bits.

We prototype MagKey on a one-layer flexible printed circuit (FPC) and a two-layer printed circuit board (PCB) using COTS analog components as shown in Figure 3b. We conduct extensive experiments in various practical scenarios to evaluate the performance of MagKey. The evaluation involves 30 volunteers of diverse genders, ages, and skin tones. Note that MagKey is compatible with the existing IPI-based key generation scheme, and thus supports three key generation modes, i.e., PPT only, IPI only, and PPT plus IPI. The field studies show that MagKey can effectively utilize the new random feature of heartbeats (i.e., PPT), and achieves consistently high

Table 1. A summary of the literature on heartbeat-based key generation system.

| Work | Randomness extraction | BGR | BAR | Heartbeat signals | Skin tones | Moisture | Lightweight |
|---|---|---|---|---|---|---|---|
| MagKey (ours) | Peak-to-peak trend | 1 bit/s | 94.2% | BCG | √ | √ | √ |
| MagKey w. IPI and IPI trend | Peak-to-peak trend /IPI/IPI trend | 6 bit/s | 94.2% | BCG | √ | √ | √ |
| Lin *et al.* [8] | IPI (bit 4 to bit 6) | 3 bit/s | N/A | SCG | √ | √ | × |
| Rostami *et al.* [22] | IPI (bit 1 to bit 4) | 4 bit/s | 96.4% | ECG | √ | × | × |
| Seepers *et al.* [23] | IPI (bit 5 to bit 7) | 3 bit/s | N/A | ECG | √ | × | × |
| Chizari *et al.* [21] | IPI trend | 1 bit/s | N/A | ECG | √ | × | × |
| Zhang *et al.* [6] | IPI trend | 1 bit/s | 94.1% | PPG | × | × | √ |

performance with the 0.96 bit/s key generation rate, particularly in scenarios involving different skin tones (up to 0.98 bit/s), body hair (up to 0.99 bit/s), tattoos (up to 0.96 bit/s), wearing positions (up to 0.77 bit/s), and moisture levels (up to 0.98 bit/s). As the IPI is a known random source, we focus on evaluating the MagKey in PPT only mode. Additionally, we test the compatibility of MagKey when also including IPI as a random source. When switching to PPT plus IPI mode, MagKey brings about a 33% improvement in key generation rate compared to pure IPI-based approaches such as [8] and [21].

In Table 1, we compare various aspects of heartbeat-based key generation methods such as randomness extraction, types of heartbeat signals, applicability to different skin tones and skin moisture levels, and whether it is lightweight. Most existing heartbeat-based key generation approaches focus on extracting entropy from the Inter-Pulse Interval (IPI). In contrast, our method leverages the peak-to-peak trend in the heartbeat signal to extract more randomness information. This approach enhances the security and randomness of key generation, thereby providing a more robust guarantee for encrypted communication and data protection.

MagKey explores the compact BCG for key generation. Traditional ECG sensors often require complex electrodes that are in direct contact with skin and are not suitable for daily use. Besides, the skin surface moisture levels can affect the results of the ECG measurements of the heartbeat; wet skin may result in poor contact between the electrodes and the skin, which can affect the transmission of electrical signals. Similarly, Photoplethysmography (PPG) sensors are influenced by factors such as body fluids and skin tones due to the elevated melanin levels in darker skin, causing absorption of the laser light and consequently reducing the signal-to-noise ratio of the measurements [24, 25]. When measuring heart rate with SCG, the sensor is usually strapped to the chest or waist, which is uncomfortable and not light enough for the patient's daily use. To address these limitations, there have been efforts to measure heartbeats using Giant Magnetoresistance (GMR) sensors [25–27]. However, the extraction of peak-to-peak trends for key generation using GMR sensors to acquire the magnetic field vibration (MFV) signal remains unexplored. This paper extends the concept of heartbeat-based key generation to GMR sensors, offering a novel approach in this domain.

We have developed a novel approach that uses a new feature (peak-to-peak trend) as a random source, which improves the efficacy and robustness of existing heartbeat-based key generation methods. While the bit generation rate of MagKey is approximately 1 bit/s, it provides a "free" random source for heartbeat-based key generation

schemes. In practice, we can combine PPT with inter-pulse interval (IPI) for key generation, as both are derived from the heartbeat signal. Consequently, MagKey achieves a key generation rate of about 6 bits/s by incorporating techniques from Rostami *et al.* [22] and Seepers *et al.* [23] to extract keys through IPI and IPI trends. The major advantages of MagKey are its robustness and inclusiveness compared to other heartbeat-based key generation systems. MagKey can handle heartbeat measurement and key generation on wet skin and across different skin tones, while being very lightweight. These integrated features highlight MagKey's versatility and potential to enhance the overall efficiency of key generation.

Additionally, the BCG method is inherently designed for stationary applications, which aligns with its characteristics. BCG is typically monitored in resting conditions, e.g., in a lying, seated, or standing still posture [28]. Some studies have subjects sit quietly in a chair [29, 30] or on a bed [31]. Additionally, it is important to highlight that heartbeat-based key generation is particularly vulnerable to motion artifacts [8, 23]. To address potential issues in dynamic environments, we propose incorporating accelerometers as complementary devices in different scenarios.

The main contributions of this paper are summarized as follows:

- To the best of our knowledge, this paper proposes the first-of-its-kind sensing modality, i.e., MFV, for BCG measurement that leverages a combination of low-cost permanent magnetic and GMR sensors. Additionally, this paper first proposes harnessing the PPT inherent in BCG as a novel source for random key generation.
- We propose a power-efficient hardware-software co-design tailored for the BCG-based key generation scheme. We apply a filter-based signal pre-processing method in the analog domain to obtain the MFV signal, propose a quantification method to characterize the PPT, and introduce an effective PPT screening approach to mitigate the effects of noise and motion artifacts on key generation.
- We prototype MagKey on a one-layer flexible printed circuit (FPC) and a two-layer printed circuit board (PCB), and follow the Institutional Review Board (IRB) protocol to conduct extensive experiments in different environments to evaluate its usability, effectiveness, and security.

The rest of this paper is organized as follows. §2 presents the feasibility study. §3 shows the details of our designed key generation scheme. §4 shows a wide range of evaluations to verify Magkey's effectiveness and robustness. §5 presents attack models and performs security analysis. §6 reviews related work. Finally, §8 concludes the paper.

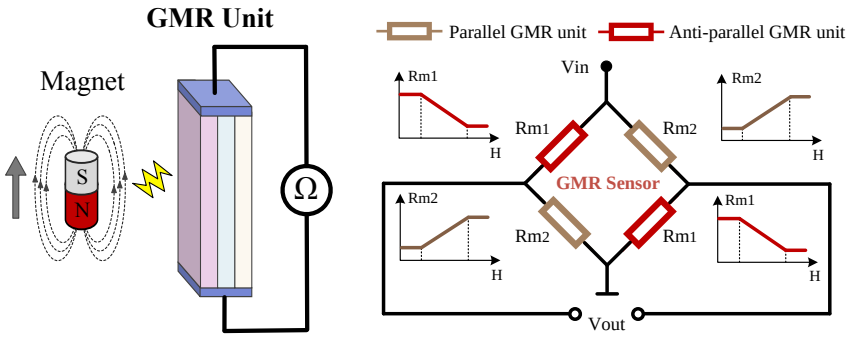
## 2 PRELIMINARY AND FEASIBILITY

In this section, we first introduce the heartbeat detection method by using the GMR sensor and then we explore the feasibility of symmetric key generation by leveraging the magnetic field vibration.

### 2.1 Heartbeat Detection with the GMR Sensor

**GMR Primer.** The giant magnetoresistance (GMR) refers to the phenomenon in which the electrical resistivity of a magnetic material changes greatly when there is an external magnetic field nearby. In other words, the GMR can convert subtle magnetic field changes into significant resistance changes. There are two types of GMR units: parallel GMR and anti-parallel GMR, which indicate a positive or negative correlation between resistance and external magnetic field strength. A typical GMR sensor consists of two parallel GMR units and two anti-parallel GMR units. These four GMR units form a complete Wheatstone bridge to detect subtle changes in the magnetic field. As shown in Figure 2, two parallel GMR units of the bridge arms exhibit $Rm1 = R + \Delta R(H)$, while the remaining two anti-parallel GMR units exhibit $Rm2 = R - \Delta R(H)$. The output of this full-bridge GMR sensor is:

$$V_{\text{out}} = V_{\text{in}} \left( \frac{R_{m2}}{R_{m1} + R_{m2}} - \frac{R_{m1}}{R_{m1} + R_{m2}} \right) = V_{\text{in}} \left( \frac{\Delta R(H)}{R} \right) \tag{1}$$




(a) GMR unit (b) GMR Sensor

Fig. 2. Structure of (a) GMR unit and (b) GMR Sensor.

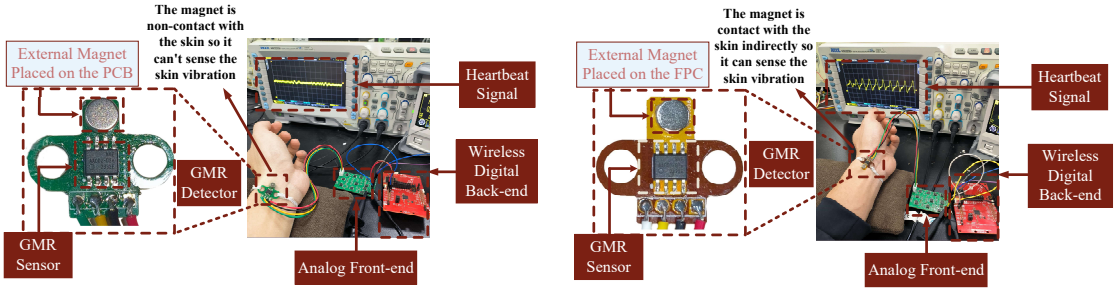
where $V_{in}$ is the bias voltage, $R$ is the initial resistance of the GMR element, and $\Delta R(H)$ is the resistance change caused by the external magnetic field. From the above equation, the output of the GMR sensor is zero when the external magnetic field does not change. When the external magnetic field changes, the output of the GMR sensor can reflect the changes in the magnetic field significantly.

**Heartbeat detection by leveraging the biomagnetism variation.** Previous work has demonstrated the potential of leveraging biomagnetism to monitor heartbeat signals [32–34]. This approach is based on a physiological process where the blood circulation within the body during each heartbeat gives rise to the movement of charged particles (ions). These ions, in turn, induce a biomagnetic field, the strength of which corresponds to the fluctuations occurring with individual heartbeat. For example, MagWear [35] proposes a dedicated hardware design to detect the biomagnetism to monitor the heartbeat signals by using the GMR sensor. Figure 3a shows an illustration of heartbeat detection using biomagnetism. An external magnet is placed on the PCB board and non-contact above the arm. The magnetic field of this external magnet is affected by the biomagnetism and can be detected by the GMR sensor. We use this device to monitor the heartbeats of two volunteers. Figure 4a shows the results. We observe the GMR readings are not stable with the low signal-to-noise ratio, making it difficult to observe clear and stable heartbeat patterns. This is expected since the biomagnetism signal has an extremely low strength (e.g., typically below $10^{-10}T$ [36]), and the subtle biomagnetism signal is also susceptible to external interference and individual differences.

