Using Vibration for Secure Pairing with Implantable Medical Devices: Development and Usability Study

Mo Zhang, Chaofan Wang, Weiwei Jiang, David Oswald, Toby Murray, Eduard Marin, Jing Wei, Mark Ryan, Vassilis Kostakos

Submitted to: JMIR Biomedical Engineering
on: February 05, 2024

Table of Contents

Using Vibration for Secure Pairing with Implantable Medical Devices: Development and Usability Study

Mo Zhang[1, 2] MSCS; Chaofan Wang[3] PhD; Weiwei Jiang[4] PhD; David Oswald[2] PhD; Toby Murray[1] PhD; Eduard Marin[5] PhD; Jing Wei[1] PhD; Mark Ryan[2] PhD; Vassilis Kostakos[1] PhD

[1]School of Computing and Information Systems The University of Melbourne Melbourne AU
[2]School of Computer Science University of Birmingham Birmingham GB
[3]College of Computer Science and Artificial Intelligence Wenzhou University Wenzhou CN
[4]Nanjing University of Information Science and Technology Nanjing CN
[5]Telefonica Research Spain Barcelona ES

Corresponding Author:
Mo Zhang MSCS
School of Computing and Information Systems
The University of Melbourne
Melbourne Connnect
700 Swanston Street, Carlton
Melbourne
AU

Abstract

Background: Implantable Medical Devices (IMDs), such as pacemakers, increasingly communicate wirelessly with external devices. To secure this wireless communication channel, a pairing process is needed to bootstrap a secret key between the devices. Previous work has proposed pairing approaches that often adopt a “seamless” design and render the pairing process imperceptible to patients. This lack of user perception can significantly compromise security and pose threats to patients.

Objective: The objective of this work is to explore the use of highly perceptible vibrations for pairing with IMDs. We aim to propose a novel technique that leverages the natural randomness in human motor behavior as a shared source of entropy for pairing, potentially deployable to current IMD products.

Methods: We develop a proof-of-concept to demonstrate our proposed technique. We build a wearable prototype designed for individuals to simulate being an IMD patient (we do not test on real patients to avoid potential risks), and devise signal processing algorithms that utilize accelerometer readings to facilitate secure pairing with an IMD. We thoroughly evaluate the accuracy, security, and usability of our technique in a lab study with 24 participants.

Results: Our proposed pairing technique achieves high pairing accuracy, with a zero false acceptance rate (indicating low risks from adversaries) and a false rejection rate of only 0.6% (suggesting that legitimate users will likely experience very few failures). Our approach also offers robust security, which passes the National Institute of Standards and Technology statistical tests (with all p-values > 0.01). Moreover, our technique has high usability, evidenced by an average System Usability Scale questionnaire score of 73.6 (surpassing the standard benchmark of 68 for "good usability") and insights gathered from the interviews. Furthermore, the entire pairing process can be efficiently completed within five seconds.

Conclusions: Vibration can be used to realize secure, usable, and deployable pairing in the context of IMDs. Our method also exhibits advantages over previous approaches, e.g., lenient requirements on the sensing capabilities of IMDs and the synchronization between the IMD and the external device.

(JMIR Preprints 05/02/2024:57091)
DOI: https://doi.org/10.2196/preprints.57091

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?
✓ **Please make my preprint PDF available to anyone at any time (recommended).**

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✔ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Original Paper

Mo Zhang, M.Sc., mo.zhang@student.unimelb.edu.au, 0000-0002-7302-9088, School of Computing and Information Systems, The University of Melbourne; School of Computer Science, University of Birmingham
Chaofan Wang, Ph.D., chaofanas@gmail.com, 0000-0001-8213-6582, College of Computer Science and Artificial Intelligence, Wenzhou University
Weiwei Jiang, Ph.D., weiweijiangcn@gmail.com, 0000-0003-4413-2497, Nanjing University of Information Science and Technology
David Oswald, Ph.D., d.f.oswald@bham.ac.uk, 0000-0001-8524-5282, School of Computer Science, University of Birmingham
Toby Murray, Ph.D., toby.murray@unimelb.edu.au, 0000-0002-8271-0289, School of Computing and Information Systems, The University of Melbourne
Eduard Marin, Ph.D., eduard.marinfabregas@telefonica.com, 0000-0002-5002-0187, Telefonica Research Spain
Jing Wei, Ph.D., jwwei2@student.unimelb.edu.au, 0000-0002-8522-8607, School of Computing and Information Systems, The University of Melbourne
Mark Ryan, Ph.D., m.d.ryan@bham.ac.uk, 0000-0002-1632-497X, School of Computer Science, University of Birmingham
Vassilis Kostakos, Ph.D., vassilis.kostakos@unimelb.edu.au, 0000-0003-2804-6038, School of Computing and Information Systems, The University of Melbourne

Using Vibration for Secure Pairing with Implantable Medical Devices: Development and Usability Study

Abstract

Background: Implantable Medical Devices (IMDs), such as pacemakers, increasingly communicate wirelessly with external devices. To secure this wireless communication channel, a pairing process is needed to bootstrap a secret key between the devices. Previous work has proposed pairing approaches that often adopt a “seamless” design and render the pairing process imperceptible to patients. This lack of user perception can significantly compromise security and pose threats to patients.
Objective: The objective of this work is to explore the use of highly perceptible vibrations for pairing with IMDs. We aim to propose a novel technique that leverages the natural randomness in human motor behavior as a shared source of entropy for pairing, potentially deployable to current IMD products.
Methods: We develop a proof-of-concept to demonstrate our proposed technique. We build a wearable prototype designed for individuals to simulate being an IMD patient (we do not test on real patients to avoid potential risks), and devise signal processing algorithms that utilize accelerometer readings to facilitate secure pairing with an IMD. We thoroughly evaluate the accuracy, security, and usability of our technique in a lab study with 24 participants.
Results: Our proposed pairing technique achieves high pairing accuracy, with a zero false acceptance rate (indicating low risks from adversaries) and a false rejection rate of only 0.6% (suggesting that legitimate users will likely experience very few failures). Our approach also offers robust security, which passes the National Institute of Standards and Technology statistical tests (with all p-values > 0.01). Moreover, our technique has high usability, evidenced by an average System Usability Scale questionnaire score of 73.6 (surpassing the standard benchmark of 68 for "good usability") and insights gathered from the interviews. Furthermore, the entire pairing process can be efficiently completed within five seconds.
Conclusions: Vibration can be used to realize secure, usable, and deployable pairing in the context

of IMDs. Our method also exhibits advantages over previous approaches, e.g., lenient requirements on the sensing capabilities of IMDs and the synchronization between the IMD and the external device.

Keywords: Implantable medical device; Pairing; Vibration; Security; Usability

Introduction

Background

Implantable Medical Devices (IMDs), such as pacemakers, implantable cardioverter defibrillators, or insulin pumps are widely deployed and evolving at a rapid pace [64]. Due to their form factors and use cases, modern IMDs typically rely on a wireless interface to communicate with external devices. For instance, doctors use programmer devices to reprogram the patient's IMD (e.g., to change the patient's therapy) and gather telemetry data. Such wireless connectivity can bring about much convenience to patients and doctors. However, it also poses new security and privacy threats, such as eavesdropping on sensitive medical data or hijacking life-critical functions. The consequences of such attacks can be severe because they can cause serious injuries or even death. However, these risks have often been overlooked. While no real-world attack against an IMD has been confirmed to date, previous research has demonstrated that many IMDs available on the market today severely lack effective security mechanisms, and that attacks on patients would be practically possible [21, 37–39, 51].

To protect wireless communication links, it is essential for the IMD and external device to undergo a pairing process. This process aims to *exchange a cryptographic key* between them, which can then be utilized to secure the wireless channel using standard protocols and techniques [12]. However, implementing such a key exchange in a secure manner is challenging because IMDs are resource-constrained with limited memory, computational power, as well as non-rechargeable and non-replaceable batteries. Moreover, IMDs do not have physically accessible input or output interfaces, such as a keyboard or a screen, once they are implanted. This obstructs traditional pairing methods used in technologies like Bluetooth, where manually typing a four-digit PIN code on the devices is a standard procedure [10]. Furthermore, network connections with these devices can be ad-hoc. For instance, in an emergency (e.g., patients with cardiac implants can experience syncope symptoms and become unconscious [52]), a doctor may quickly have to use a new programmer device to connect to the patient's IMD. Due to these limitations of IMDs, conventional pairing techniques (such as the ones based on symmetric/public keys [1]) are often not a viable option [39, 74].

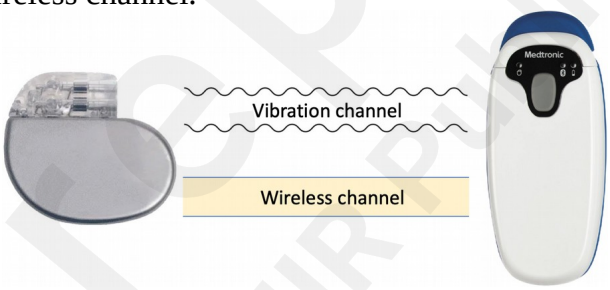
Previous work has proposed a variety of pairing techniques to overcome this challenge [57]. Rasmussen et al. [50] propose an approach where the IMD and external device send ultrasound to each other and measure the signal transmission time to determine the distance between them. If the distance is short enough, the two devices treat each other as legitimate entities and then exchange a key. Marin et al. [39] and Tomlinson et al. [68] propose a pairing method by transmitting a low alternating current through the patient's skin and tissue. Denning et al. [14] and Gollakota et al. [19] propose to delegate security to a proxy device that the patient can carry around (such as a bracelet). The proxy jams the wireless channel when it is present, while it can be removed during an examination or emergency. [34, 48, 53] propose a pairing process by the IMD and external device synchronously and simultaneously measuring a human physiological signal (such as heartbeats).

Across those prior approaches, a crucial aspect has been systematically overlooked: user perception. We observe that previous work has attempted to follow a "seamless" design approach that makes the

IMD pairing as unobtrusive as possible to the patient, rendering the pairing process almost imperceptible at the same time. This can prevent patients from detecting unexpected pairing attempts made by adversaries in proximity, thereby hindering their ability to appropriately respond to such security threats, e.g., by seeking assistance or fleeing the scene (We assume the patient has fundamental cognitive and physical capabilities; otherwise, there are many more straightforward ways to cause severe impact). Admittedly, the design principle of making the key exchange essentially invisible is prevalent in many everyday security systems, e.g., when surfing the Internet, users usually do not notice the key exchange process with a remote server [15]. However, this heavily relies on the assumption that the pairing is sufficiently secure and is initiated by the legitimate user. As this assumption is often not met in the case of IMDs [5, 20, 36, 62], we question if this principle suits the IMD context, where the device is part of the patient, and its security is life-critical.

To address this issue, a pairing protocol needs to incorporate a perceivable and robust (i.e., cannot be hidden or canceled by an adversary) signal. For instance, adding visual or audio cues on the external device could certainly enhance users' perception of the pairing. However, these cues would not be essential to the underlying cryptographic protocol (IMDs do not have cameras or microphones to sense these signals). As such, an adversary can develop an external device that mutes such cues, and thus may launch an unauthorized pairing without the patient's awareness. This leads us to consider vibration as an Out-Of-Band (OOB) channel (i.e., any communication channel other than a wireless channel) for pairing, as shown in Figure 1.

Figure 1: IMD and external device. The vibration channel is used to exchange a key that subsequently secures the wireless channel.



Vibrations are highly perceivable and have been widely used in smart consumer devices for notification services. Additionally, vibration has the potential to be generated and detected by hardware components that are cheap, widely deployed, and miniaturized. In particular, accelerometers, the primary type of vibration receiver used in previous approaches, are already present in state-of-the-art IMDs for medical purposes [41, 44, 49]. Another advantage of using vibration is its limited range of reliable reception. In the IMD context, this implies that if an external device intends to transmit a vibration to an IMD, it must be physically attached to the patient's skin for a while [29]. If an adversary overpowers the signal with a very strong vibration from a distance, the patient can easily notice this.