**Heartbeat detection by leveraging the magnetic field vibration (MFV).** Instead of directly using biomagnetism to detect heartbeat signals, we leverage the skin vibration detected by the magnetic field vibration for heartbeat detection. Figure 3b shows an illustration of heartbeat detection using magnetic field vibration. We place an external magnet on the FPC, which directly contacts the arm. In this way, the FPC acts as a vibration platform and the skin vibration induced by the heartbeat can also cause the external magnet to vibrate. Hence the GMR sensor readings will change due to the external magnetic field vibration. Figure 4b shows the detection results. The GMR sensor readings reflect the vibrational displacement of the magnet caused by the skin vibration, thus reflecting the heartbeat signal. We observe that the detection method based on the magnetic field vibration performs better compared with the subtle biomagnetism. The GMR sensor readings exhibit obvious periodicity and stability with a high signal-to-noise ratio.

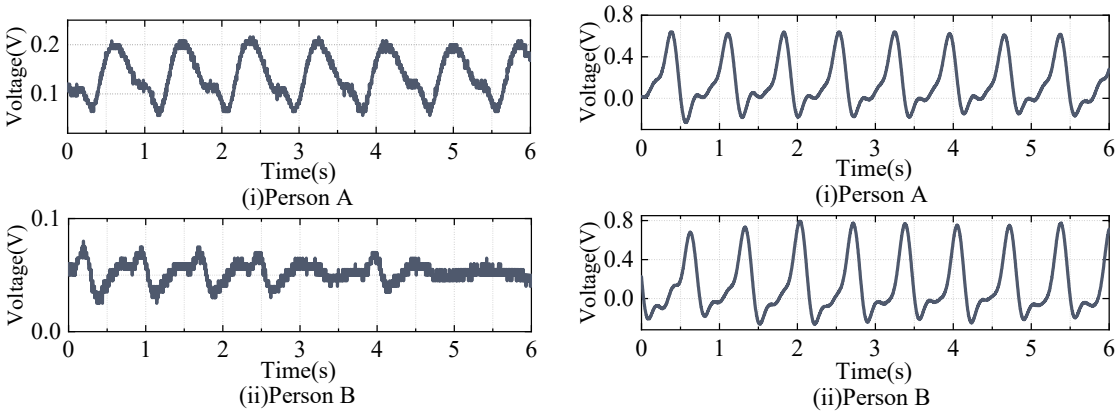
## 2.2 Feasibility of the Magnetic Field Vibration (MFV) Signals for Symmetric Key Generation

We explore the feasibility of the MFV signals for symmetric key generation from the following aspects.




(a) Heartbeat detection using biomagnetism (b) Heartbeat detection using magnetic field vibration

Fig. 3. An illustration of heartbeat detection using biomagnetism vs. magnetic field vibration induced by skin vibration. (a) An external magnet is placed on the PCB and can't sense the skin vibration because the PCB is a hard material. (b) An external magnet is placed on the FPC and thus can sense the skin vibration.




(a) Heartbeat detection using biomagnetism. (b) Heartbeat detection using magnetic field vibration

Fig. 4. Heartbeat detection using biomagnetism vs. magnetic field vibration.

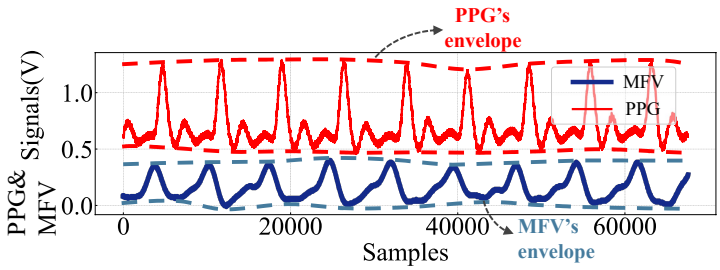



Fig. 5. Similarity measurements of peak-to-peak trends and inter-pulse intervals of heartbeats: PPG sensor and GMR sensor placed on the same person at the same time.

**Similarity between the MFV and PPG Signals.** We first investigate whether the MFV signal can accurately capture heartbeat features. We place a PPG sensor [37] on a volunteer's fingertip to measure the heartbeat. Simultaneously, we measure the MFV signal on the volunteer's wrist of the same hand. As depicted in Figure 5,

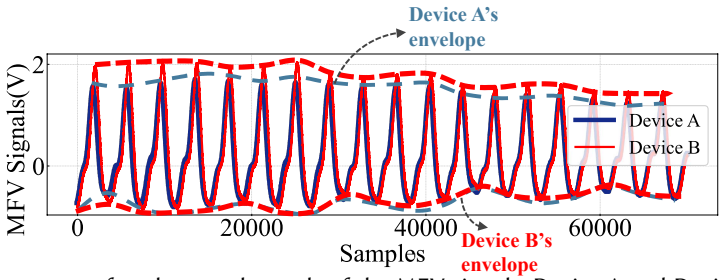



Fig. 6. Similarity measurements of peak-to-peak trends of the MFV signals: Device A and Device B placed on the same person at the same time.

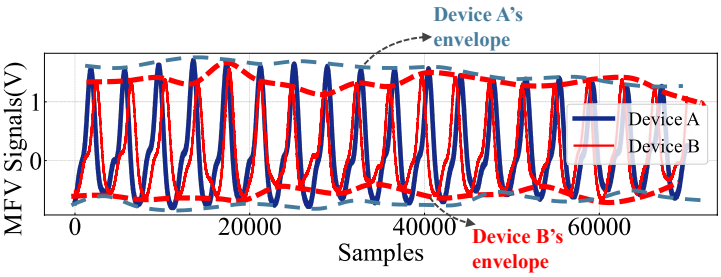



Fig. 7. Disimilarity measurements: Device A and Device B placed on the same person at different times.

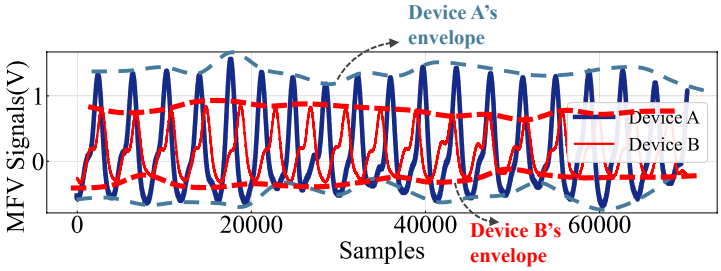



Fig. 8. Disimilarity measurements: Device A and Device B placed on the different persons at the same time.

both the PPG and MFV signals exhibit similar peak-to-peak trends and inter-pulse intervals. However, it's worth noting a time delay between the MFV and PPG signals. This delay arises due to the placement of the sensors at different locations, causing them to experience cardiac blood ejection at different times.

**Similarity of Peak-to-peak Trend (PPT) of the MFV signal.** An important feature for the feasibility of symmetric key generation is the similarity of the MFV signals measured when a pair of wearables is placed on the same human body. GMR sensors are very sensitive to magnetic fields, and when neighboring devices are placed in the same area (e.g., on the same wrist) at the same time, the PPT of the MFV signals may not be the same for a variety of reasons (blood vessel size, depth of the vessel burial, and the sensor placement, which affect the proximity of the vessel to the magnet and the volume of blood flow in the circulation). However, similar PPT measurements can be obtained due to the relative consistency of vascular distribution and nervous system regulatory mechanisms. We perform preliminary experiments on the same human body to verify the similarity and consistency of the PPT measurements of the MFV signals. Figure 6 shows similar measurements of PPT of the MFV signals measured simultaneously by a pair of devices positioned on the wrist of the same human body. Consequently, such similarity and consistency in MFV signal measurements serve as the foundation for generating symmetric keys using GMR sensors.

**Temporal Irrelevance of PPT of the MFV signal.** Next, we verify that the trends of the peak-to-peak value of the MFV signals measured at different times are different for the same individual. Because blood flow and velocity in the radial artery change over time, such changes may be influenced by a variety of factors, including physical status, activity level, and environmental conditions. Therefore, we measure the peak-to-peak trends of the MFV signals at different times. In particular, we perform measurements on the same human body at different times. There is no correlation between the results measured by the two devices at different times, as shown in Figure 7.
**Individual Variations in PPT of the MFV signal.** Finally, we verify that the trends of the peak-to-peak values of the MFV signals measured at the same time are different for different individuals. Figure 8 illustrates the variability in the peak-to-peak trends of the MFV signals between different individuals. This reveals that only GMR sensors that are attached to the same individual can provide similar measurements for key generation and device authentication.

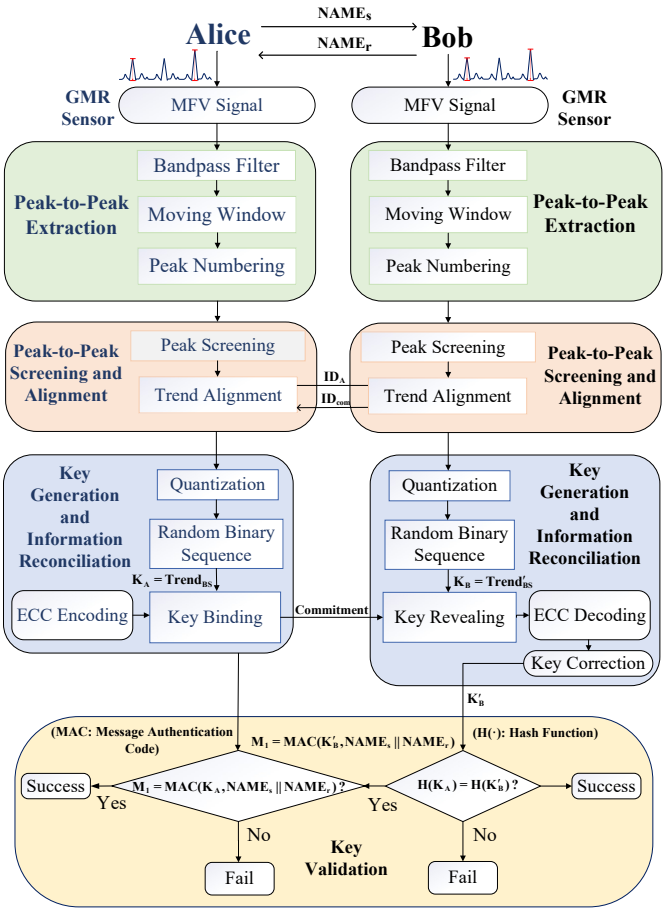



Fig. 9. System overview.

# 3 METHODOLOGY

## 3.1 System Overview

Figure 9 shows the system overview of MagKey, which includes four phases: MFV signal measurement, peak-to-peak extraction, key establishment and information reconciliation, and key validation. In the initial phase of MagKey, both devices independently measure the peak-to-peak values of the MFV signals and extract their trends for key generation. Then, fuzzy commitment is used to correct the inconsistency of the symmetric key. Finally, during the key validation phase, both devices use the message authentication code to confirm that they have generated the same key simultaneously.

## 3.2 MFV signal measurement

Fig. 10 shows the process shows the process of measuring the magnetic field vibration (MFV) signal. Initially, the GMR sensor detects changes in the magnetic field and produces an analog signal proportional to these changes. To amplify the MFV signal, an amplifier with a gain of approximately 30 is used, resulting in an amplified signal of approximately 0.5V.

However, the amplified MFV signal may be susceptible to noise interference, as the noise is also amplified along with the signal. To mitigate this problem, a band-pass filter, comprising a low-pass and a high-pass filter, is employed to isolate the MFV signal corresponding to the heartbeat frequency. The bandpass filter allows signals in the range of [0.6Hz, 3Hz] to pass through, effectively matching the heartbeat frequency.