Related Work

Vibration-Based Secret Transmission in Ad-Hoc Networks

Previous work has proposed vibration as an OOB channel for transmitting secrets between two devices that physically contact each other [29, 30, 54, 55, 59, 70, 71]. Table 1 summarizes their application scenarios and hardware setups. Most are designed for wearables and Internet of Things (IoT) devices that are not implanted in the human body. As a common setup, the transmitter (such as a smartphone) is equipped with a vibration motor and the receiver contains a sensor to detect the

vibrations, such as an accelerometer [29, 30, 55, 59, 70], gyroscope [71] or microphone [54]. Moreover, there are two primary types of vibration motors in use [46]: Eccentric Rotating Mass (ERM) motors generate vibration by spinning an off-center weight and are extensively used due to their simplicity and low cost. Linear Resonant Actuator (LRA) motors, on the other hand, vibrate by oscillating a mass along a linear path, offering more precise control over vibration patterns and are being gradually employed by advanced consumer devices.

Table 1. Setup for previous vibration-based secret transmission. The application context refers to the intended receiver device.

Technique	Application Context	Motor Type	Receiver Sensor Type	Sampling Rate (Hz)
Vibrate-to-Unlock [59]	RFID tag	ERM or LRA	Accelerometer	Not reported
SYNCVIBE [30]	Wearable	ERM or LRA	Accelerometer	1600
SecureVibe [29]	IMD	ERM or LRA	Accelerometer	3200
VibroComm [71]	IoT device	ERM or LRA	Gyroscope	32000
Ripple [55]	Mobile device	LRA	Accelerometer	1600
Ripple II [54]	Mobile device	LRA	Microphone	48000
Touch-And-Guard [70]	Wristband device	ERM	Accelerometer	250

Prior work predominantly directly embeds the secret within the vibration signal itself [29, 30, 54, 55, 59, 71]: the transmitter encodes the secret into vibration using specific modulation methods, and the receiver picks up this vibration with a sensor and decodes the secret. For instance, [29, 30, 60] employ On-off keying modulation to encode the secret, transmitting a ‘1’ with a carrier signal and a ‘0’ with no carrier. Another strategy leverages vibration to “amplify” the secret from humans: Wei et al. [70] propose an approach that pairs an IoT device with a wristband device, where the IoT device contains a vibration motor, and both devices have an accelerometer. When the user (who wears the wristband) touches the IoT device, the motor emits a vibration that sweeps through a range of frequencies. Contrary to the above methods, the vibration here does not carry the secret and remains consistent across different sessions. Instead, the secret comes from the (to some extent random) resonant properties of the user’s hand-arm area, which can be derived from the accelerometer readings.

However, we argue that most work (in their current form) is not deployable in existing IMD products because they have stringent requirements on the receiver sensor. Microphones do not exist in IMDs, nor is there any indication they will be included in the foreseeable future; while inertial sensors (i.e., accelerometer and gyroscope) often require sampling rates in several thousands of Hz or higher. While there are no published reports on current IMDs’ inertial sensor sampling rates, we doubt whether these devices have been or will be equipped with such high-performance sensors: First, a primary function for which inertial sensors are incorporated into IMDs—patient routine activity recognition [41, 44, 49]—only takes at most a few hundred Hz to gain high accuracy [9, 28]. Second, other technologies that fulfill specific medical purposes for IMDs typically use sampling rates of up to one thousand Hz [13, 65, 66]. Third, the power consumption of inertial sensors often rises exponentially as the sampling rate increases [28], while IMDs have constrained batteries. Future studies could certainly explore if prior work remains effective at reduced sensor sampling rates such

as a few hundred Hz. Nevertheless, this is likely to significantly impact the performance, because vibration signal demodulation often requires sensor data with high resolution [55].

Overall, we find that only [70] demands a lower sampling rate of 250 Hz. This is because the secret relies on the resonant frequencies of the user's hand-arm region, which are situated in the low-frequency domain ranging from several to a few hundred Hz [2, 3]. Nonetheless, its practicality was only validated for wristbands but has not been tested in other deployment environments or with different hardware setups. In this paper, we start with the approach of [70] in a prototype that simulates the environment of an IMD and demonstrate that it may not be the optimal choice. Consequently, we propose a new and reliable vibration-based technique for pairing with IMDs using accelerometers with the same or potentially lower sampling capabilities.

Suitable Protocols for Out-Of-Band Channel-Based Pairing

Previous work has extensively proposed using an OOB channel for pairing with resource-constrained devices, including IMDs [22, 29, 39, 53, 61]. Typically, the ultimate objective of such pairing is to establish a 128-bit cryptographic key between two devices for data encryption [12]. However, these works commonly propose to directly exchange the entire key through the OOB channel, which raises several concerns.

First, OOB channels often have much lower data throughput compared to conventional wireless channels. For instance, the data throughput of the aforementioned vibration-based method [70] is only 7.15 bits per second. As a result, a 128-bit key bootstrap would require at least 18 seconds, potentially posing issues of usability and safety in emergencies (when medical staff need to access the patient's IMD in a short time). Second, OOB channels face threats from advanced side-channel eavesdropping attacks. For example, a vibration channel might be compromised using microphones in proximity due to acoustic leakage [20]. Transmitting the entire cryptographic key through such channels simplifies eavesdropping attacks, as an adversary does not have to recover the secret in real-time during its transmission; instead, they can record the pairing communication traffic and conduct offline brute-force analysis to recover the key, potentially compromising the security of the pairing significantly [20]. The adversary's success allows unauthorized access to all sensitive data previously encrypted by this key, leading to severe consequences.

To mitigate these concerns, prior work has suggested the use of a Password-authenticated Key Agreement (PAKE) method [27, 33, 53]. PAKE is a cryptographic protocol aiming at exchanging a high-entropy cryptographic key between parties who have previously shared a short and low-entropy secret. A concrete example of PAKE is Diffie-Hellman Encrypted Key Exchange [8]. This approach allows two devices to initially exchange a short bitstring, after which they execute a PAKE to further exchange a 128-bit key. The latter step can be fast and thus largely reducing the impact of the low data rate of OOB channels. Additionally, PAKE provides forward secrecy and rules out offline brute-force attacks. This is the approach that we adopt in our work, and therefore we consider that vibration is only to be used to exchange an ephemeral and low-entropy secret between the IMD and the external device, followed by the execution of a PAKE to facilitate a more robust key exchange.

Objectives

The objective of this paper is to explore the potential of using vibration for pairing with resource-constrained IMDs. We aim to i) propose a novel technique that leverages vibration to extract secrets from the naturally random human motor behavior for pairing, ii) develop a prototype as a proof-of-concept to demonstrate our technique, and iii) evaluate our prototype's accuracy, security, and usability in a lab study involving 24 participants.

We will publish the data from our user study and software used in our prototypes under a permissive open-source license. For the reviewers, these anonymous materials are temporarily available in [75].

Methods

Pairing Technique

Our pairing process requires the user (patient or doctor) to repeatedly attach the external device to the patient's body (near the IMD's location) for a few times. For our work, we refer to each repetition of the user as a *cycle*, and the complete pairing process (including several cycles) as a *run*. Each cycle comprises three main steps:

- *Device Attachment.* The user attaches the external device to the body and holds it steadily.
- *Vibration broadcast.* The external device emits a vibration signal for a short period. The signal is always the same and does not serve as the secret. Both the IMD and external device take a measurement of the acceleration. The user releases the external device when the vibration stops.
- *Randomness extraction.* Both devices process the sensed acceleration signal and derive a shared secret from it.

The security of pairing relies on the randomness of the shared secret, which originates from the diverse physiological characteristics of the human body as well as the inherent variability of human behavior [24]. In particular, the latter includes, e.g., the varying position where the external device is attached and the spontaneous manner in which the device is held, such as various levels of grip strength. The vibration signal itself remains constant in each cycle and is *not* a source of randomness. Instead, it serves as a "catalyst" that allows the randomness of body and motion to be reflected in the accelerometer measurements.

Obtaining a Shared Secret from Human

The design of vibration strategy in each cycle—namely, the control of the motor to vibrate at a certain frequency(s) for a certain time frame(s)—is crucial. We first explore the feasibility of the aforementioned work [70] when applied to the context of IMDs. We replicate the exact same experimental settings using our prototype that simulates the human body environment (elaborated in the following sections): The accelerometer sampling rates of the external device and IMD are set as 250 Hz (According to the Nyquist-Shannon sampling theorem, the devices can accurately measure vibrations at frequencies up to 125 Hz). In each cycle, the motor is programmed to sweep between 20 Hz to 125 Hz within 1.75 seconds. During this period, two devices measure the Z-axis acceleration data (aligning with the user's sagittal plane), and subsequently generate the frequency spectrum by doing Fast Fourier Transform (FFT).

One researcher of our team performs 100 cycles as a preliminary test. The results are shown in the figures below. For clarity, we normalize the frequency spectrum and manually divide the data into four categories according to the number of peaks shared by both devices (the locations of the resonant frequency peaks were regarded as secrets in [70]). The shared peaks are marked with red arrows.

Figure 2: With one stable peak (72%).

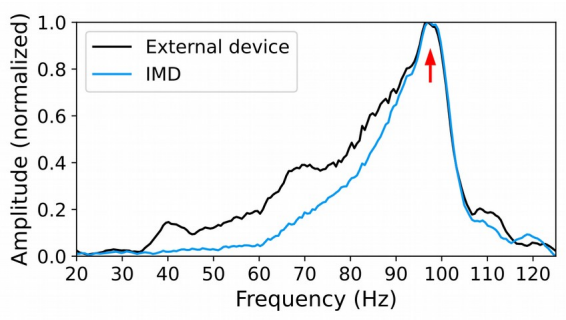


Figure 3: With two stable peaks (17%).

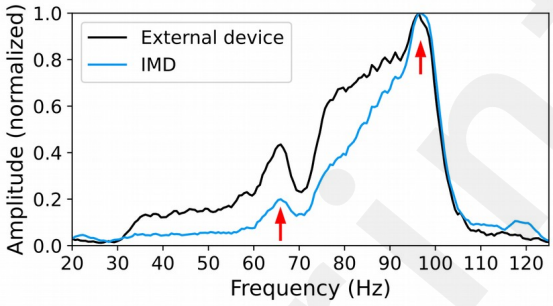


Figure 4: With three stable peaks (2%).

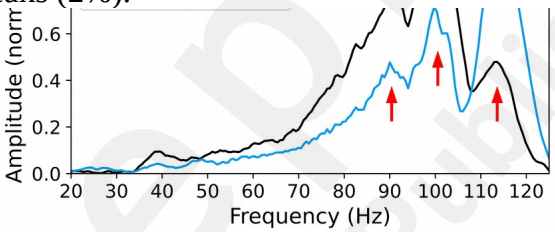
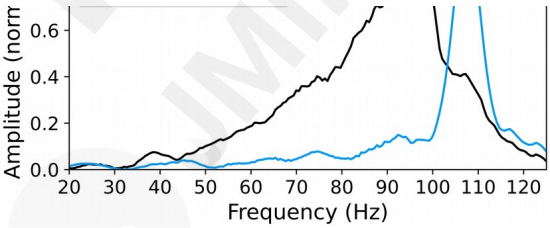


Figure 5: Noisy data (9%).



Among all, 72 cycles show one stable peak; 17 cycles have two common peaks while only 2 possess three peaks. Apart from these, in 9 cycles, the data is so noisy that it is impossible to capture any shared peaks. Our results differ significantly from [70] where an average of 4-8 peaks can be obtained per cycle. Additionally, the peaks in [70] are somehow uniformly distributed over the whole 20-125 Hz range, while ours are almost always in the range of 80-110 Hz. Our interpretation for the discrepancy in the performance of this strategy is the presence of the plastic board/shell in our prototype setup, which “masks” the resonant frequencies of the human body. Unfortunately, in the context of IMD pairing, the existence of such components (e.g., a plastic or metal device housing) is inevitable. In practice, we expect that unknown and varied environments may lead to very erratic performance of this approach.

However, we still draw inspiration from the above test. The variance of frequency response among cycles implies the natural randomness inherent in the user attachment motions, given that the physical characteristics of the vibration, the user (i.e., body and hand) and the environment (i.e., prototype) are unchanged. Intuitively, we want to test if a constant-frequency vibration is a viable option. We program the motor to emit a 50 Hz vibration for 1 s per cycle, and the same researcher executes 100 cycles using our prototype. For each cycle, we collect Z-axis acceleration data from both devices and generate the frequency spectrum using FFT.

Figure 6 shows an example of the frequency spectrum in one cycle. We observe that two devices can obtain very similar data, especially for a prominent amplitude peak. Figure 7 illustrates the spectrum change of the IMD over ten consecutive cycles. Each row in this figure corresponds to a frequency spectrum obtained in one cycle, and the bright spots indicate the prominent peaks on the curve. We observe that the peak locations vary around 50 Hz, suggesting the presence of a degree of randomness. Furthermore, two device capture exactly the same peak locations in 98 out of 100 cycles, yielding a low error rate. These findings indicate that providing an excitement of a constant-frequency vibration, the prominent peak location in the frequency domain is a potentially qualified shared entropy source between the IMD and the external device, which can be utilized for pairing purposes.

Figure 6: Frequency spectrum given a constant vibration (50 Hz, 1 s) in one cycle.

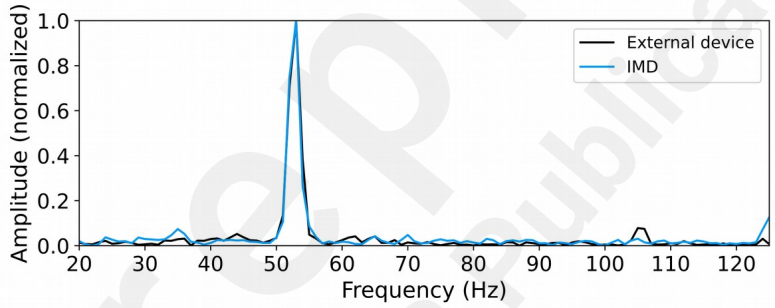
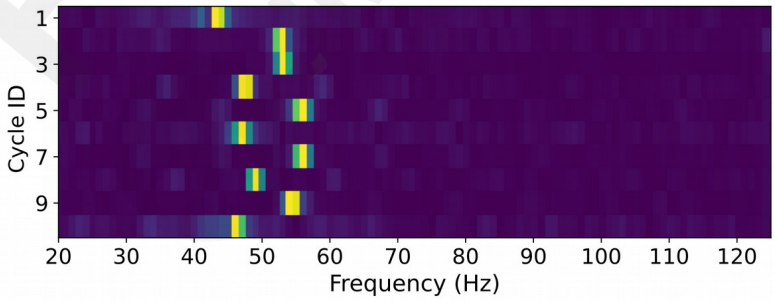


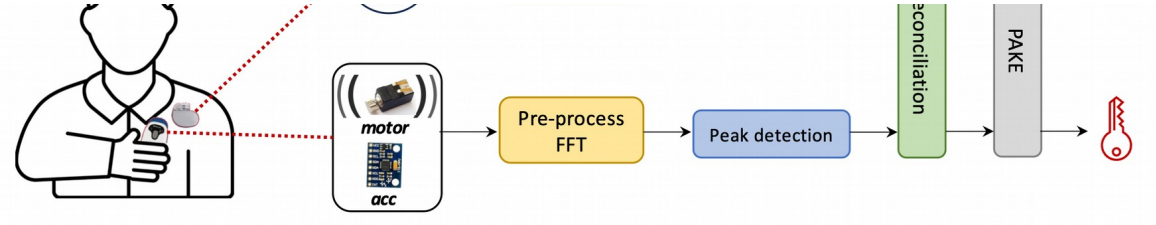
Figure 7: Frequency spectrum of IMD, given a constant vibration (50 Hz, 1 s) in ten consecutive cycles.



Signal Processing Workflow

Figure 8 shows the workflow of our pairing technique (assuming the IMD is a pacemaker). In each cycle, the patient holds the external device and attaches it on their chest. During the attachment, the motor vibrates and both the IMD and the external device measure a pair of Z-axis acceleration data.

Figure 8: An overview of our pairing technique.



The two devices first initiate a pre-processing step: To remove the noise of the direct current component, each device subtracts the acceleration data with its mean value. In addition, the frequency transition of a vibration motor is not ideal and instantaneous [29, 30], i.e., when the motor is switched on from standstill or switched off, the generated vibration signal is not amplified or attenuated immediately but with a slow and damped response. This means that the transition parts (i.e., two ends) of a vibration signal segment are often noisy. To address this issue, we apply a Hanning window on the data to suppress the noise at transition frames and highlight the middle part.

Subsequently, each device applies FFT on the acceleration signal to obtain the frequency spectrum. The frequency range of 0 to 20 Hz is then excluded to avoid the effects of noisy motion artifacts like human breathing movements [73]. As mentioned, there is a prominent amplitude peak in the frequency spectrum. In order to detect the location of this peak, each device simply traverses the frequency domain to find the frequency value corresponding to the maximum amplitude. This solution is straightforward and has demonstrated significant robustness in our study, because the prominent peak is often significant enough and overwhelms the other local optima caused by the noise (see Figure 6).

Based on the above procedure, after the user completes a pairing (i.e., a run) by repeating the attachment for several times, each of the two devices will possess a sequence of peak locations. However, these sequences may not be exactly the same due to the measurement noise and human error (e.g., hand wobbles). We design a two-step reconciliation process to resolve this: First, each peak location is encoded into a binary format using Gray code [18]. This coding method ensures minimal bit mismatches if the discrepant peak locations are very close on two devices, which is the case of our technique. These binary values are then concatenated in sequence to form a continuous bitstring on each device. Second, we employ a cryptographic algorithm known as a fuzzy extractor [16, 74] to reconcile any remaining bit differences between the two bitstrings without revealing the secret itself. Specifically, we utilize a syndrome construction of fuzzy extractor based on a Reed-Solomon (RS) error correction code (detailed in the Results section). This approach is chosen for its high efficiency and low power consumption characteristics, as reported in [74]. As long as the rate of bit mismatches falls within the error- correcting capability of the chosen RS code, the IMD and the external device agree on an identical bitstring as a shared secret, which is used as the input of a PAKE to further exchange a cryptographic key (see the Related Work section).

Note that we intentionally design the signal processing to be straightforward and lightweight for computation, considering the limited resources of the IMDs. We also explored the use of, e.g., signal smoothing techniques, but found that they only slightly decreased mismatches while imposing additional burden on the IMD. We thus omitted such steps.

Adversary Model

Given our review of relevant literature about IMD pairing techniques [19, 22, 37, 50, 53, 57, 72], we assume a sophisticated adversary following the Dolev-Yao model [17] who has full knowledge of

our pairing protocol, has full control over the (wireless) communication channels, and can be a Man-in-the-middle (MITM) attacker by intercepting legitimate devices' signals and sending their own messages instead. In particular, the adversary can launch two types of attacks relevant in the particular context of our pairing technique:

- *Impersonation attack.* The adversary uses a sequence of peak locations in an attempt to impersonate a legitimate device. They could succeed if their sequence closely matches the one measured by the IMD or external device. This sequence can be previously collected from any users or even themselves.
- *Brute-Force attack.* The adversary brute-forces possible peak location sequences and launches MITM attacks to decipher and/or manipulate the communication between legitimate devices. The brute-force can be done online, i.e., during the pairing process, the adversary tries every possible sequence until they hit a correct one. This attack is limited by the rate at which an adversary can run multiple pairing sessions with the target device. Alternatively, this can be done offline, where the adversary records the pairing traffic and performs offline analysis to crack the secret after pairing. This attack, if at all possible in the context of a specific pairing technique, is limited by the adversary's computational resources.
- *Acoustic eavesdropping*. The adversary may also attempt to eavesdrop on the vibration signals using a microphone near the patient to reveal the secret. The impact of such attacks is analyzed in the Discussion section.

As mentioned, we do not assume that the adversary has the capability to actively inject vibrations to pair with the IMD, as such a case could be easily noticed by the patient [29]. We also do not consider Denial-of-Service attacks such as signal jamming, because they can be mitigated using existing solutions [22, 29].

User Study

To validate our proposed pairing technique, we design and test our prototype in a user study. We assume that the IMD is a pacemaker implanted beneath the chest, but also note that the type of IMD or implantation place can be easily varied, e.g., an insulin pump beneath the waist area. We consider the external handheld device as being similar in shape to a smartphone with a plastic case. Moreover, both devices contain an accelerometer, and the external device is equipped with a vibration motor.

Prototype Implementation

We show an overview of our prototype in Figure 9. The prototype consists of three main parts:

- *IMD.* In our hardware setup, we use an InvenSense triaxial MPU-6050 accelerometer [26] to simulate a pacemaker and house it inside a 3D-printed case (Acc2 in Figure 10). An Arduino Nano 33 BLE board interfaces with the sensor and records data on an SD card for analysis. This board contains a 32-bit Cortex-M microcontroller and closely resembles the capabilities of an IMD [43]. The sampling rate of the accelerometer is set at 250 Hz, the same as in previous work [70].
- *External device.* We do not directly use a smartphone as the external device because the most common operating systems on mobile devices—Android and iOS systems do not provide an API interface for direct control of the vibration motor frequency. Instead, we employ an ERM type vibration motor [45], which has been widely deployed in commercial portable devices such as smartphones, along with another MPU-6050 sensor (Acc1 in Figure 10) to simulate an external device. These components are mounted on a 11 cm × 7 cm × 0.5 cm plastic cuboid board, replicating the size and shape of a typical smartphone. This mock-up also includes a (white) handle to aid participant grip. A separate Arduino

Nano 33 BLE board controls the vibration motor and the accelerometer. In particular, the Arduino board can control the vibration frequency by providing different driving voltages using Pulse Width Modulation technique. The sampling rate of the accelerometer is also 250 Hz.

The vibration motor should start to vibrate only when the external device has been well attached to the user's body. To ensure this in our study, we incorporate a buzzer into our prototype that emits a beep sound 0.5 seconds prior to each activation of the motor, serving as a cue for participants to attach the device. This design demonstrated effectiveness during our user study. However, note that this is just a preliminary solution for prototyping purposes. In a real-world set up, the external device can certainly utilize a proximity sensor or a camera to autonomously determine when it has been attached to the body.

- *Chest environment.* Given that pacemakers are embedded inside the body, it is important for our experiments to mimic an environment that resembles the human chest. We adopt the design in previous research [22, 29, 39], and use 1 cm layer of bacon and 2 cm layer of lean ground beef to replicate the chest's physical properties (see Figure 11). The 1 cm depth is a standard depth for pacemaker implantation [47]. In our study, we embed our pacemaker simulator within the meat layers, which are kept inside a food storage bag at room temperature. This bag of meat is subsequently placed in a pocket stitched onto an elastic chest band, positioned around an area corresponding to the human heart's location (see Figure 10). Participants were asked to wear the chest strap throughout the user study to mimic the conditions of pacemaker users. The meat was replaced at the beginning of each day to prevent spoiling.

Figure 9: Prototype overview.