After passing through the bandpass filter, the amplitude distribution range of the MFV signal contains negative voltages that cannot be adequately sampled by the microcontroller's (MCU) analogue-to-digital converter (ADC), which only captures positive voltages. To overcome this, a voltage lift circuit is implemented to shift the MFV signal. The original peak-to-peak value from the bandpass filter is approximately 0.5V with a range of [-0.25V, 0.25V]. By boosting the signal by approximately 1V, the signal range is adjusted from [-0.25V, 0.25V] to [0.75V, 1.25V], which is within the sampling range of the MCU's ADC, which operates between [0V, 3.3V]. This conditioning process ensures that the MFV signal is properly prepared for accurate sampling by the MCU.

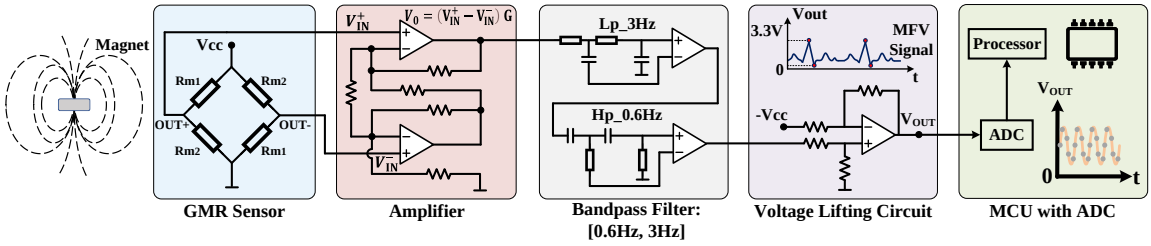



Fig. 10. MFV signal measurement.

## 3.3 Peak-to-peak Extraction

Peak-to-peak extraction is a crucial step in extracting keys from the MFV signals. To obtain vital human physiological information from the MFV signals, we first design a band-pass filter that eliminates background interference noise. Given that the typical human heart rate ranges from 60 to 100 bpm, we filter the signal output from the GMR sensor with a band-pass filter in the range of 0.6 Hz to 3 Hz. This eliminates both the DC and high-frequency components. Second, we divide the MFV signals into different intervals based on a sliding window that starts at the beginning of the signal and slides sequentially. The length of the window is the current heartbeat

period, which is defined by the time difference between two adjacent peaks in the original MFV signals. Next, we locate the maximum and minimum values within each interval. Peak-to-peak values are calculated by taking the difference between the maximum and minimum values, and then these peak-to-peak values are numbered in chronological order, starting with one. Continue to move the window until the entire heartbeat signal has been swept. The window size can be adjusted adaptively according to the current heartbeat period. Algorithm 1 describes the method for extracting peak-to-peak values from the MFV signals.

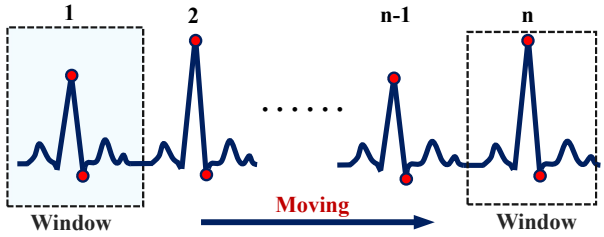



Fig. 11. Peak-to-peak Extraction.

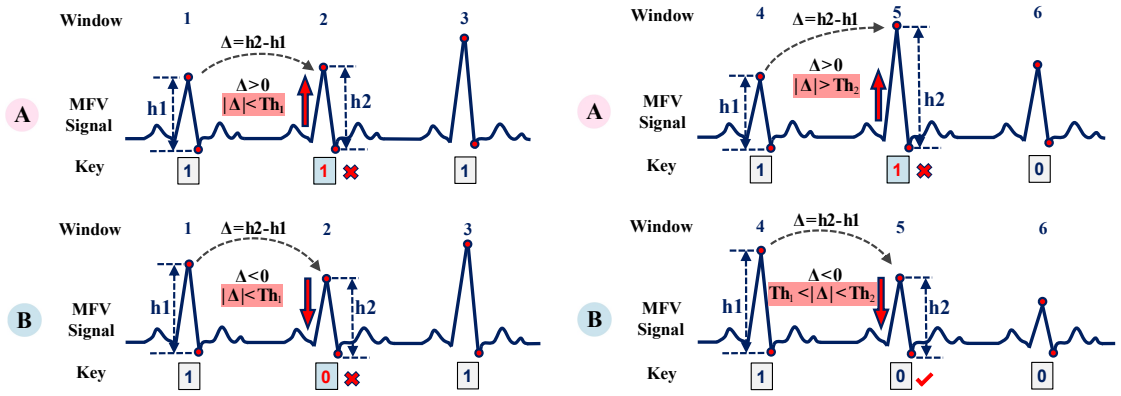
**Algorithm 1** Peak-to-Peak Extraction

**INPUT**:*MFV signals* $V_{MFV}$
$V_{Peak2Peak} \leftarrow 0$
$ID \leftarrow 0$
$V_{max} \leftarrow 0$
$V_{min} \leftarrow 1$
**OUTPUT**:$\{ID, V_{Peak2Peak}\}$
**for** each $window \in [1, n]$ **do**
  **if** $V_{MFV} > V_{max}$ **then**
    $V_{max} = V_{MFV}$ ;
  **end if**
  **if** $V_{MFV} < V_{min}$ **then**
    $V_{min} = V_{MFV}$ ;
  **end if**
  $V_{Peak2Peak} \leftarrow V_{max} - V_{min}$ ;
  $ID \leftarrow ID + 1$ ;
  **return** $\{ID, V_{Peak2Peak}\}$
**end for**

## 3.4 Peak-to-peak Screening and Trend Alignment

After extracting the peak-to-peak values of the MFV signals, we further need to conduct peak-to-peak screening and trend alignment. There are two cases that affect the peak-to-peak values.

**Case 1: a lower-boundary threshold to reduce the impact of noise.** The peak-to-peak value trends of the MFV signals in two devices vary due to noise rather than changes in the physiological characteristics of the human body. In Figure 12a, Device A captures a second MFV signal with a larger peak-to-peak value than the




(a) The noise impact on the peak-to-peak values of MFV signals. A lower threshold $Th_1$ is used to reduce the noise impact. The common ID is : {1, 3}.

(b) The movement impact on the peak-to-peak values of MFV signals. An upper threshold $Th_2$ is used to reduce the impact of movement. The common ID is : {4, 6}.

Fig. 12. The impact of noise and sudden movement on the peak-to-peak values of MFV signals.

first MFV signal, while Device B captures a second MFV signal with a smaller peak-to-peak value than the first MFV signal. The trend of the peak-to-peak values is different among them, but they all change by a small amount. Therefore, we consider that their changes are caused by noise. To solve the inconsistent trend of the peak-to-peak values caused by noise, We need a low-boundary threshold $Th_1$. We consider the peak-to-peak value to be effective only if it exceeds a threshold value of $Th_1 = \alpha \cdot \sigma$, where $\alpha$ is the threshold scaling factor, and $\sigma$ is the standard deviation of samples from MFV signals.

**Case 2: an upper-boundary threshold to reduce the impact of sudden movement.** The peak-to-peak values of the MFV signals may increase abruptly due to the sudden movement. The small external magnet attached to the skin not only detects the skin vibration caused by the heartbeat, but also tracks the movement of the body part where the device is placed. In Figure 12b, Device A captures a second MFV signal with a larger peak-to-peak value than the first MFV signal due to sudden movement while Device B captures a second MFV signal with a smaller peak-to-peak value than the first MFV signal due to heartbeats, making it difficult to align the MFV signals. In order to solve this problem, we need an upper-boundary $Th_2$ threshold to reduce the impact of sudden movement. We consider the peak-to-peak value to be effective only if it is lower than a threshold value of $Th_2 = (1 - \alpha) \cdot \mu$, where $\mu$ is the mean of the samples of the MFV signals.

**Summary.** We present a filtering technique that retains only the sequence numbers whose peak-to-peak variation is between the lower threshold $Th_1$ and the upper threshold $Th_2$, where the lower threshold is determined by noise while the upper threshold is determined by movement. Algorithm 2 provides a method for the peak-to-peak screening and alignment of MFV signals. The determination of the parameter $\alpha$ is discussed in §4.3. Each device then directly compares its own and another device's peak-to-peak sequence numbers, only keeping the common values. For example, the effective peak-to-peak sequence of Device A and Device B is $ID_{common} = ID_A \cap ID_B$, where $ID_A$ and $ID_B$ are the peak-to-peak sequences of Device A and Device B, respectively. This process is trend alignment.

**Algorithm 2** Peak-to-Peak Screening

**INPUT**:$\{ID(i), V_{Peak2Peak}(i)\}$
$Th_1 \leftarrow \alpha \cdot \sigma$
$Th_2 \leftarrow (1-\alpha) \cdot \mu$
**OUTPUT**:$\{ID(i), V_{Peak2Peak}(i)\}$
**for** each $i \in [1, n]$ **do**
  **if** $Th_1 < |V_{Peak2Peak}(i) - V_{Peak2Peak}(i-1)| < Th_2$ **then**
    $V_{Peak2Peak}(i) \leftarrow V_{Peak2Peak}(i)$ ;
    $ID(i) \leftarrow ID(i)$ ;
  **else**
    $ID(i) \leftarrow 0$ ;
    $V_{Peak2Peak}(i) \leftarrow 0$ ;
  **end if**
**end for**

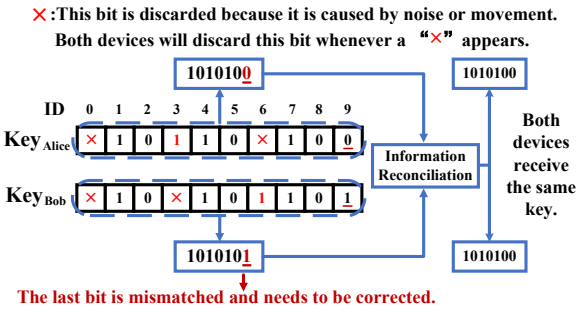



Fig. 13. Key generation and information reconciliation.

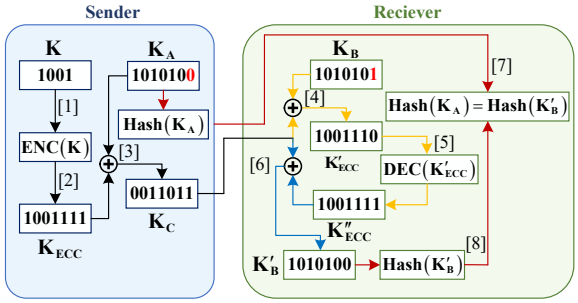



Fig. 14. Fuzzy Commitment.

## 3.5 Key Generation and Information Reconciliation

**Key generation.** After the trend alignment, the two devices perform a quantization operation on the peak-to-peak value corresponding to the serial number of the common list, if the current peak-to-peak value is greater than the previous peak-to-peak value, it is quantized as bit "1", otherwise it is quantized as bit "0".

**Information reconciliation.** When the keys are generated by the two devices, it is likely that the keys will not be identical due to imperfections in the sensors and variability in physiological characteristics, as shown in Figure 13. Therefore, we conduct the information reconciliation to correct the key mismatches that may exist between them.