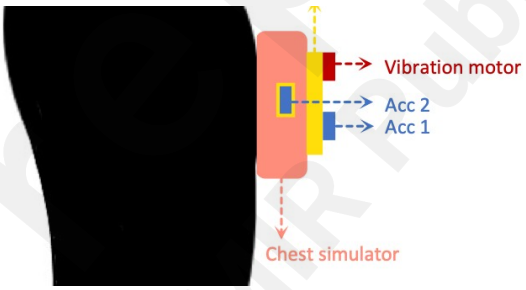


Figure 10: Hardware setup.

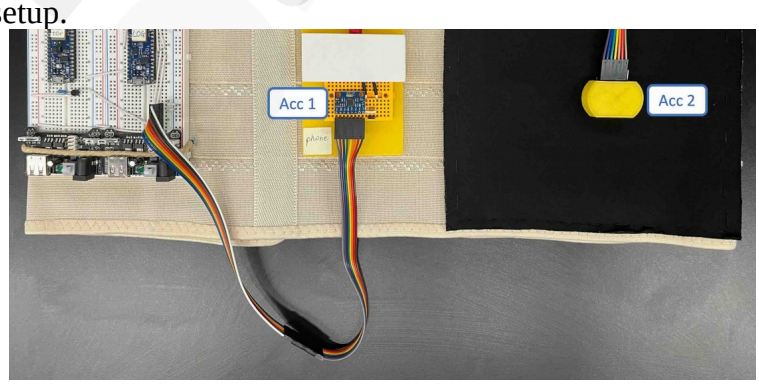


Figure 11: Chest simulator.

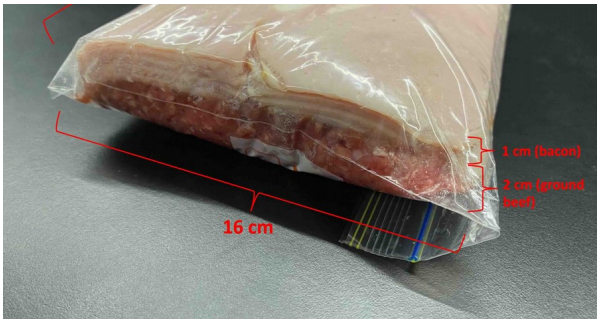


Figure 12: Participant in user study.

Apart from the above, we also develop an Android application that connects with the external device (the Arduino) via a Bluetooth Low Energy link. This app is used to control the start of each pairing process and program the vibration condition (i.e., frequency and duration) of the motor on the fly during the user study (otherwise, we need to frequently reload firmware in Arduino via usb cable). We omit the details of the app since it is not the focus of our study.

We highlight that our prototype (especially the chest strap and meat bag that are worn by participants) only aims to simulate the experience of a pacemaker patient during the user study—in real-world applications, the user would only need to hold an external device and perform attachments on the patient's body. We also note that in the domain of IMD security research, accurately simulating the environment of an IMD often poses a significant challenge, and most prior work proposing IMD pairing techniques lack practical prototype implementation and evaluation with humans [14, 19, 39, 48, 50]. To the best of our knowledge, our work presents the first wearable pacemaker prototype that allows for direct participant interaction and testing.

Participant Recruitment

We first conducted a pilot study with six individuals (ages 22 to 32, four females and two males) to identify and resolve any problems with our experimental setup. Subsequently, we recruited 24 participants for the main study, including 11 males and 13 females of ages ranging from 18 to 52. All participants were recruited via online advertisements and were offered $30 for their time.

According to governing legislation, research involving human subjects requires approval from a Human Research Ethics Committee within the research institution, governed by the National Health and Medical Research Council. Our user study obtained approval from it.

Experiment Procedure

We manipulate two essential vibration settings, frequency and duration, and measure the effect on

pairing performance. We set three levels of vibration motor frequencies to 50 Hz, 75 Hz and 100 Hz, considering that the motors and accelerometers in consumer devices are often limited (recall that an accelerometer with a sampling rate of 250 Hz can only measure vibration frequencies less than 125 Hz). During our preliminary tests, we noticed that due to the inherent instantaneous nature of vibration motors, the frequency spectrum obtained from vibrations lasting less than 400 ms was often noisy with multiple peaks, leading to high mismatch rates between the two devices. On the other hand, vibrations over one second did not appear to offer additional benefits but harmed time efficiency and impacted user experience. Therefore, we set vibration durations to 400 ms, 700 ms and 1000 ms. The 9 possible vibration frequency/duration combinations are intentionally set to avoid extensive workload for participants in the user study.

During the user study, participants were instructed to wear our prototype and sit on a chair. Then they need to grasp the external device simulator and repeatedly attach it to the black pocket area of the chest strap, as shown in Figure 12. They were advised to attach the device in a random manner (such as to random positions), and (in each cycle) stay attached until the vibration had completely ceased. Before starting the data collection, participants were asked to acquaint themselves with the prototype to understand the pairing process. This introductory process took under a minute for all participants. Subsequently, for each of the 9 vibration conditions, participants were asked to conduct the attachment for 5 consecutive cycles as one run, and complete 4 such runs in total. The order in which participants used different vibration frequencies was counterbalanced, while the order of using different vibration durations was fixed (always from short to long).

At the end of the user study, participants were requested to fill out a standard System Usability Scale (SUS) questionnaire [31] to assess the usability of the pairing method. We then conducted an interview with them to gather further insights. Full details of the questionnaire and interview are given in Multimedia Appendix 1.

Results

Evaluation Metrics

Our study focuses on certain metrics to evaluate the pairing performance.

Accuracy

The accuracy of a pairing system is typically measured by False Rejection Rate (FRR) and False Acceptance Rate (FAR) [4, 32, 33]. FRR is the frequency at which the pairing between legitimate devices is incorrectly rejected. FAR indicates the frequency that a pair of illegitimate devices (such as the IMD and a malicious external device) is mistakenly authorized, and gauges the resilience of pairing against impersonation attacks. A high FRR and FAR could lead to poor usability and security, respectively.

During the pairing process, there is often mismatch (denoted by d) between the readings of the IMD and the external device due to inherent noises. A successful pairing requires that two devices share the exact same secret. As aforementioned, we use a fuzzy extractor scheme to correct the mismatch. At the core of this method is the selection of a threshold (denoted by Thr): the mismatch can be rectified (and thus the pairing is accepted) if $d \leq Thr$; otherwise, the pairing is rejected. A false rejection occurs when $d > Thr$ for a legitimate data pair, and false acceptance when $d \leq Thr$ for an illegitimate pair. As such, one can balance FRR and FAR by adjusting Thr. Because security is of utmost importance for the IMDs, we set a smaller Thr to ensure FAR = 0, and use the corresponding lowest FRR to represent accuracy.

Security

The FAR metric evaluates the system's security against impersonation attacks. On the other hand, the resilience against brute-force attacks is determined by the randomness level of the attachment motions, which can be measured in two primary ways: i) By the National Institute of Standards and Technology (NIST) statistical test suite [56] that provides a comprehensive randomness assessment of a random number generator, a method widely recognized within the cybersecurity community [33, 53, 70]. ii) By measuring entropy, which quantifies the amount of information contained in each motion event. We employ the Shannon entropy (the unit is bit), a method extensively used in previous work [34, 40, 67, 70].

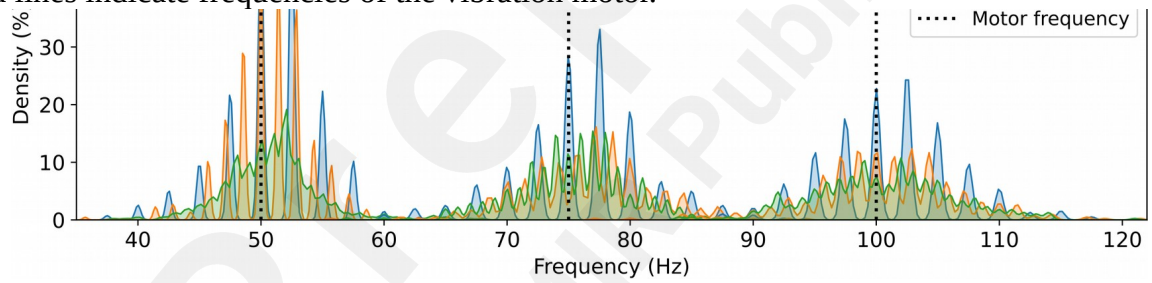
Usability

Usability is assessed based on the results from our SUS questionnaires and interviews.

Shared Secrets

Figure 13 shows the distribution of all peak locations (i.e., the secret) collected by the IMD from 24 participants. The plotted distributions have been slightly smoothed for better visualization. We observe that for a specific vibration frequency, such as 50 Hz, the peak locations range between 30 and 70 Hz and generally approximate a normal distribution centered by the motor's frequency, suggesting a certain degree of randomness from the user. Additionally, it appears that the distribution is slightly flatter (thereby the level of randomness increases) with an increase in vibration frequency. This observation is later substantiated by the entropy measurements.

Figure 13: Distribution of peak location measured by the IMD among 24 participants. The black dashed lines indicate frequencies of the vibration motor.



The possible options for peak locations in the frequency domain are not continuous due to the sample-based nature of the time domain acceleration data. Notably, the more time domain samples, the higher the frequency domain resolution. For instance, with an accelerometer sampling rate of 250 Hz, the frequency resolution is 2.5 Hz for a 400 ms measurement window. This indicates that potential peak locations are in discrete intervals such as 47.5 Hz, 50 Hz, 52.5 Hz, and so on. Consequently, we observe more "jagged" curves for shorter vibration durations like 400 ms, and denser curves for longer vibrations such as 1000 ms.

Mismatch is calculated by subtracting peak location values between the IMD and the external device, and represents the level of noise and error. The mismatch distribution for our prototype, as illustrated in Figure 14, resembles a normal distribution centered around a mean near zero and with a standard deviation of 2.8 Hz. This implies that user-induced errors and sensor noise are limited in our prototype. Note that this result takes into account situations where participants did not strictly follow our pairing norms during the study. For instance, there were a number of occasions when participants released the external device while it was still vibrating. Such cases were *not* excluded from our

dataset as they present a more realistic use scenario; otherwise, we expect that the mismatch levels would be even lower. On the other hand, Figure 15 and Figure 16 show that the degree of mismatch does not have a straightforward correlation with either the vibration frequency or the duration.

Figure 14: Mismatch of all data among 24 participants.

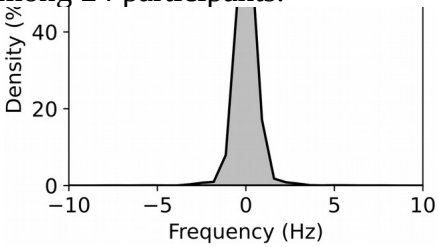


Figure 15: Mismatch with vibration frequency among 24 participants.

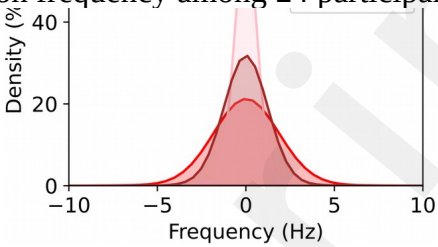
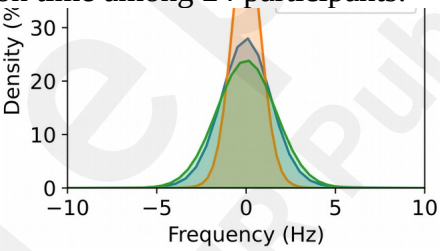


Figure 16: Mismatch with vibration time among 24 participants.



Pairing Accuracy

For each of the 9 vibration conditions, we build two sets to measure accuracy:

- Set I comprise 96 (= 24 × 4) pairs of peak locations, each with a length of five (since we collected five cycles per run). All the pairs in Set I come from legitimate pairings of an IMD and an external device.
- Set II has 96 pairs of peak locations (the same size as Set I), where each pair is created by randomly mixing data from illegitimate device pairings. An example would be a pair originating from participant A's IMD and participant B's external device, or from participant A's IMD and external device, but collected in different pairing sessions.

An effective pairing technique should maximize the acceptance of pairs from Set I (i.e., low FRR), while minimizing the acceptance of pairs from Set II (i.e., low FAR). Note that not all five motions are necessarily needed, i.e., we can vary the length of runs ranging from one to five, by truncating the initial elements.

The following figures show the accuracy of our prototype across various numbers of attachment

motions performed. FAR is 0 in all cases, and we consider that an FRR below 5% signifies good usability (note that a more lenient FRR threshold of 10% was suggested in previous work [33, 40]). As expected, increasing the number of motions consistently improves the accuracy of the pairing. Moreover, given a specific vibration frequency, longer vibration duration leads to higher accuracy. This is due to the increase of entropy with prolonged vibration, which will be further discussed in the coming sections. An additional observation is the association between vibration frequency and accuracy. With a fixed vibration duration and number of motions, we find that the FRR tends to drop as the vibration frequency rises. This insight requires further investigations.

Figure 17: FRR *vs.* number of attachments, under 50 Hz vibration frequency.

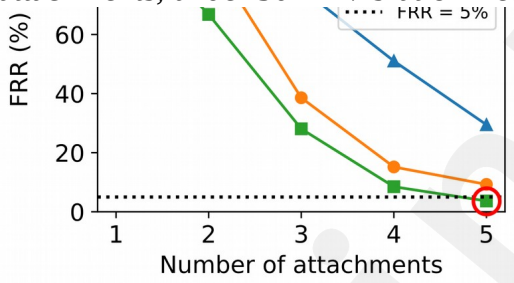


Figure 18: FRR *vs.* number of attachments, under 75 Hz vibration frequency.

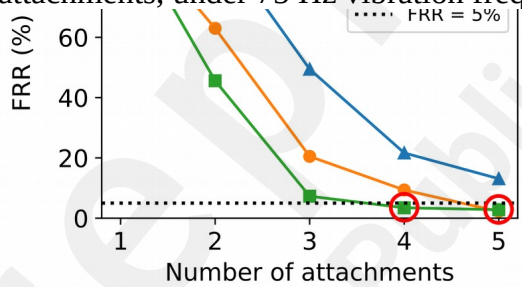


Figure 19: FRR *vs.* number of attachments, under 100 Hz vibration frequency.

Overall, the red circles in the above figures indicate the five out of nine vibration conditions that offer acceptable accuracy levels (with FAR = 0 and FRR < 5%). For example, a vibration condition of 50 Hz for 1000 ms per cycle requires the user to execute five attachments to achieve pairing with FAR = 0 and FRR = 3.7% (see Figure 17). Note that for other vibration conditions, more than five motions are likely to also yield satisfactory accuracy. However, this was not tested by us and would demand more effort from the user, which could harm usability and even safety (e.g., availability in emergencies). As a result, such settings are not considered in the following.

Security Assessment

Randomness Analysis

We refer to previous work [33, 53, 70] to assess the randomness of the secret generated by our technique. The previous accuracy evaluation has led us to consider only the five vibration conditions that demonstrated acceptable levels of accuracy. For each of these conditions, we take the floor of the (fractional) entropy value for that specific setting (see Table 3), and extract that number of least significant bits from each peak location value. These bits are then concatenated together following the order in our user study. Subsequently, we combine these bitstrings from all five vibration conditions as a single 8.6 kbits string, and evaluate its randomness using the NIST statistical test suite [56].

The full results are given in Table 2. The outputs of the NIST statistical tests are *p*-values that represent the probability the data is generated by an eligible random number generator. If a *p*-value is smaller than a threshold (usually 0.01 [33, 53, 70]), the randomness hypothesis is rejected. Table 2 shows that all *p*-values are larger than 0.01 and hence *pass* the NIST tests. Note that we do not conduct Maurer's Universal Statistical Test, as it requires a minimum data input of 387.8 kbits that is not met in our case. This test was also omitted by previous work [33, 70].

Table 2. NIST statistical test results for attachment motions.

Test	*p*-value	Test	*p*-value
Frequency	0.880	Block Frequency	0.143
Runs	0.111	Longest Runs	0.099
Binary Matrix Rank	0.170	FFT	0.622
Non-overlap Template	0.160	Overlapping Template	0.377
Serial (p-value$_1$)	0.638	Linear Complexity	0.716
Serial (p-value$_2$)	0.677	Approximate Entropy	0.176
Cumulative Sums (forward)	0.191	Random Excursions	0.216
Cumulative Sums (reverse)	0.259	Random Excursions Var.	0.403

Entropy Analysis

Table 3 shows the entropy value contained in each motion across different vibration conditions. Overall, a single motion in our study carries an entropy from 2.61 to 4.48 bits. For a certain vibration frequency, the entropy grows with higher vibration durations. This is because given a fixed sampling rate of the accelerometer, a longer measurement brings about a larger sample size and thus higher frequency domain resolution. This provides more possible peak locations and thus increases the entropy level. Furthermore, for a given vibration duration, the entropy value rises with an increase in vibration frequency. This observation aligns with the findings discussed earlier. We leave the study of this phenomenon to future work. Nevertheless, there is an upper limit to the choice of vibration frequency, often limited by the capability of the motor and accelerometer in practice.

Table 3. Entropy of each attachment motion (unit is bit).

	50 Hz	75 Hz	100 Hz
400 ms	2.61	3.12	3.87
700 ms	3.03	3.86	4.15
1000 ms	3.15	4.01	4.48

It is noteworthy that some entropy is sacrificed due to the reconciliation process that rectifies mismatches between the two devices. Here, we make a preliminary estimation of the entropy loss: Using the encoding method in [33] on our dataset, the maximum bit mismatch rates (i.e., percentage of different bits between two devices) for our prototype vary between 0.7% and 3.0% for different vibration conditions. This can be addressed by a fuzzy extractor with (31, 29) RS code that has a 3.23% error tolerance [35, 74], potentially leading to an entropy loss of 6.5%. Note that this is a preliminary estimate, and more rigorous calculations are necessary in real-world implementations, which is beyond the scope of this paper.

Participant Feedback

The average SUS score for our pairing technique is 73.6 (SD = 18.14), which generally passes the typical benchmark value of 68 for “good usability” [31]. It is important to note that the SUS questionnaires were completed after an extensive data collection process including a repetition of 180 attachment motions. We expect that users carrying out a more realistic task would report even higher usability scores.

We gained further insights into usability from the interviews. Over half of the participants (15 out of 24) explicitly indicated that our technique was easy to use. For example, one participant (p8) commented “The attachment doesn’t require me to think. This is an advantage. I don’t know what is happening here, but I prefer it as it requires less effort”, and another participant (p13) remarked “It’s easy. You don’t really have to move that much, and you can do it while you’re sitting as well”. Some participants expressed their preference for the vibrational feedback. One participant (p1) said “The vibration is good feedback, and I don’t have to visually see anything”, and one participant (p21) mentioned, “I feel more in control”, while another participant (p22) noted “The process is like listen to my heart”. Additionally, some participants conveyed that they found the pairing process to be enjoyable and fun. For example, three participants described the vibration as a hand massage and two compared the pairing activity to using a stethoscope.

Most participants (18 out of 24) experienced no discomfort during the study. Nonetheless, the rest six people did report some discomfort at the end of the study. Four participants noted that the intensity of the vibrations was excessive, e.g., one participant (p4) stated, “I feel like my entire chest is vibrating, and I don’t like the feeling”. This concern might be resolved by selecting a vibration motor with lower amplitude. Additionally, four participants reported feeling fatigued after the data collection process, but also noted this was due to the repetition of 180 attachments and that less motions will alleviate this issue. Furthermore, one participant (p3) criticized the prototype design and mentioned that the external device simulator was too big. We leave the refinement of our prototype as future work.

Optimal Configurations

As a reminder, the attachment motions aim to exchange a short secret between two devices, which then serves as the basis for executing a PAKE. Based on our analysis so far, we summarize all pairing configurations that: i) exhibits high accuracy with zero FAR and FRR under 5%, and ii) generates a level of entropy surpassing a standard four-digit PIN code (with an entropy of 13.3 bits), which is commonly used in pairing of Bluetooth technologies and other security systems [10]. All viable settings that meet these requirements (with minimum required number of motions) are shown in Table 4. The presented entropy has accounted for the loss incurred during the mismatch reconciliation process. Moreover, the time values include both the vibration duration and an additional “preparation time”, which refers to the interval necessary for a user to detach and then re-attach the external device to their body; in our study, this interval was 0.5 seconds.

Table 4. Summary of well-performing pairing configurations.

Vibration Condition	# motion	(FAR, FRR)	Entropy	Time (s)
50 Hz, 1000 ms	5	(0, 3.7%)	14.7	7.5
75 Hz, 700 ms	5	(0, 2.2%)	18.0	6
75 Hz, 1000 ms	4	(0, 3.5%)	15.0	6
100 Hz, 700 ms	4	(0, 0.6%)	15.5	4.8
100 Hz, 1000 ms	4	(0, 0.6%)	16.8	6

In summary, we find that with a vibration configuration set at 100 Hz and 700 ms, a user can carry out 4 attachment motions to enable the exchange of a secret with (FAR, FRR)=(0, 0.6%) and entropy of 15.5 bits. This process can be completed in a mere 4.8 seconds.

Discussion

The use of vibration as an OOB communication channel for pairing (i.e., key exchange) has gained attention, largely due to the enhanced perceptual experience it provides to users, which is desirable for security applications. However, existing work in this domain (including [29] that focuses on IMDs) encountered practical deployment challenges when considering existing IMDs. These challenges stem from the high sensor sampling requirements or erratic response to environmental changes, as we have verified in our study.

Our work introduces a new and reliable approach, which only requires a low sampling rate accelerometer and relies on the natural randomness inherent in human behavior for secure pairing. We empirically validate the feasibility of our technique through a study involving 24 participants. Overall, we find that the workload required to bootstrap a secure pairing is minimal, and we estimate that it requires the user to attach a device to the body only 4 times, with the whole process taking roughly 5 s. With an FAR of 0 and an FRR of 0.6%, the risk posed by adversaries is low, and legitimate users will likely experience very few failures. The entropy shared through the pairing motions exceeds that of a standard four-digit PIN code needed by Bluetooth pairing [10].

As mentioned in the Related Work section, the use of a PAKE eliminates offline brute-force attacks. In addition, a proper implementation of PAKE also restricts the number of online MITM attempts. Typically, the adversary has a very limited period to obtain the secret and usually only one chance for a MITM attack [8]; failing within this period would make recovering the key impossible. As an estimate, 4 motions with 15.5 bits entropy reduce the adversary’s success probability on online brute-force attacks to a value as low as 0.002% [27] (assuming the adversary is limited to guessing only). Therefore, we believe these motions serve as adequate input for a PAKE. It is noteworthy that if needed, higher entropy can be easily achieved by performing more motions.

Our user study confirmed the high usability of our pairing method. Participants found it straightforward to understand, learn, and perform. The process of attaching the device is very intuitive, like using a stethoscope as described by the participants. As an example, one participant (p2) displayed a level of ease and nearly fell asleep during our intensive data collection, yet they continued to perform the motions properly, even with their head dropping and eyes closed. Additionally, our technique brings about certain entertainment to users, being both relaxing and enjoyable (such as described as hand massage). This aspect could be advantageous in certain therapeutic treatments, where physical interaction can enhance memory, concentration, and mental

health [25]. Moreover, it is worth noting that for patients who are unable (e.g., due to disabilities or unconsciousness in emergencies) or unwilling to execute the motions, our pairing allows medical practitioners or caregivers (who have received appropriate training) to execute the motions on the patient's body on their behalf.