We use fuzzy commitment primitives[38], which combine both error correction code (ECC) and cryptographic techniques, to address potential inconsistencies in the key generation between two devices. The error correction code can detect and correct any discrepancies in the binary sequences generated by the devices that are within the correction capacity. For example, Alice and Bob will use the same set of error correction codes, i.e. Bose-Chaudhuri-Hocquenghem (BCH) codes in this paper. Successful correction can only be performed if the sequence of bits extracted by both devices has a small number of bit errors. Specifically, the number of mismatched bits between the keys generated by Alice and Bob should be within the error tolerance range of the error correction code. If the number of error bits exceeds this error tolerance range, the correction process cannot be finished.

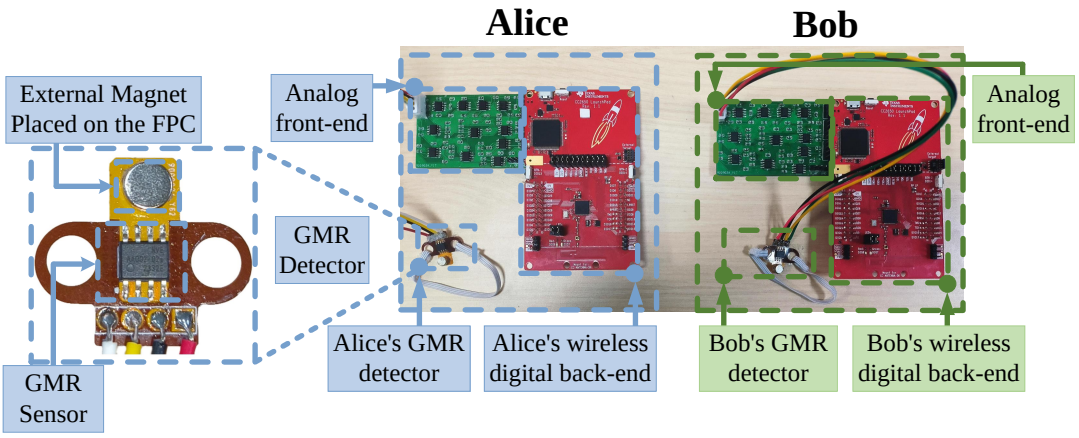



Fig. 15. Hardware prototype.

Thus, the error correction code must have the ability to correct mismatched bits between two legitimate users, while preventing a successful attack by an illegitimate user.

Figure 14 shows the specific process of fuzzy commitment. The sender performs the ECC encoding process (step "[1]" in Figure 14) on the nonce $K$ to obtain the message $K_{ECC}$, which adds redundant information to $K$. Let the function $ENC(\cdot)$ denote the mapping from $K$ to $K_{ECC}$, then $K_{ECC} = ENC(K)$ ("[2]"). In contrast, the receiver uses the ECC decoding process $DEC(\cdot)$ to correct erroneous bits in $K_{ECC}$, denoted by $K''_{ECC} = DEC(K'_{ECC})$ ("[5]"). For the fuzzy commitment, the first step is to perform an XOR operation and create a commitment. The sender performs the XOR operation with $K_{ECC}$ and the binary sequence $K_A$ to generate the ciphertext $K_C$, which is written as $K_C = K_{ECC} \oplus K_A$ ("[3]"). The sender then creates a commitment as follows: $Commitment = \{K_C, Hash(K_A)\}$, where $Hash(\cdot)$ represents a one-way hash function ("[7]"). When the receiver receives the ciphertext $K_C$, it first XORs its own binary sequence $K_B$ with the ciphertext $K_C$ and $K_C \oplus K_B$) to get the error correction code $K'_{ECC}$ ("[4]"), which may have error bits. After error correction, we get $K''_{ECC}$. If the percentage of error bits in the length of the codeword $K'_{ECC}$ is within the error correction capability, the key can be successfully revealed by $K'_B = K''_{ECC} \oplus K_C$ ("[6]") and both devices agree on the same key ($Hash(K_A) = Hash(K'_B)$, i.e., $K_A = K'_B$) ("[8]"), otherwise the process must be restarted.

### 3.6 Key Validation

After validating that $K_A = K'_B$, the receiver sends the Message Authentication Code (MAC) to the sender for key validation, denoted by $M_1 = MAC(K'_B, NAME_S \,||\, NAME_R)$, where $NAME_S$ and $NAME_R$ are the names of the sender and the receiver, respectively, and $||$ represents the concatenate operation. The sender then computes the message authentication code of the message (i.e., $MAC(K_A, NAME_S \,||\, NAME_R)$) and compares it to $M_1$ to verify that the two legitimate devices have successfully generated the same symmetric key.

## 4 EVALUATION

### 4.1 MagKey Prototype

We prototype the MagKey using off-the-shelf analog components and the ultra-low-power TI CC2650 Launchpad. Figure 15 shows the hardware prototype. MagKey consists of three main components: (1) a GMR detector, (2) an analog front-end, and (3) a wireless digital back-end.

- **The GMR detector.** The GMR detector consists of a GMR sensor and an external magnet. We choose NVE AA002 [39] as the GMR IC. For the external magnet, we choose a permanent magnet with a strength of 125mT and a size of 5mm × 2mm. To make the external magnet on the GMR detector better reflect the strength of the heartbeat signals, we fix the magnet of the GMR detector on the flexible printed circuit (FPC). The skin vibration causes the FPC deformation and then further causes the magnet to be displaced. The FPC is a soft material and can sense the vibration of the skin more sensitively, compared to placing the magnet directly on the PCB. In addition, we place the GMR sensor on a reinforced FPC, which makes the structure of the GMR detector more stable. Our hardware design balances performance and wearing comfort.
- **The analog front-end.** The output of the GMR sensor is connected to a low power amplifier consisting of an INA126 IC [40] with a gain of 30. This configuration enables the detection and amplification of subtle variations in the MFV signals. The resulting output signal is subsequently fed to a filter processing circuit. There is a high-pass filter and a low-pass filter consisting of OP07 [41] from Texas Instruments, with cutoff frequencies of 0.6 Hz and 3 Hz, respectively. By merging these two high-pass and low-pass filters, a band-pass filter [0.6 Hz, 3 Hz] can be created, which eliminates other signals to obtain the desired heartbeat signals. The operational amplifier INA126 amplifies the filtered analog signal with a gain of 20. The signal is then converted by a voltage converter to 0-3.3V and transmitted to the wireless digital back-end.
- **The wireless digital back-end.** For the wireless digital back-end, we choose Texas Instruments' low-power wireless MCU, the CC2650, which integrates a 2.4GHz RF transceiver compatible with the low-power Bluetooth (BLE) 4.2 specification and the IEEE 802.15.4 PHY and MAC. We use the CC2650's on-chip 12-bit ADC to sample the signals processed by the analog front-end and convert them to digital signals for further processing. Therefore, the MCU is responsible for (1) acquiring the analog signals, converting them to digital signals, and processing them to generate the keys; (2) subsequent wireless communication between the devices, including information exchange, information verification, and key validation.
- **Magnet Safety.** The Magnet Safety Guideline from ACGIH dictates that a magnetic field strength up to 600mT [42] is acceptable for routine exposure of the extremities. Our evaluation shows that by placing magnetic pads under the magnet to reduce the magnetic fields, the magnetic field strength absorbed by the skin is less than 60 mT. This level of magnetic field strength is safe for daily use according to the ACGIH safety guidelines. Furthermore, we recommend that individuals with cardiac implants to consult with their medical practitioner to ensure that the magnetic field will not adversely affect their health, as magnetic field exposure of less than 0.5 mT is considered safe for this population [43].

## 4.2 Experiment Setup

In this section, we use our MagKey prototype to capture human heartbeat signal data for secure device pairing. In order to evaluate the efficiency and security of MagKey, we investigate various influencing factors. These include users of different ages, genders, BMIs, and skin tones, as well as different environments, users' motion status, the part of the device being worn, the users' physiological state, algorithmic parameters, and different attack scenarios. We then measure the randomness of the generated keys and their energy consumption.

**Evaluation metrics.** We use the following three metrics to characterize the performance of MagKey:

- Bit agreement rate (BAR): The BAR is the percentage of matching bits generated by Alice and Bob, i.e., the number of matching bits over the length of the key.
- Bit generation rate (BGR): The BGR is the number of bits that the system can produce per second; it indicates the rate of key generation.
- Entropy: Entropy quantifies the unpredictability and randomness of generated keys as measured by Shannon Entropy. This metric reveals the information that each bit provides. A greater entropy value, ranging from 0 to 1, indicates more randomness in the generated keys.

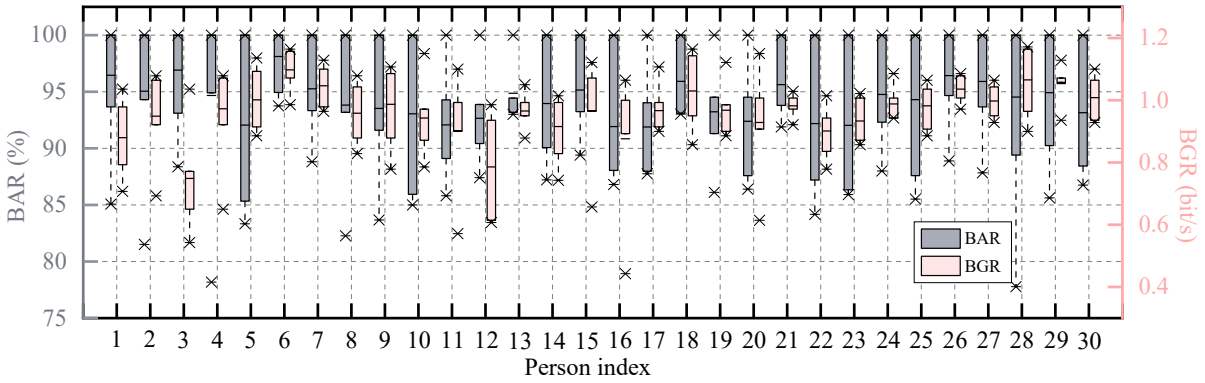



Fig. 16. Overall performance.

**Data collection.** We recruit 30 volunteers (15 females and 15 males) between the ages of 21 and 53 with different skin tones, weights, and heights (BMI ranging from 15.2 to 31.6) to participate in our experiments. During data collection, the prototype devices will be individually attached to each participant's wrist. Our test procedure engrosses a 3-minute evaluation for each user conducted 6 times. The sampling rate is 500Hz.

## 4.3 Field Study

**Overall performance.** We evaluate the bit agreement rate and the bit generation rate of the key generation process of 30 volunteers, as shown in Figure 16. MagKey performs well across all 30 participants, achieving an average of 94.2% for the bit agreement rate and 0.96 bit/s for the bit generation rate.

**Impact of gender and age.** Next, we investigate the impact of age and gender on the performance of MagKey. As illustrated in Figure 17a, MagKey remains robust across genders. Specifically, the bit agreement rate is 94.6% for females and 94.0% for males. At the same time, the bit generation rate is 0.95 bit/s for females and 0.97 bit/s for males. We then divide the 30 participants into four different groups to investigate the effect of age in detail. As shown in Figure 17b, we observe that both the BAR and the BGR are higher in the 20-30 age and the 30-40 age groups, at 95.5%, 94.5% and 0.96 bit/s, 1.01 bit/s, respectively, while the 50-60 age group showed relatively slightly lower BAR and BGR at 93.4% and 0.92 bit/s, this trend can be attributed to the decreasing intensity and slowing frequency of heart activity as individuals age.