Our proposed method only requires an accelerometer, a component already present in the latest generation IMDs [41, 44, 49]. The signal processing for the IMD is computationally lightweight and works efficiently on 32-bit Cortex-M microcontrollers, which closely resemble IMDs' capabilities [43]. The other algorithms in our system, like the fuzzy extractor and PAKE, are well established and have been successfully used on similar or even less advanced hardware [33, 74]. Furthermore, our approach solely depends on vibration at a constant frequency, which can be easily implemented on readily available consumer devices such as smartphones and tablets. This is beneficial considering that medical device companies already equip the IMDs with the ability to connect to personal mobile devices. For example, Medtronic has developed a smartphone app that allows patients to view some basic characteristics of their pacemakers over Bluetooth [42]. Moreover, while our work assumes that the IMD is a pacemaker, we argue that the technique can be easily transferred to other types of IMDs or even external wearables. This is because our method leverages accelerometers for vibration measurements, which are independent of the location in the body. Additionally, although our prototype used an ERM type vibration motor, we believe that our method also works with LRA motors because it only requires a constant-frequency vibration.

Comparison with Prior Vibration-Based Work

Our pairing technique significantly relaxes the demands on the IMD's sampling capability. We utilize an accelerometer operating at 250 Hz, in contrast to previous work that often relies on sampling rates of several thousand Hz or more. In particular, the sampling rate can be further decreased by using lower vibration frequencies. For example, with a 50 Hz vibration, the frequency domain peaks cluster between 30 and 70 Hz (see Figure 13), indicating that an accelerometer with a 140 Hz maximum is adequate. However, lowering the sampling rate will diminish the resolution in the frequency domain and thus decrease the entropy per motion, and requires extended sampling durations or more motions to compensate for the reduction in entropy.

Another advantage of our pairing technique is that it forces multiple physical interactions with the patient, i.e., repeatedly attaching the external device to the patient's body. Such bodily motions can add an additional layer of perception beyond the vibration signals themselves. In contrast, most prior work requires just a single initial touch. Moreover, conventional approaches typically try to avoid user-generated noise. For instance, the user needs to ensure stable contact between devices during data transmission. Conversely, our method harnesses user noise and benefits from it as a source of entropy. Indeed, our dataset includes many instances with significant user noise/error, like when a participant releases the external device before the vibration completely stops. In such scenarios, the IMD only captures a portion of the vibration within its measurement window. Despite this, our technique maintains high reliability.

Furthermore, previous work that encodes secrets into vibrations often demands precise time synchronization in milliseconds between devices, which itself is a challenging task for resource-constrained devices [69]. In contrast, our approach allows for more lenient synchronization—as long as the two devices capture similar vibration signals within most of their measurement windows, the peak locations effectively match. This aspect greatly simplifies the synchronization requirements, enhancing the feasibility of our technique for IMDs or other devices with limited resources.

Notably, our data throughput is significantly lower than [29, 30, 55, 55, 71], and is comparable with

[60, 70]. Considering the scenario of transmitting a four-digit PIN code for use in a PAKE, previous work [29, 30, 55, 55, 71] only needs 0.0004 to 0.665 s, which is much faster than the 4.8 seconds required by our method. However, this rapid transmission, while advantageous in many daily applications, may not be suitable for IMD pairing contexts. In such contexts, the vibration serves not only for secret exchange but also as a crucial cue for patients to be aware of the pairing process. For instance, vibrations lasting less than a second might be too fleeting for patients to notice and react accordingly [58], e.g., stopping an adversary's actions, thus raising significant security concerns. In contrast, we argue that a duration of 4.8 s strikes a balance: it is long enough to be noticeable, yet short enough to maintain usability and safety in emergencies.

Considerations of Health Implications with Vibrations

Our proposed pairing technique incorporates the use of vibrations, a feature that naturally raises concerns regarding the potential long-term health impacts on patients. However, it is important to note that current research indicates that only long-term and excessive exposure to vibrations (e.g., due to specific occupations) is linked to adverse effects on mental and physical health [11, 63]. In contrast, our method involves brief vibrational interactions, which last less than five seconds and may not occur every day. This limited exposure could reduce the likelihood of the negative health consequences.

Despite this, we acknowledge the critical importance of thoroughly understanding any health implications associated with our approach, in particular in the delicate context of patient care. To this end, future collaborations with medical domain experts (such as physicians and representatives from medical companies) would be necessary to facilitate more comprehensive evaluations, and ensure that any health risks are meticulously assessed and addressed.

Resilience to Acoustic Eavesdropping Attacks

Vibration is essentially a low-frequency audio signal, which inevitably emits acoustic side-channel information that might be eavesdropped using a microphone. This is particularly threatening for methods that encode secrets within vibration signals. For example, Halevi and Saxena [20] found that secrets transmitted this way could be severely compromised using an off-the-shelf microphone from a few meters away. To mitigate this, Kim et al. [29] and Anand and Saxena [5, 6] proposed using Gaussian white noise or masking signals to obscure the acoustic leaks. These approaches have shown promise in reducing side-channel vulnerabilities against advanced eavesdropping attacks.

In comparison, as shown in [70], the risks associated with eavesdropping are significantly reduced when the vibration is not the carrier of the secret. Our research aligns with this guideline, using a constant vibration signal across sessions to minimize acoustic leakage. In addition, existing countermeasures [5, 6, 29] are also applicable to our method, and can be easily implemented by having the external device's speaker emit an audio concurrently with the motor's vibrations.

Limitations

Our work has certain limitations. Our experiments did not explicitly recruit participants who were IMD patients (mainly due to ethics constraints of the institutions where the user study was conducted). Further validation of our approach with these patient groups is necessary.

We designed our prototype in line with previous work in the IMD security community [22, 29, 39]. However, there is room for enhancement particularly in its size and weight. Future research should develop more skin-conformable and miniaturized prototypes. Nevertheless, we believe that the current imperfections of our prototype do not compromise the validity of our results, because the

pairing mainly relies on natural random human behavior, which is largely environment-independent [23, 24].

Furthermore, in our prototype, we utilize a single type of vibration motor and chest simulator, and explore a limited range of vibration conditions in terms of frequency and duration. Despite these constraints, we believe that our study demonstrates the feasibility of our proposed method. Moreover, we anticipate that employing a variety of chest simulators (e.g., those with different meat combinations), or actual deployment in patients' bodies, will not only maintain the functionality of our system, but potentially enhance its effectiveness. This improvement is expected due to the increased entropy level coming from the added randomness introduced by varying physical body characteristics.

Another aspect of future work is to empirically evaluate the susceptibility of our pairing technique against microphone-based eavesdropping attacks at a distance. In addition, we expect our method to be viable on commercial mobile devices, but we have not yet validated this. Future work could look at the practical aspects of implementation on a smartphone or tablet.

Conclusion

In this paper, we explore the potential of leveraging vibration to pair with an IMD. We propose a novel technique that uses a straightforward constant-frequency vibration to extract secrets from natural and random human motor behavior for device pairing. We implement and validate our technique through a user study. Overall, we show that it is feasible to establish a cryptographic key in 5 s with high usability, based only on standard vibration motors and accelerometers with low sampling capabilities. The ubiquity of accelerometers in today's commercial smart devices and IMDs maximizes the chance of acceptance of our design. In general, we hope that our work will serve as a reference for pairing with resource-constrained devices using vibrations in body area networks.

Acknowledgements

Mo Zhang is funded by the Priestley PhD Scholarship program organized by the University of Melbourne and University of Birmingham.

Conflicts of Interest

None declared.

Abbreviations

ERM: Eccentric rotating mass
FAR: False acceptance rate
FFT: Fast Fourier transform
FRR: False rejection rate
IMD: Implantable medical device
IoT: Internet of things
LRA: Linear resonant actuator
MITM: Man in the middle
OOB: Out-Of-Band
PAKE: Password-authenticated key agreement
RS: Reed-Solomon
SUS: System usability scale

Multimedia Appendix 1: Questionnaire and Interview Design.

We use a standard SUS questionnaire, which is widely accepted by the research community to assess usability. It consists of ten questions and provides participants with a five-point scale, ranging from “strongly disagree” to “strongly agree”. The results of the SUS questionnaire can be quantified into a score between zero and 100; a score higher than a threshold (usually 68) suggests good system usability. The complete list of questions is listed below.

(1) I think that I would like to use this pairing method frequently.
(2) I found the pairing unnecessarily complex.
(3) I thought the pairing method was easy to use.
(4) I think that I would need the support of a technical person to be able to pair.
(5) I found the various functions in this pairing method were well integrated.
(6) I thought there was too much inconsistency in this pairing method.
(7) I would imagine that most people would learn how to pair very quickly.
(8) I found the pairing method very cumbersome to use.
(9) I felt very confident using the pairing method.
(10) I needed to learn a lot of things before I could get going with this pairing method.

At the end of the user study, we asked each participant two interview questions to gain further insights. The conversation was recorded and analyzed by the principal researcher. The details of the questions are given below:

(1) Can you share your experiences of using the pairing method?
(2) Have you noticed anything uncomfortable in the pairing process?

References

1. Carlisle Adams and Steve Lloyd. 2003. Understanding PKI: concepts, standards, and deployment considerations. Addison-Wesley Professional. ISBN: 0672323915.
2. SA Adewusi, Subhash Rakheja, Patrice Marcotte, and J Boutin. 2010. Vibration transmissibility characteristics of the human hand–arm system under different postures, hand forces and excitation levels. Journal of sound and vibration; 329, 14:2953–2971.
3. S Adewusi, M Thomas, VH Vu, and W Li. 2014. Modal parameters of the human hand-arm using finite element and operational modal analysis. Mechanics & Industry 15, 6:541–549.
4. Imtiaj Ahmed, Yina Ye, Sourav Bhattacharya, Nadarajah Asokan, Giulio Jacucci, Petteri Nurmi, and Sasu Tarkoma. 2015. Checksum gestures: continuous gestures as an out-of-band channel for secure pairing. In Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing:391–401.
5. S Abhishek Anand and Nitesh Saxena. 2017. Coresident Evil: Noisy Vibrational Pairing in the Face of Co-Located Acoustic Eavesdropping. In Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks:173–183.
6. S Abhishek Anand and Nitesh Saxena. 2018. Noisy vibrational pairing of IoT devices. IEEE Transactions on Dependable and Secure Computing 16, 3:530–545.
7. ARM. 2022. CMSIS DSP software library, Real FFT Functions. https://www.keil.com/pack/doc/CMSIS/DSP/html/group RealFFT.html.
8. Steven Michael Bellovin and Michael Merritt. 1992. Encrypted key exchange: Password-based protocols secure against dictionary attacks.
9. Gerald Bieber, Thomas Kirste, and Michael Gaede. 2014. Low sampling rate for physical activity recognition. In Proceedings of the 7th international conference on pervasive