**Impact of BMI.** We investigate the effect of different body mass indexes (BMI) on the performance of the MagKey. BMI is a measure of body fat based on a person's height and weight. We divide 30 participants into four groups: underweight (BMI <18.5), healthy (BMI between 18.5-24.9), overweight (BMI between 25.0-29.9), and obese (BMI >30.0). Figure 18a shows that the BAR of the four groups are 95.1%, 95.0%, 93.8%, 92.9%, and the BGR are 0.98 bit/s, 0.96 bit/s, 0.98 bit/s, 0.91 bit/s, respectively. MagKey's BAR and BGR are relatively low for obese subjects. This is because the blood vessels of obese subjects are located deeper from the skin surface. As a result, the pulse caused by the heartbeats is attenuated when it reaches the skin surface, causing the skin to vibrate less.

**Impact of skin tones.** We investigate the impact of skin tone on the performance of the MagKey. Our main goal is to assess the inclusivity of the MagKey for a specific study population, considering the sensitivity of the PPG sensor to skin tone. We found that 14 out of 30 participants rated their skin tone between 1-3, 10 rated it between 4-6 and 6 rated it between 7-10. Although we have not yet covered the entire Monk scale, we believe our findings will apply to a more diverse and broader population. Unlike the PPG sensor, which is sensitive to optical paths, the MagKey is resilient to skin tone, as shown in Figure 18b. Across all three skin tone groups, the bit agreement

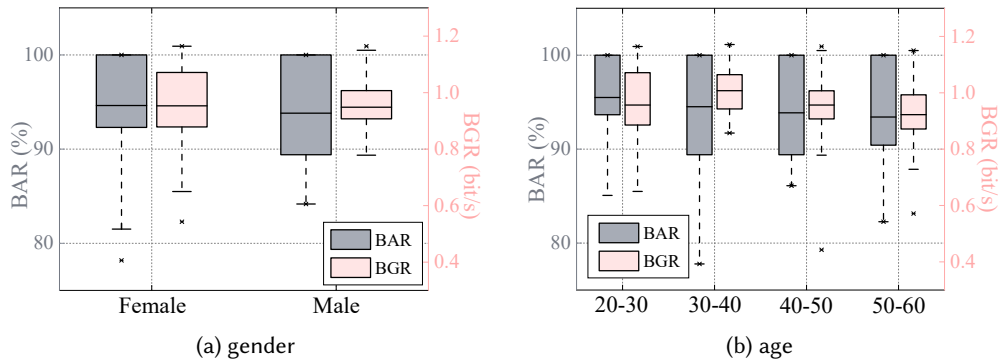



Fig. 17. Magkey performance under different gender and age.

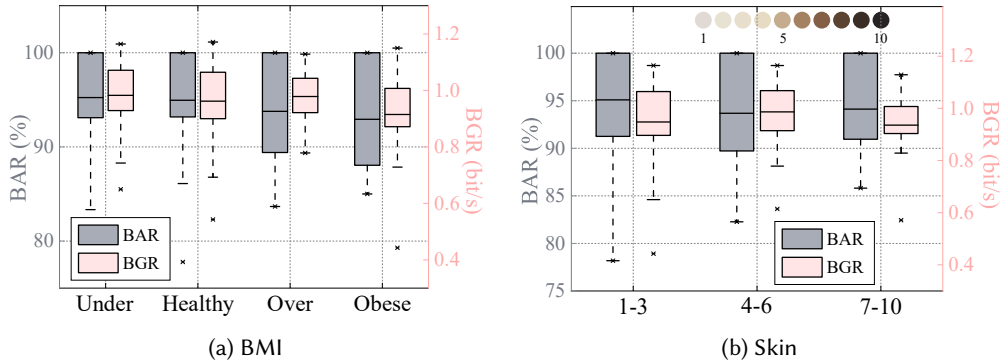


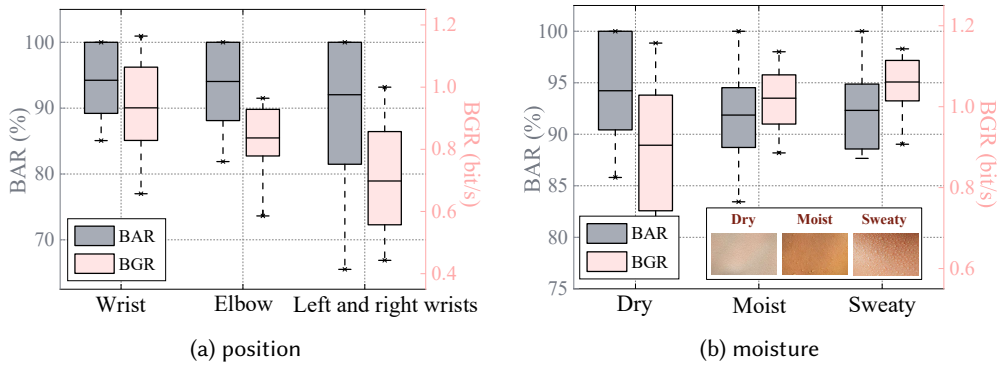

Fig. 18. Magkey performance under different BMI and skin tones.

and bit generation rates for different skin tones are maintained in the range of 93.7% - 94.6% and 0.94 - 0.98 bit/s range, demonstrating its inclusivity.

**Impact of measuring position.** We investigate the effects of two sensors placed on the same wrist, on the same elbow, and on the left and right wrists of the same person to validate the robustness of the MagKey. Figure 19a shows the bit agreement rate and the bit generation rate for all pairwise combinations. The bit agreement rate is 94.2% when the two sensors are placed on the same wrist. Placing the sensors on the elbows results in a bit agreement rate of 94.1% and a bit generation rate of 0.84 bit/s. Similarly, placing the two sensors on the left and right wrists results in a bit agreement rate of 91.7% and a bit generation rate of 0.70 bit/s. Moving from the same wrist to the left and right wrists, the MagKey's bit agreement rate drops by 2.5%, but is still above 90%.

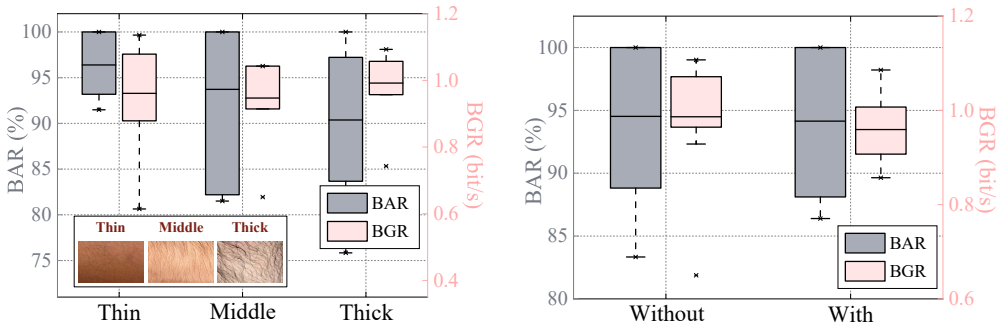
**Impact of moisture levels.** We investigate the impact of moisture levels on the performance of the MagKey. We test the wrists of 15 volunteers at different humidity levels. As shown in Figure 19b, we find that the MagKey adapts to different humidity levels. Going from dry to sweaty, MagKey's bit agreement rate changes from 94.2% to 92.3%, while the bit generation rate increases from 0.90 bit/s to 1.06 bit/s.

**Impact of body hair.** Next, we investigate the impact of body hair on the key generation using MFV signals on the same wrist of the person, and Figure 20a shows the result. As the body hair gets thicker, the bit agreement rate drops from 96.4% to 90.3%, while the bit generation rate remains at about 0.98bit/s. This is to be expected, but still acceptable. Longer body hair makes it more difficult for the FPC and its magnet to sense skin vibrations.




(a) position (b) moisture

Fig. 19. Magkey performance under different measuring position and skin moisture.




(a) body hair (b) tattoo

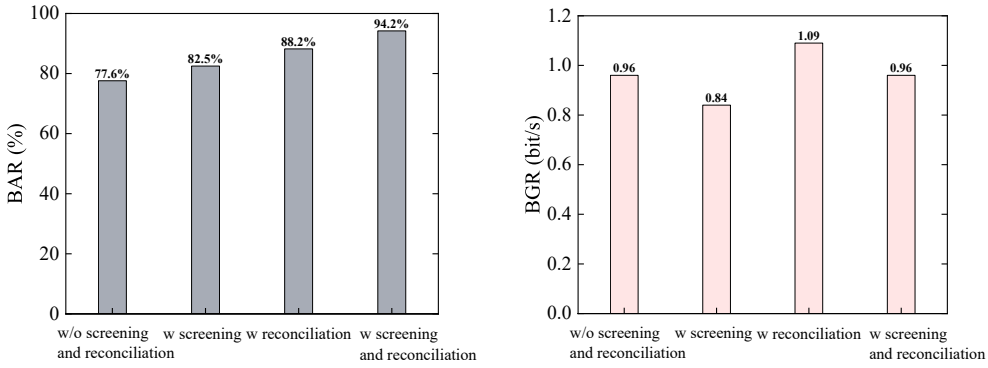
Fig. 20. Magkey performance under different body hair and tattoo.

However, the weight of the magnet brings the FPC closer to the skin. In addition, gel can also be used to make the FPC adhere to the skin without causing discomfort.

**Impact of tattoos.** We investigate the impact of tattoos on the MagKey performance. Similar to the effect of skin tone, tattoos can affect the propagation of optical signals. However, the MagKey is not affected by tattoos, the BAR with and without tattoos is 94.5% and 94.1%, and the BGR with and without tattoos is 0.99 bit/s and 0.96 bit/s, as shown in Figure 20b.

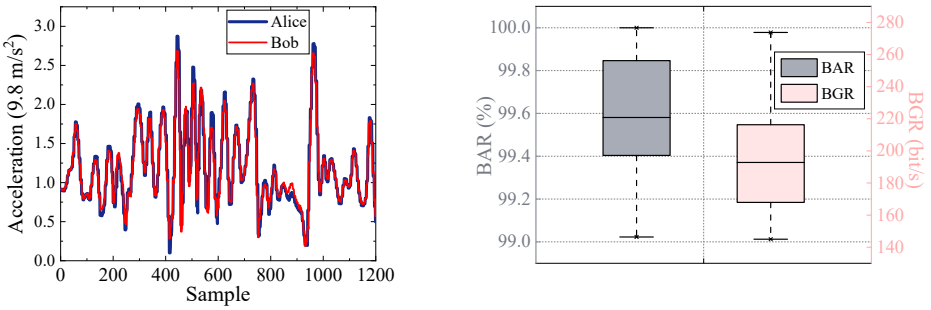
**Impact of peak screening and reconciliation method.** We evaluate our peak screening algorithm and the information reconciliation method. As discussed earlier, the peak-to-peak trends of Alice's and Bob's MFV signal measurements cannot be accurately matched due to the effects of noise and sudden movement. Therefore, we propose a peak screening method for initial screening, followed by information reconciliation to correct the mismatched bits between the keys of the two devices. We present the bit agreement and bit generation rates under various conditions consisting of four scenarios: Neither the peak screening nor the fuzzy commitment is used, only peak screening is used without fuzzy commitment, only fuzzy commitment is used without peak screening, and both peak screening and fuzzy commitment are used simultaneously.

Figure 21 presents the bit agreement rate and bit generation rate for all four cases. As can be seen from Figure 21, the bit agreement rate is only 77.6% and the bit generation rate is 0.96bit/s when peak screening and fuzzy




(a) BAR (b) BGR

Fig. 21. The effect of the screening and key reconciliation method.




(a) motion (b) motion effect

Fig. 22. Magkey performance under motion.

commitment are not used. On the other hand, when peak screening is used without fuzzy commitment technique, the bit agreement rate increases to 82.5% while the bit generation rate is 0.84 bit/s because some bits are filtered by the screening method. When the fuzzy commitment technique is used without peak screening, the bit agreement rate increases further to 88.2%, but is still below 90% because the number of mismatched bits exceeds the error correction capability of ECC. As a result, some of the mismatched bits between Alice and Bob cannot be corrected. And the bit generation rate increases to 1.09 bit/s. Finally, when both peak screening and fuzzy commitment technique are used, the bit agreement rate increases to 94.2%. On the other hand, the bit generation rate reaches 0.96bit/s.

**Impact of motion.** Key generation using motion signals has been studied extensively. However, it requires some effort on the part of the user, which increases the burden on the user. A recent accelerometer-based estimation from a large or population representative study suggests that adults spend about 8.2 hours per day sitting still (range 4.9-11.9 hours/day) [44]. In addition, according to a recent survey, adults (≥ 18 years) reported a mean ± s.d. time in bed of 7.8 ± 0.9h [45]. Our system works well for key generation when the person is stationary and can be integrated with the accelerometers so that motion signals can be used to generate keys, and we conduct experiments to demonstrate this. Most wearable devices are now equipped with accelerometers, and the potential of accelerometers to capture motion signals and use them for key generation has been studied extensively. Our

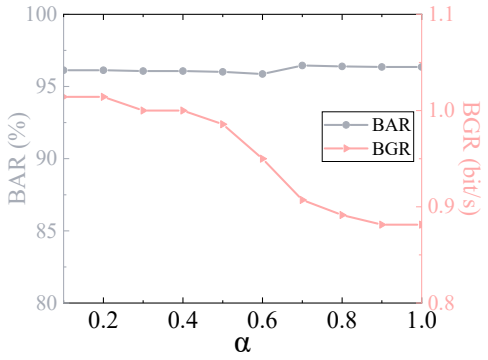



Fig. 23. Magkey performance under different parameter $\alpha$.

method uses heartbeat signals from the GMR sensor for key generation during stationary periods. When the accelerometer detects wrist motion of the user wearing both the GMR sensor and the accelerometer, it switches to motion mode. The key generation process is based on the magnitude of the acceleration signal, initiated upon detecting wrist movement, as illustrated in Figure 22a. The magnitude of the acceleration signals is calculated by $\text{Acc} = \sqrt{a_x^2 + a_y^2 + a_z^2}$, where $a_x$, $a_y$, $a_z$ are the values of the acceleration in the X, Y and Z directions in the triaxial accelerometer, respectively. To generate the key, we first extract the acceleration signal from the first peak to synchronize the two devices. The traditional guard band-based quantization method [46] is used for quantization, and the combination of the index-based method [47] and the fuzzy commitment is used for reconciliation. We evaluate the bit agreement rate and the bit generation rate of this approach, as shown in Figure 22b. The average bit agreement rate is 99.6% and the average bit generation rate is 192.8 bit/s.

**Impact of parameter $\alpha$.** We investigate the impact of the threshold scaling factor $\alpha$ on the performance of MagKey. The result is shown in Figure 23. When peak screening is used, the bit agreement rate increases from 96.1% to 96.4% as the threshold scaling factor $\alpha$ in the peak screening algorithm increases, while the bit generation rate decreases from 1.01bit/s to 0.88bit/s as the threshold scaling factor $\alpha$ increases, as more potentially mismatched bits are discarded. Additionally, to balance BAG and BGR, we choose $\alpha = 0.2$ in our setting based on the result.

## 4.4 Randomness

In addition, we further test the randomness of all 128-bit keys after reconciliation using the popular NIST statistical test suite [48]. The results of the tests are shown in the Table 2. The p-value in the table indicates the probability that the data set was generated by a random process. If the p-value is less than 0.01, then the assumption of randomness is rejected. All p-values are greater than 0.01, so the generated key sequence passes the NIST randomness test. Next, we calculate the entropy of the generated keys, which is about 0.998. Therefore, the MFV signal is suitable to be extracted as a cryptographic key.

## 4.5 Power Consumption

The power consumption of the MagKey consists of five components: the GMR sensor, the analog front-end (which includes the voltage amplifier, filter, and voltage lifting circuit), the ADC, the MCU, and the reconciliation process. We use the Rigol DP932A [49] to measure the power consumption of these main components. Table 3 summarizes the power consumption for each component of the MagKey.

Table 2. NIST Test Results

| NIST TEST | p-value |
|---|---|
| Frequency | 0.075363 |
| Block Frequency | 0.895171 |
| Runs | 0.180275 |
| Longest Run | 0.092219 |
| Binary matrix rank | 0.068101 |
| DFT | 0.043038 |
| Non overlapping template matching | 0.213689 |
| Serial | 0.592685 |
| Cumulative sums | 0.150727 |
| Random Excursions | 0.615498 |
| Random Excursions Variant | 0.087197 |

To accurately measure the power consumption of the MagKey implemented on the CC2650 LaunchPad, we first establish a baseline by recording the power readings after the MCU's startup. This baseline allows us to subtract the initial power consumption from subsequent readings, enabling us to isolate and analyze the power consumed specifically by the ADC and reconciliation processes.

The power consumed by the GMR sensor, analog front-end, ADC, MCU, and reconciliation is 3.63 mW, 34.98 mW, 2.64 mW, 0.033 mW, and 55.44 mW. Since the average bit generation rate of MagKey is about 1 bit/s, it takes about 128 seconds to generate a 128-bit key, and the reconciliation process takes about 1.8 seconds, resulting in a total power consumption of about 5.294 J to generate a 128-bit key. On the other hand, when the MagKey is idle, it consumes only 0.033mW of power. Given a pair of AA batteries with a capacity of 8,140 mWh (i.e. 29,304 J), the MagKey can operate for up to 5,413 hours (approximately 7.5 months), assuming that key generation is performed once an hour. However, it is important to note that the MagKey does not need to be active all the time, as key generation is only required during the transfer of sensitive information.

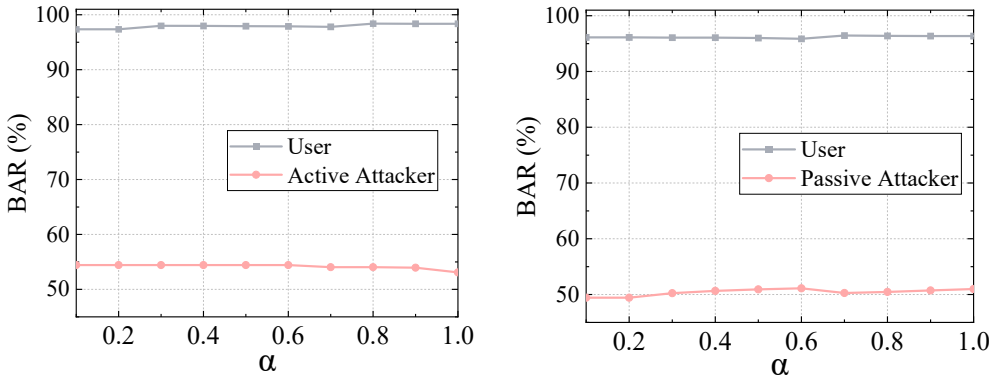
Table 3. Power consumption of each component in MagKey.

| Component | GMR sensor | Analog front-end | ADC | MCU | Reconciliation | Total |
|---|---|---|---|---|---|---|
| Power (mW) | 3.63 | 34.98 | 2.64 | 0.033 | 55.44 | N/A |
| Time (s) (generation of a 128-bit key) | 128 | 128 | 128 | 128 | 0.2 | N/A |
| Energy (J) | 0.464 | 4.477 | 0.338 | 0.004 | 0.011 | 5.294 |

## 5 THREAT MODEL AND PERFORMANCE ANALYSIS

### 5.1 Active Attacks

To illustrate a potential security breach, it is possible for an attacker to gain access to a user's historical peak-to-peak trend data. This can be done by Eve submitting a key that has been generated from the historical data when attempting to pair with an authorized device. To combat this type of attack, the key generated by MagKey ought to offer forward secrecy. To simulate this, we split each user's data into two parts. The former part is the historical data, which is used to pair with the latter. These two parts represent data measured by the same user at




(a) BAR under active attack

(b) BAR under passive attack

Fig. 24. BAR under different attacks.

different times. According to Figure 24a, the maximum bit agreement rate of 54.3% shows that the peak-to-peak trends over time are quite random, confirming the security of MagKey against this type of attack.

### 5.2 Passive Attacks

The passive attacker, with knowledge of the key generation mechanism, is able to monitor the communication between Alice and Bob. By eavesdropping on the key generation dialog, Eve attempts to pair authorized devices with keys generated from her own MFV signal peak-to-peak data. To thwart this attack, MagKey must guarantee that each user's extracted key is unique. Next, we simulate this scenario by pairing devices placed on the same part of the body between different people. When exchanging messages, Alice and Bob only exchange the indexes of the samples. If an attacker tries to impersonate Alice to communicate with Bob, their samples can easily be converted to different bits due to the difference in MFV signal data between Bob and the attacker. As shown in Figure 24b, the highest bit agreement rate between the attacker and Bob is only 52.2%, which is much lower than the bit agreement rate between legitimate users. It is difficult for the attacker to generate a key that matches the legitimate user's key.

## 6 RELATED WORK

We review research topics relevant to MagKey in this section.

**Key generation method based on heartbeat signals.** Heartbeat signals have great potential for use in authentication and key generation schemes within Wireless Body Area Networks (WBAN) because heartbeat signals carry unique characteristics of an individual, such as cardiac function information [50]. In addition, heartbeat signals can be collected and analyzed by various sensors. Commonly used sensors include electrocardiography (ECG) and photoplethysmography (PPG) sensors. ECG sensors collect the electrical activity of the heart muscle through electrodes attached to the chest, providing information on heart rhythm and ECG waveforms, Rostami *et al.* use ECG to acquire heartbeat signals and extract the four least significant bits of an inter-pulse interval (IPI) for cryptographic device pairing [22]. Xu *et al.* use ECG to acquire heartbeat signals for key generation to protect implantable medical devices [51]. The PPG sensor, on the other hand, can be placed on the ear, finger, *etc.*, and detects heartbeat signals by irradiating body tissues and measuring changes in light absorption by blood in microvessels [52], Zhang *et al.* use PPG to acquire heartbeat signals and extract a bit from the trend of an IPI for key generation [6]. In addition, seismocardiography (SCG) enables the measurement of heartbeat signals

by monitoring the response of the chest to cardiac systole and diastole. Wang *et al.* measure SCG signals for authentication using a device equipped with an accelerometer sensor [53]. Heart rate variability (HRV) [54] and inter-pulse intervals (IPIs) [8, 22] can be extracted from the heartbeat signals. These features can be used for authentication and key generation. However, the aforementioned key generation and authentication methods using heartbeat signals have inherent drawbacks, e.g. ECG requires complex electrodes, PPG is affected by body fluids and skin tones, and SCG measurement may require wearing a strap on the chest, resulting in non-portability or discomfort.