technologies related to assistive environments:1–8.
10. C. Bisdikian. 2001. An overview of the Bluetooth wireless technology. IEEE Communications Magazine 39, 12:86–94. https://doi.org/10.1109/35.968817
11. Massimo Bovenzi et al. 2005. Health effects of mechanical vibration. G Ital Med Lav Ergon 27, 1: 58–64.
12. Joan Daemen and Vincent Rijmen. 1999. AES proposal: Rijndael. (1999).
13. Michael Hamman De Vaal, James Neville, Jacques Scherman, Peter Zilla, Micah Litow, and Thomas Franz. 2010. The in vivo assessment of mechanical loadings on pectoral pacemaker implants. Journal of biomechanics 43, 9:1717–1722.
14. Tamara Denning, Kevin Fu, and Tadayoshi Kohno. 2008. Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security. In Proceedings of the 3rd Conference on Hot Topics in Security. USENIX Association, USA, Article 5, 7 pages.
15. Tim Dierks and Christopher Allen. 1999. The TLS protocol version 1.0. Technical Report.
16. Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. 2008. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM journal on computing 38, 1:97–139.
17. D. Dolev and A. Yao. 1983. On the security of public key protocols. IEEE Transactions on Information Theory 29, 2:198–208. https://doi.org/10.1109/TIT.1983.1056650
18. Robert W Doran. 2007. The gray code. Technical Report. Department of Computer Science, The University of Auckland, New Zealand.
19. Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. 2011. They can hear your heartbeats: Non-invasive security for implantable medical devices. In Proceedings of the ACM SIGCOMM 2011 conference:2–13.
20. Tzipora Halevi and Nitesh Saxena. 2010. On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping. In Proceedings of the 17th ACM conference on Computer and communications security:97–108.
21. Daniel Halperin, Thomas S Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H Maisel. 2008. Security and privacy for implantable medical devices. IEEE pervasive computing 7, 1:30–39.
22. Daniel Halperin, Thomas S Heydt-Benjamin, Benjamin Ransford, Shane S Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H Maisel. 2008. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In 2008 IEEE Symposium on Security and Privacy. IEEE:129–142.
23. Ran Halprin and Moni Naor. 2009. Games for extracting randomness. In Proceedings of the 5th Symposium on Usable Privacy and Security:1–12.
24. Jun Han, Albert Jin Chung, Manal Kumar Sinha, Madhumitha Harishankar, Shijia Pan, Hae Young Noh, Pei Zhang, and Patrick Tague. 2018. Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types. In 2018 IEEE symposium on Security and Privacy. IEEE:836–852.
25. Maryam Hedayati, Shima Sum, Seyed Reza Hosseini, Mahbobeh Faramarzi, and Samaneh Pourhadi. 2019. Investigating the effect of physical games on the memory and attention of the elderly in adult day-care centers in Babol and Amol. Clinical interventions in aging:859–869.
26. InvenSense. 2013. MPU-6000 and MPU-6050 Product Specification Revision 3.4. https://invensense.tdk.com/wp-content/uploads/2015/0 2/MPU-6000-Datasheet1.pdf.
27. Jonathan Katz, Rafail Ostrovsky, and Moti Yung. 2002. Forward secrecy in password-only key exchange protocols. In International Conference on Security in Communication Networks. Springer, 29–44.
28. Aftab Khan, Nils Hammerla, Sebastian Mellor, and Thomas Plötz. 2016. Optimising sampling rates for accelerometer-based human activity recognition. Pattern Recognition

Letters 73 (2016), 33–40.
29. Younghyun Kim, Woo Suk Lee, Vijay Raghunathan, Niraj K Jha, and Anand Raghunathan. 2015. Vibration-based secure side channel for medical devices. In 2015 52nd ACM/EDAC/ IEEE Design Automation Conference. IEEE, 1–6.
30. Kyuin Lee, Vijay Raghunathan, Anand Raghunathan, and Younghyun Kim. 2018. SYNCVIBE: Fast and secure device pairing through physical vibration on commodity smartphones. In 2018 IEEE 36th International Conference on Computer Design. IEEE, 234–241.
31. James R Lewis. 2018. The system usability scale: past, present, and future. International Journal of Human–Computer Interaction 34, 7 (2018), 577–590.
32. Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. In The 25th Annual International Conference on Mobile Computing and Networking. Association for Computing Machinery, New York, NY, USA, Article 33, 17 pages.
33. Xiaopeng Li, Qiang Zeng, Lannan Luo, and Tongbo Luo. 2020. T2pair: Secure and usable pairing for heterogeneous iot devices. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. 309–323.
34. Qi Lin, Weitao Xu, Jun Liu, Abdelwahed Khamis, Wen Hu, Mahbub Hassan, and Aruna Seneviratne. 2019. H2B: Heartbeat-based secret key generation using piezo vibration sensors. In Proceedings of the 18th International Conference on Information Processing in Sensor Networks. 265–276.
35. Shu Lin and Daniel J Costello. 2001. Error control coding. Vol. 2. Prentice hall.
36. Eduard Marin, Enrique Argones Rúa, Dave Singelée, and Bart Preneel. 2019. On the Difficulty of Using Patient's Physiological Signals in Cryptographic Protocols. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies. Association for Computing Machinery, New York, NY, USA, 113–122.
37. Eduard Marin, Dave Singelée, Flavio D Garcia, Tom Chothia, Rik Willems, and Bart Preneel. 2016. On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them. In Proceedings of the 32nd annual conference on computer security applications. 226–236.
38. Eduard Marin, Dave Singelée, Bohan Yang, Ingrid Verbauwhede, and Bart Preneel. 2016. On the feasibility of cryptography for a wireless insulin pump system. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. 113–120.
39. Eduard Marin, Dave Singelée, Bohan Yang, Vladimir Volski, Guy AE Vandenbosch, Bart Nuttin, and Bart Preneel. 2018. Securing wireless neurostimulators. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 287–298.
40. Rene Mayrhofer and Hans Gellersen. 2009. Shake well before use: Intuitive and secure pairing of mobile devices. IEEE Transactions on Mobile Computing 8, 6 (2009), 792–806.
41. Medtronic. 2016. Rate Response Feature. https://www.medtronicacademy.com/features/rate-response-rr-feature.
42. Medtronic. 2021. MyCarelink heart mobile app. https://global.medtronic.com/xg-en/mobileapps/patient-caregiver/cardiac-monitoring/mycarelink-heart-app.html.
43. Medtronic. 2022. Azure Pacing System. https://europe.medtronic.com/xd-en/healthcare-professionals/products/cardiac- rhythm/pacemakers/azure.html
44. Medtronic. n.d.. Medtronic Sensor. https://www.cardiocases.com/en/pacingdef ibrillation/specif icities/programming- exercise/medtronic/medtronic-sensor.
45. Precision Microdrives. 2021. Model No. 307-103 Vibration Motor. https://catalogue.precisionmicrodrives.com/product/datasheet/307- 103-9mm-vibration-motor-25mm-type-datasheet.pdf.
46. Precision Microdrives. 2021. Vibration Motors – ERMs and LRAs. https://www.precisionmicrodrives.com/vibration-motors-erms-and- lras.
47. Anna S. Petronio, Jan-Malte Sinning, Nicolas Van Mieghem, Giulio Zucchelli, Georg Nickenig, Raffi Bekeredjian, Johan Bosmans, Francesco Bedogni, Marian Branny, Karl Stangl, Jan Kovac, Molly Schiltgen, Stacia Kraus, and Peter de Jaegere. 2015. Optimal

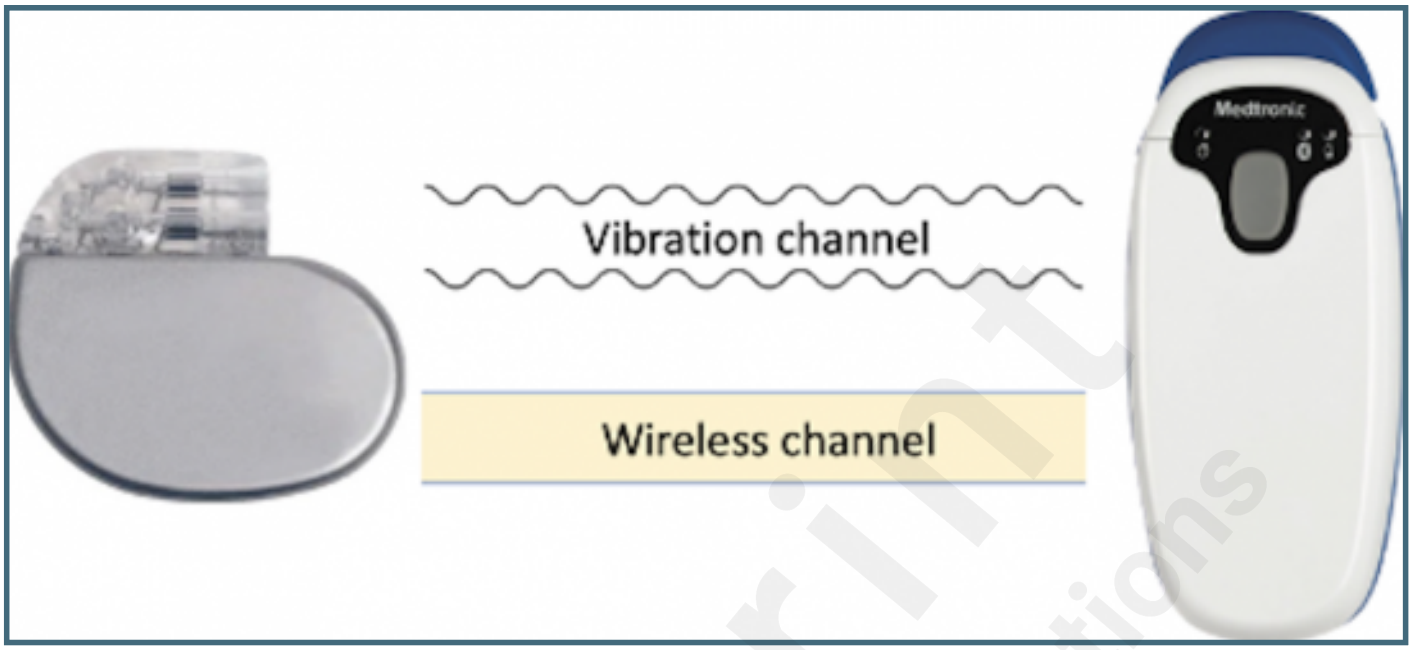
Implantation Depth and Adherence to Guidelines on Permanent Pacing to Improve the Results of Transcatheter Aortic Valve Replacement With the Medtronic CoreValve System: The CoreValve Prospective, International, Post-Market ADVANCE-II Study. JACC: Cardiovascular Interventions 8, 6 (2015), 837–846.
48. C.C.Y. Poon, Yuan-Ting Zhang, and Shu-Di Bao. 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communications Magazine 44, 4 (2006), 73–81.
49. Venkata K Puppala, Benjamin C Hofeld, Amberly Anger, Sudhi Tyagi, Scott J Strath, Judith Fox, Marcie G Berger, Kwang Woo Ahn, and Michael E Widlansky. 2020. Pacemaker detected active minutes are superior to pedometer-based step counts in measuring the response to physical activity counseling in sedentary older adults. BMC geriatrics 20, 1 (2020), 1–11.
50. Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S Heydt-Benjamin, and Srdjan Capkun. 2009. Proximity-based access control for implantable medical devices. In Proceedings of the 16th ACM conference on Computer and communications security. 410–419.
51. Luca Reverberi and David Oswald. 2017. Breaking (and fixing) a widely used continuous glucose monitoring system. In 11th USENIX Workshop on Offensive Technologies.
52. Eduardo Arrais Rocha, Gisele Schineider Cunha, Aline Bezerra Tavares, Antônio Brazil Viana Júnior, Ana Rosa Pinto Quidute, Francisca Tatiana Moreira Pereira, Marcelo de Paula Martins Monteiro, Maria Eduarda Quidute Arrais Rocha, Camila Rabelo Ferreira Gomes, and Carlos Roberto Martins Rodrigues Sobrinho. 2020. Syncope in patients with cardiac pacemakers. Brazilian Journal of Cardiovascular Surgery 36 (2020), 18–24.
53. Masoud Rostami, Ari Juels, and Farinaz Koushanfar. 2013. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In Proceedings of Conference on Computer and Communications Security. 1099–1112.
54. Nirupam Roy and Romit Roy Choudhury. 2016. Ripple {II}: Faster communication through physical vibration. In 13th USENIX Symposium on Networked Systems Design and Implementation. 671–684.
55. Nirupam Roy, Mahanth Gowda, and Romit Roy Choudhury. 2015. Ripple: Communicating through physical vibration. In 12th USENIX Symposium on Networked Systems Design and Implementation. 265–278.
56. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, M Levenson, M Vangel, D Banks, Nathanael Heckert, James Dray, and S Vo. 2001. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.
57. Michael Rushanan, Aviel D Rubin, Denis Foo Kune, and Colleen M Swanson. 2014. Sok: Security and privacy in implantable medical devices and body area networks. In 2014 IEEE symposium on security and privacy. IEEE, 524–539.
58. Jonghyun Ryu. 2010. Psychophysical model for vibrotactile rendering in mobile devices. Presence 19, 4 (2010), 364–387.
59. Nitesh Saxena, Md Borhan Uddin, and Jonathan Voris. 2009. Treat'em like other devices: user authentication of multiple personal RFID tags. In SOUPS, Vol. 9. 1–1.
60. Nitesh Saxena, Md Borhan Uddin, Jonathan Voris, and N Asokan. 2011. Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In 2011 IEEE International Conference on Pervasive Computing and Communications. IEEE, 181–188.
61. Stuart Schechter. 2010. Security That Is Meant to Be Skin Deep: Using Ultraviolet Micropigmentation to Store Emergency-Access Keys for Implantable Medical Devices. In 1st USENIX Workshop on Health Security and Privacy. USENIX Association, Washington, DC.
62. Robert Mark Seepers, Wenjin Wang, Gerard De Haan, Ioannis Sourdis, and Christos Strydis. 2017. Attacks on heartbeat-based security using remote photoplethysmography. IEEE journal of biomedical and health informatics 22, 3 (2017), 714–721.
63. Helmut Seidel. 1993. Selected health risks caused by long-term, whole-body vibration. American journal of industrial medicine 23, 4 (1993), 589–604.