**Key generation method based on channel information or body signals.** Revadiga *et al.* utilize the fading characteristics of the wireless channel between the two devices, i.e., the received signal strength indicator, to extract the secret key [55]. Channel state information is also used for key generation [56]. Lee *et al.* present an over-the-air device authentication scheme that leverages ambient electromagnetic radiation [57]. Wei *et al.* propose a cross-sensor symmetric key generation system that collects inertial measurements from motion sensors and acoustic measurements from microphones, respectively, and generates keys using inertial and acoustic measurements [58]. Yan *et al.* use induced body electric potentials (iBEPs) for authentication [59], while Miao *et al.* use skin electric potential (SEP) for key generation [5]. Zhao *et al.* capture common hand movements during handshaking using accelerometers for secure pairing [60]. Pourbemany *et al.* propose the use of respiratory inductive volumetric tracing and accelerometers for breath pairing, ensuring that the devices are part of the same body area network [61].

**GMR sensor applications.** Researchers have come up with the idea of using biomagnetism as a way to monitor human vital signs, mainly through GMR sensors that measure induced biomagnetic field signals. GMR sensors are increasingly being used to monitor vital signs such as heart rate [26, 27], respiration [32], and blood pressure [62]. Bai *et al.* explore how to make the maximum coupling between magnetic flux and arterial blood in a magneto plethysmo gram sensor head [34]. Lee *et al.* investigate the application of a Magneto-Plethysmographic sensor to measure the velocity of peripheral blood flow. The results showed a strong correlation between the sensor measurements and ultrasound Doppler measurements [63]. Guo *et al.* present a biomagnetism-based vital signs monitoring system that can monitor the heart rate and respiration rate of users [35, 64].

Previous research has demonstrated the feasibility of using GMR sensors for vital signs monitoring, which is essentially based on biomagnetic sensing. Differently, our study focuses on the utilization of MFV signals from the GMR sensor for key generation.

## 7 DISCUSSION

**Stationary setup.** MagKey requires a stationary setup. It is important to note that this setup is a prerequisite for utilizing the Ballistocardiography (BCG) signal and other signals generated by heart movements (e.g., SCG, ECG). As a result, existing BCG-related studies typically collect data under resting conditions, such as lying down, sitting, or standing still [28–31]. Moreover, it is important to highlight that heartbeat-based key generation schemes are particularly fragile to motion artifacts [8, 23], as additional movement can easily affect the sensed heartbeat signal. To address this issue, we propose to incorporate an accelerometer as a complementary device.

**Errors in the resistance value of the GMR element.** While variations in resistance occur due to hardware imperfections in GMR sensors, once the sensor is produced, its resistance value becomes fixed under a specific magnetic field. Our system utilizes the output variations of the GMR sensor to quantify and generate the key. Additionally, among various factors, temperature has a greater impact on the resistance of the GMR [65], resulting in changes in the output voltage. However, the Wheatstone bridge structure of the GMR sensor includes a self-contained temperature compensation function. As a result, the output voltage change due to a temperature change of 3°C is less than 1 mV when the supply voltage is 3.3 V [39]. In contrast, the average voltage change caused by skin surface displacement due to the heartbeat is about ±30 mV.

Given that we rely on the trend of the peak-to-peak values of adjacent heartbeats to generate keys, and considering that the average duration of a heartbeat interval is around 0.8 s, if the GMR sensor experiences a temperature change of ±3°C within this timeframe, the resultant change in peak-to-peak value would be about ±1 mV. Importantly, in typical usage scenarios where the device is worn on the body, extreme temperature changes within such short timeframes are unlikely. Even if the GMR sensor were to experience a significant temperature difference within such short timeframes, calculations indicate that our system would only record a misjudgment at a lower threshold $Th_1$ of 0.3 if the temperature difference experienced by the GMR exceeds 60°C within 0.8 s.

Our GMR sensors are typically placed on the skin's surface, where the normal temperature range is narrow—generally between 36.6°C and 37.2°C, even sweating and exercise or having a fever will cause only a small temperature change of less than 3°C due to thermoregulation [66], so the output voltage change of the GMR sensor caused by temperature change is negligible. Finally, our peak-to-peak screening can further mitigate any influence of temperature variations by filtering out peaks with variations below the lower threshold $Th_1$.

Therefore, we believe that both manufacturing imperfections and temperature variations have a negligible impact on the performance of the system.

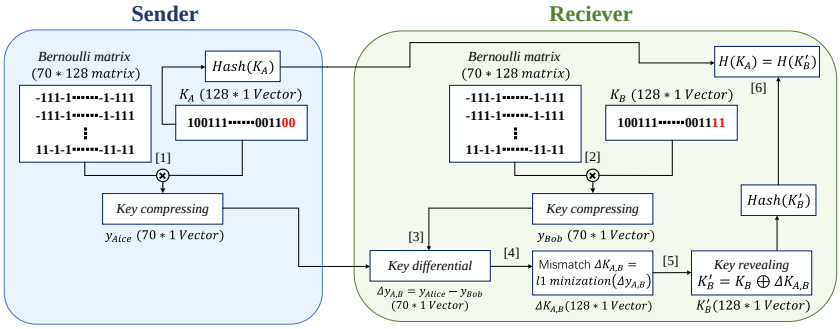



Fig. 25. Compressed sensing-based reconciliation.

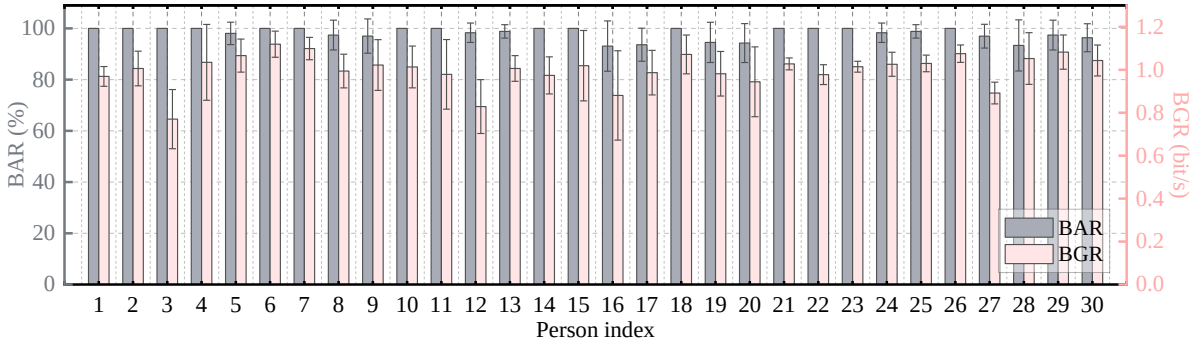



Fig. 26. Overall performance with Compressed sensing-based reconciliation.

**Improving the BGR and BAR.** To improve the BAR and BGR, we employ a compressed sensing-based reconciliation method in the key generation process, a technique widely utilized in key reconciliation processes [8, 46, 67]. We replace the reconciliation method from fuzzy commitment-based reconciliation to compressed sensing-based

reconciliation, everything else remains the same. The compressed sensing-based reconciliation process is shown in Fig. 25. We evaluate the bit agreement rate and the bit generation rate of the key generation process of 30 volunteers, as shown in Figure 26. MagKey performed well across all 30 participants, with an average bit agreement rate of 98.2% (a 4% improvement compared to 94.2% with fuzzy commitment) and an average bit generation rate of 1.0 bits/s (a 0.04 bit/s improvement compared to 0.96 bit/s with fuzzy commitment).

## 8 CONCLUSION

In this study, we introduce MagKey, a pioneering endeavor aimed at exploring the viability of BCG-based key generation for wearable devices. MagKey addresses the challenges associated with effective BCG sensing by innovatively converting skin vibration resulting from recoil forces into magnetic field vibration (MFV). Our research underscores that the peak-to-peak trend (PPT) of MFV signals serves as a dependable source for key extraction, thereby enhancing the key generation rate. To counteract the influence of noise and motion artifacts on key generation, MagKey devises a robust signal processing pipeline. We implement a prototype of MagKey and conduct comprehensive experiments to assess its performance across diverse scenarios. Additionally, we conduct thorough security analyses to validate MagKey's resilience against various potential attacks. Through these efforts, MagKey not only advances the frontier of BCG-based key generation, but also lays a foundation for secure and efficient wearable device pairing.

## ACKNOWLEDGMENTS

This work was supported in part by the "Pioneer" and "Leading Goose" R&D Program of Zhejiang Program under Grant 2025C02043, in part by the Fundamental Research Funds for the Central Universities under Grant 226-2024-00004, 226-2023-00111, in part by the National Science Fund of China (NSFC) under Grant 62472379, Grant 62394341, and Grant 62394344, and in part by the Key Research and Development Program of Zhejiang Program under Grant 2024C01065. Xiuzhen Guo is the corresponding author.

## REFERENCES

[1] Nico Surantha, Prabadinata Atmaja, Maulana Wicaksono, et al. A review of wearable internet-of-things device for healthcare. *Procedia Computer Science*, 179:936–943, 2021.

[2] Yongjie Yang, Tao Chen, Yujing Huang, Xiuzhen Guo, and Longfei Shangguan. Maf: Exploring mobile acoustic field for hand-to-face gesture interactions. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–20, 2024.

[3] Allied Market Research. https://www.alliedmarketresearch.com/body-adapted-wearable-electronics-market.

[4] Haotian Jiang, Jiacheng Zhang, Xiuzhen Guo, and Yuan He. Sense me on the ride: Accurate mobile sensing over a lora backscatter channel. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, pages 125–137, 2021.

[5] Yuchen Miao, Chaojie Gu, Zhenyu Yan, Sze Yiu Chau, Rui Tan, Qi Lin, Wen Hu, Shibo He, and Jiming Chen. Touchkey: Touch to generate symmetric keys by skin electric potentials induced by powerline radiation. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 7(2):1–21, 2023.

[6] Junqing Zhang, Yushi Zheng, Weitao Xu, and Yingying Chen. H2k: A heartbeat-based key generation framework for ecg and ppg signals. *IEEE Transactions on Mobile Computing*, 22(2):923–934, 2023.

[7] Lin Yang, Wei Wang, and Qian Zhang. Secret from muscle: Enabling secure pairing with electromyography. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pages 28–41, 2016.

[8] Qi Lin, Weitao Xu, Jun Liu, Abdelwahed Khamis, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. H2b: Heartbeat-based secret key generation using piezo vibration sensors. In *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, pages 265–276, 2019.

[9] Selcan Kaplan Berkaya, Alper Kursat Uysal, Efnan Sora Gunal, Semih Ergin, Serkan Gunal, and M Bilginer Gulmezoglu. A survey on ecg analysis. *Biomedical Signal Processing and Control*, 43:216–235, 2018.

[10] Andriy Temko. Accurate heart rate monitoring during physical exercises using ppg. *IEEE Transactions on Biomedical Engineering*, 64(9): 2016–2024, 2017.

[11] Amirtahà Taebi, Brian E Solar, Andrew J Bomar, Richard H Sandler, and Hansen A Mansy. Recent advances in seismocardiography. *Vibration*, 2(1):64–86, 2019.

[12] Mohamed Abul Hassan, Aamir Saeed Malik, David Fofi, Naufal Mohamed Saad, Yasir S Ali, and Fabrice Meriaudeau. Video-based heartbeat rate measuring method using ballistocardiography. *IEEE Sensors Journal*, 17(14):4544–4557, 2017.

[13] David Da He, Eric S Winokur, and Charles G Sodini. An ear-worn vital signs monitor. *IEEE Transactions on Biomedical Engineering*, 62 (11):2547–2552, 2015.

[14] Weidong Gao and Zhenwei Zhao. Extraction of heart beat feature based on ballistocardiogram signal from multi-channel piezoelectric ceramic sensors. *IEEE Sensors Journal*, 2022.

[15] Tal Klap and Zvika Shinar. Using piezoelectric sensor for continuous-contact-free monitoring of heart and respiration rates in real-life hospital settings. In *Computing in Cardiology 2013*, pages 671–674. IEEE, 2013.

[16] Ziran He, Min Wang, Qingsong Xie, Guoxing Wang, Yang Zhao, Yong Lian, Bo Meng, and Zhengchun Peng. A heart rate measurement system based on ballistocardiogram for smart furniture. In *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, pages 151–154. IEEE, 2018.

[17] Inc. Measurement Specialties. Ldt0-028k piezo vibration rev 1. URL https://media.digikey.com/pdf/Data%20Sheets/Measurement%20Specialties%20PDFs/LDT0-028K.pdf.

[18] Carmen CY Poon, Yuan-Ting Zhang, and Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, 2006.

[19] Shu-Di Bao, Carmen CY Poon, Yuan-Ting Zhang, and Lian-Feng Shen. Using the timing information of heartbeats as an entity identifier to secure body sensor network. *IEEE transactions on information technology in biomedicine*, 12(6):772–779, 2008.

[20] Paul A Obrist. *Cardiovascular psychophysiology: A perspective*. Springer Science & Business Media, 2012.

[21] Hassan Chizari and Emil Lupu. Extracting randomness from the trend of ipi for cryptographic operations in implantable medical devices. *IEEE Transactions on Dependable and Secure Computing*, 18(2):875–888, 2019.

[22] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. Heart-to-heart (h2h) authentication for implanted medical devices. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1099–1112, 2013.

[23] Robert M Seepers, Jos H Weber, Zekeriya Erkin, Ioannis Sourdis, and Christos Strydis. Secure key-exchange protocol for implants using heartbeats. In *Proceedings of the ACM International Conference on Computing Frontiers*, pages 119–126, 2016.

[24] Brinnae Bent, Benjamin A Goldstein, Warren A Kibbe, and Jessilyn P Dunn. Investigating sources of inaccuracy in wearable optical heart rate sensors. *NPJ digital medicine*, 3(1):18, 2020.

[25] Xiuzhen Guo, Long Tan, Tao Chen, Chaojie Gu, Yuanchao Shu, Shibo He, Yuan He, Jiming Chen, and Longfei Shangguan. Exploring biomagnetism for inclusive vital sign monitoring: Modeling and implementation. 2024.

[26] K Jishnu and CS Anoop. A simple bio-instrumentation platform for vital-sign estimation using magnetopleythsmography. In *2023 International Conference on Power, Instrumentation, Energy and Control (PIECON)*, pages 1–5. IEEE, 2023.

[27] Kubera Kalyan, Vinit Kumar Chugh, and CS Anoop. Non-invasive heart rate monitoring system using giant magneto resistance sensor. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 4873–4876. IEEE, 2016.

[28] Niccolo Mora, Federico Cocconcelli, Guido Matrella, and Paolo Ciampolini. Accurate heartbeat detection on ballistocardiogram accelerometric traces. *IEEE Transactions on Instrumentation and Measurement*, 69(11):9000–9009, 2020.

[29] Carlos Alvarado-Serrano, Pablo Samuel Luna-Lozano, and Ramon Pallàs-Areny. An algorithm for beat-to-beat heart rate detection from the bcg based on the continuous spline wavelet transform. *Biomedical Signal Processing and Control*, 27:96–102, 2016.

[30] Qingsong Xie, Min Wang, Yang Zhao, Ziran He, Yongfu Li, Guoxing Wang, and Yong Lian. A personalized beat-to-beat heart rate detection system from ballistocardiogram for smart home applications. *IEEE transactions on biomedical circuits and systems*, 13(6): 1593–1602, 2019.

[31] Masaki Nagura, Yasue Mitsukura, Taishiro Kishimoto, and Masaru Mimura. A practical bcg measuring system with bed sensors and algorithm for heartbeat detection. In *2018 IEEE 15th International Workshop on Advanced Motion Control (AMC)*, pages 317–321. IEEE, 2018.

[32] Vinit Kumar Chugh, Kubera Kalyan, and CS Anoop. Feasibility study of a giant magneto-resistance based respiration rate monitor. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 2327–2330. IEEE, 2016.

[33] Chee Teck Phua, Gaëlle Lissorgues, Boon Chong Gooi, and Bruno Mercier. Statistical validation of heart rate measurement using modulated magnetic signature of blood with respect to electrocardiogram. *International Journal of Bioscience, Biochemistry and Bioinformatics (IJBBB)*, 2(2), 2012.

[34] J Rezuana Bai and V Jagadeesh Kumar. Optimal design to ensure maximum coupling between magnetic flux and arterial blood in a magneto plethysmo gram sensor head. *IEEE Sensors Journal*, 21(2):1417–1423, 2020.

[35] Xiuzhen Guo, Long Tan, Tao Chen, Chaojie Gu, Yuanchao Shu, Shibo He, Yuan He, Jiming Chen, and Longfei Shangguan. Exploring biomagnetism for inclusive vital sign monitoring: Modeling and implementation. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pages 1–15, 2024.

[36] Biomagnetism. https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/biomagnetism.

[37] SparkFun Electronics. Pulse sensor. URL https://pulsesensor.com/.

[38] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36, 1999.

[39] GMR IC AA002. https://www.digikey.cn/zh/products/detail/nve-corp-sensor-products/aa002-02e/1624601.

[40] Instrumentation amplifier INA126. https://www.ti.com/lit/ds/symlink/ina126.pdf.

[41] Ultralow Offset Voltage Operational Amplifier OP07. https://www.ti.com/lit/ds/symlink/op07.pdf?ts=1699800019783&ref_url=https%253A%252F%252Fwww.ti.com.cn%252Fproduct%252Fcn%252FOP07.

[42] Magnet Safety: Continuous Exposure Limits Guidelines. https://blink.ucsd.edu/safety/radiation/magnet/limits.html.

[43] Pacemaker Safety. https://www.kjmagnetics.com/blog.asp?p=pacemaker-safety.

[44] Adrian E Bauman, Christina B Petersen, Kim Blond, Vegar Rangul, and Louise L Hardy. The descriptive epidemiology of sedentary behaviour. *Sedentary behaviour epidemiology*, pages 73–106, 2018.

[45] Desana Kocevska, Thom S Lysen, Aafje Dotinga, M Elisabeth Koopman-Verhoeff, Maartje PCM Luijk, Niki Antypa, Nienke R Biermasz, Anneke Blokstra, Johannes Brug, Wiliam J Burk, et al. Sleep characteristics across the lifespan in 1.1 million people from the netherlands, united kingdom and united states: a systematic review and meta-analysis. *Nature human behaviour*, 5(1):113–122, 2021.

[46] Qi Lin, Weitao Xu, Guohao Lan, Yesheng Cui, Hong Jia, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. Kehkey: Kinetic energy harvester-based authentication and key generation for body area network. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 4(1):1–26, 2020.

[47] Weitao Xu, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 1–12. IEEE, 2016.

[48] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, volume 22. US Department of Commerce, Technology Administration, National Institute of . . . , 2001.

[49] RIGOL DC power supply DP932. https://www.rigol.eu/products/dc-power/dp900.html.

[50] Tao Chen, Yongjie Yang, Xiaoran Fan, Xiuzhen Guo, Jie Xiong, and Longfei Shangguan. Exploring the feasibility of remote cardiac auscultation using earphones. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, pages 357–372, 2024.

[51] Fengyuan Xu, Zhengrui Qin, Chiu C Tan, Baosheng Wang, and Qun Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *2011 Proceedings IEEE INFOCOM*, pages 1862–1870. IEEE, 2011.

[52] Kirk H Shelley. Photoplethysmography: beyond the calculation of arterial oxygen saturation and heart rate. *Anesthesia & Analgesia*, 105 (6):S31–S36, 2007.

[53] Lei Wang, Kang Huang, Ke Sun, Wei Wang, Chen Tian, Lei Xie, and Qing Gu. Unlock with your heart: Heartbeat-based authentication on commercial mobile phones. *Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies*, 2(3):1–22, 2018.

[54] Sai Kiran Cherupally, Shihui Yin, Deepak Kadetotad, Chisung Bae, Sang Joon Kim, and Jae-sun Seo. A smart hardware security engine combining entropy sources of ecg, hrv, and sram puf for authentication and secret key generation. *IEEE Journal of Solid-State Circuits*, 55(10):2680–2690, 2020.

[55] Girish Revadigar, Chitra Javali, Wen Hu, and Sanjay Jha. Dlink: Dual link based radio frequency fingerprinting for wearable devices. In *2015 IEEE 40th Conference on Local Computer Networks (LCN)*, pages 329–337. IEEE, 2015.

[56] Zhouzhou Li, Honggang Wang, and Hua Fang. Group-based cooperation on symmetric key generation for wireless body area networks. *IEEE Internet of Things Journal*, 4(6):1955–1963, 2017.

[57] Kyuin Lee, Yucheng Yang, Omkar Prabhune, Aishwarya Lekshmi Chithra, Jack West, Kassem Fawaz, Neil Klingensmith, Suman Banerjee, and Younghyun Kim. Aerokey: Using ambient electromagnetic radiation for secure and usable wireless device authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(1):1–29, 2022.

[58] Bo Wei, Weitao Xu, Kai Li, Chengwen Luo, and Jin Zhang. i 2 key: A cross-sensor symmetric key generation system using inertial measurements and inaudible sound. In *2022 21st ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 183–194. IEEE, 2022.

[59] Zhenyu Yan, Qun Song, and Rui Tan. Touch-to-access device authentication for indoor smart objects. *IEEE Transactions on Mobile Computing*, 2021.

[60] Guichuan Zhao, Qi Jiang, Xiaohan Huang, Xindi Ma, Youliang Tian, and Jianfeng Ma. Secure and usable handshake based pairing for wrist-worn smart devices on different users. *Mobile Networks and Applications*, pages 1–16, 2021.

[61] Jafar Pourbemany, Ye Zhu, and Riccardo Bettati. Breathe-to-pair (b2p) respiration-based pairing protocol for wearable devices. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 188–200, 2022.

[62] Vinit Kumar Chugh, Kubera Kalyan, CS Anoop, Amit Patra, and Shubham Negi. Analysis of a gmr-based plethysmograph transducer and its utility for real-time blood pressure measurement. In *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 1704–1707. IEEE, 2017.

[63] Young-Jae Lee, Chung-Keun Lee, Minsoo Kang, Seung-Jin Kang, Kyung-Nam Kim, Kyungho Kim, Kyeong-Seop Kim, and Jeong-Whan Lee. Magneto-plethysmographic sensor for peripheral blood flow velocity. *IEEE Sensors journal*, 14(5):1341–1342, 2014.
[64] Xiuzhen Guo, Long Tan, Chaojie Gu, Yuanchao Shu, Shibo He, and Jiming Chen. Magwear: Vital sign monitoring based on biomagnetism sensing. *IEEE Transactions on Mobile Computing*, 2024.
[65] Puja Dey, Jitendra Nath Roy, Puja Dey, and Jitendra Nath Roy. Giant magnetoresistance (gmr). *Spintronics: Fundamentals and Applications*, pages 75–101, 2021.
[66] William Bierman. The temperature of the skin surface. *Journal of the American Medical Association*, 106(14):1158–1162, 1936.
[67] Bo Wei, Weitao Xu, Mingcen Gao, Guohao Lan, Kai Li, Chengwen Luo, and Jin Zhang. Solarkey: Battery-free key generation using solar cells. *ACM Transactions on Sensor Networks*, 20(1):1–24, 2023.