64. Statista. 2022. Global number of pacemakers in 2016 and a forecast for 2023. https://www.statista.com/statistics/800794/pacemakers- market-volume-in-units-worldwide.
65. Matthew Stenerson, Fraser Cameron, Shelby R Payne, Sydney L Payne, Trang T Ly, Darrell M Wilson, and Bruce A Buckingham. 2014. The impact of accelerometer use in exercise-associated hypoglycemia prevention in type 1 diabetes. Journal of diabetes science and technology 9, 1 (2014), 80–85.
66. Matthew Stenerson, Fraser Cameron, Darrell M Wilson, Breanne Harris, Shelby Payne, B Wayne Bequette, and Bruce A Buckingham. 2014. The impact of accelerometer and heart rate data on hypoglycemia mitigation in type 1 diabetes. Journal of diabetes science and technology 8, 1 (2014), 64–69.
67. MTCAJ Thomas and A Thomas Joy. 2006. Elements of information theory. Wiley-Interscience.
68. William J Tomlinson, Stella Banou, Christopher Yu, Michele Nogueira, and Kaushik R Chowdhury. 2019. Secure on-skin biometric signal transmission using galvanic coupling. In IEEE Conference on Computer Communications. IEEE, 1135–1143.
69. Chaofan Wang, Zhanna Sarsenbayeva, Chu Luo, Jorge Goncalves, and Vassilis Kostakos. 2019. Improving Wearable Sensor Data Quality Using Context Markers. In Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers. Association for Computing Machinery, New York, NY, USA, 598–601. https://doi.org/10.1145/3341162.3349334
70. Wang Wei, Lin Yang, and Qian Zhang. 2018. Resonance-based secure pairing for wearables. IEEE Transactions on Mobile Computing 17, 11 (2018), 2607–2618.
71. Robert Xiao, Sven Mayer, and Chris Harrison. 2020. Vibrocomm: Using commodity gyroscopes for vibroacoustic data reception. In 22nd International Conference on Human-Computer Interaction with Mobile Devices and Services. 1–9.
72. Fengyuan Xu, Zhengrui Qin, Chiu C Tan, Baosheng Wang, and Qun Li. 2011. IMDGuard: Securing implantable medical devices with the external wearable guardian. In 2011 Proceedings IEEE INFOCOM. IEEE, 1862–1870.
73. Li Zhang, Parth H Pathak, Muchen Wu, Yixin Zhao, and Prasant Mohapatra. 2015. Accelword: Energy efficient hotword detection through accelerometer. In Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and services.
74. Mo Zhang, Eduard Marin, David Oswald, and Dave Singelée. 2022. FuzzyKey: Comparing Fuzzy Cryptographic Primitives on Resource-Constrained Devices. In Smart Card Research and Advanced Applications, Vincent Grosso and Thomas Pöppelmann (Eds.). Springer International Publishing, Cham, 289–309.
75. The anonymous materials involved in our research. https://osf.io/tk56r/?view_only=2be015b407474ac1a97f1bcca682d991

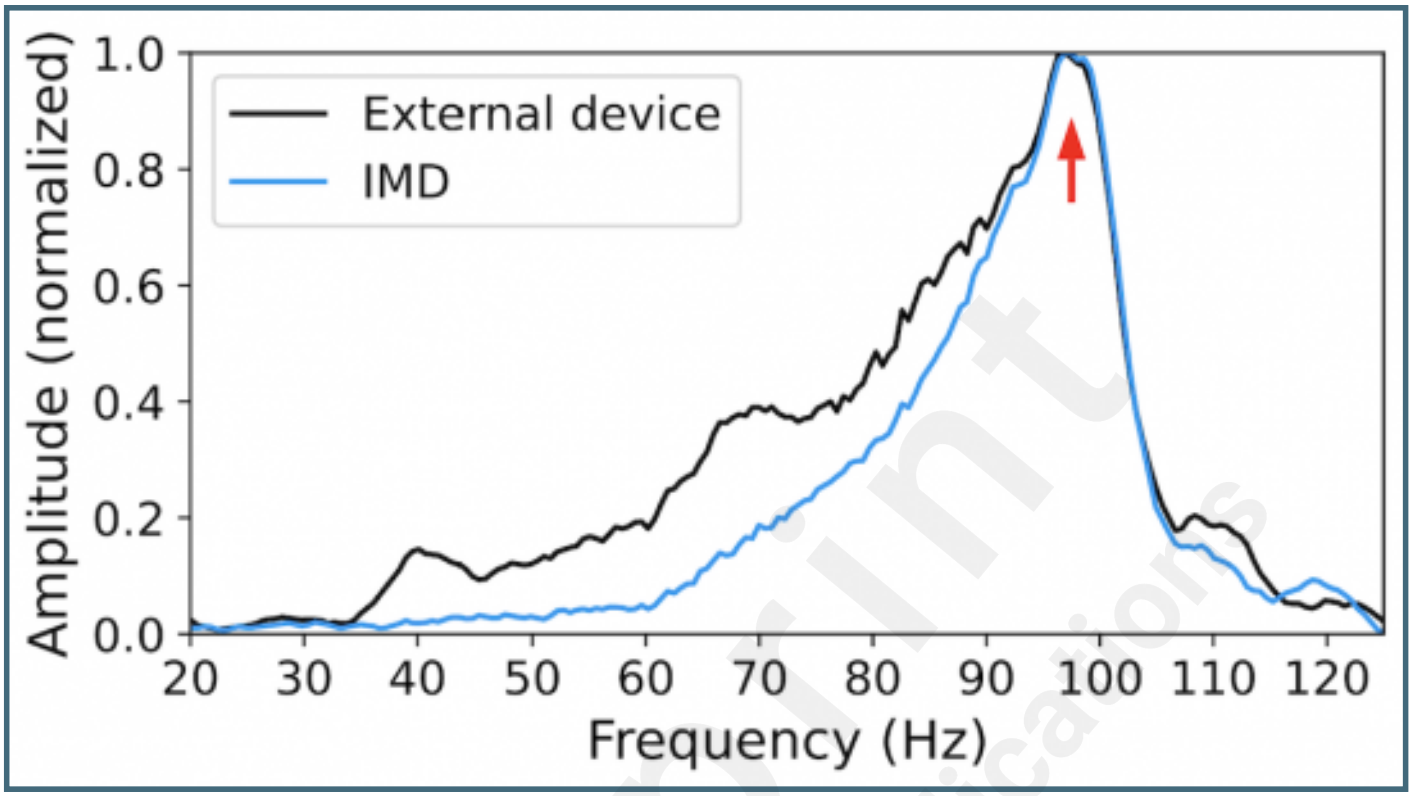
Supplementary Files

Figures

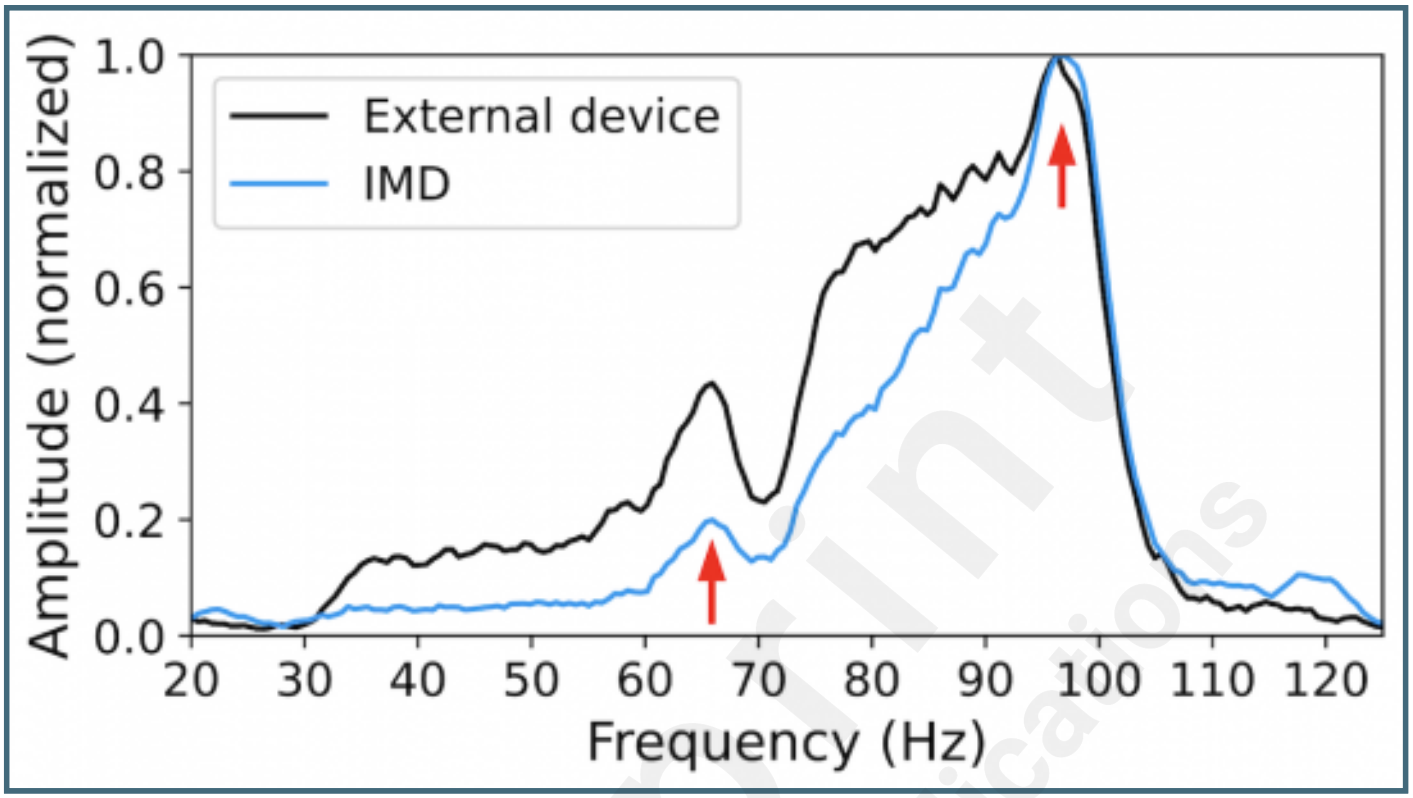
IMD and external device. The vibration channel is used to exchange a key that subsequently secures the wireless channel.



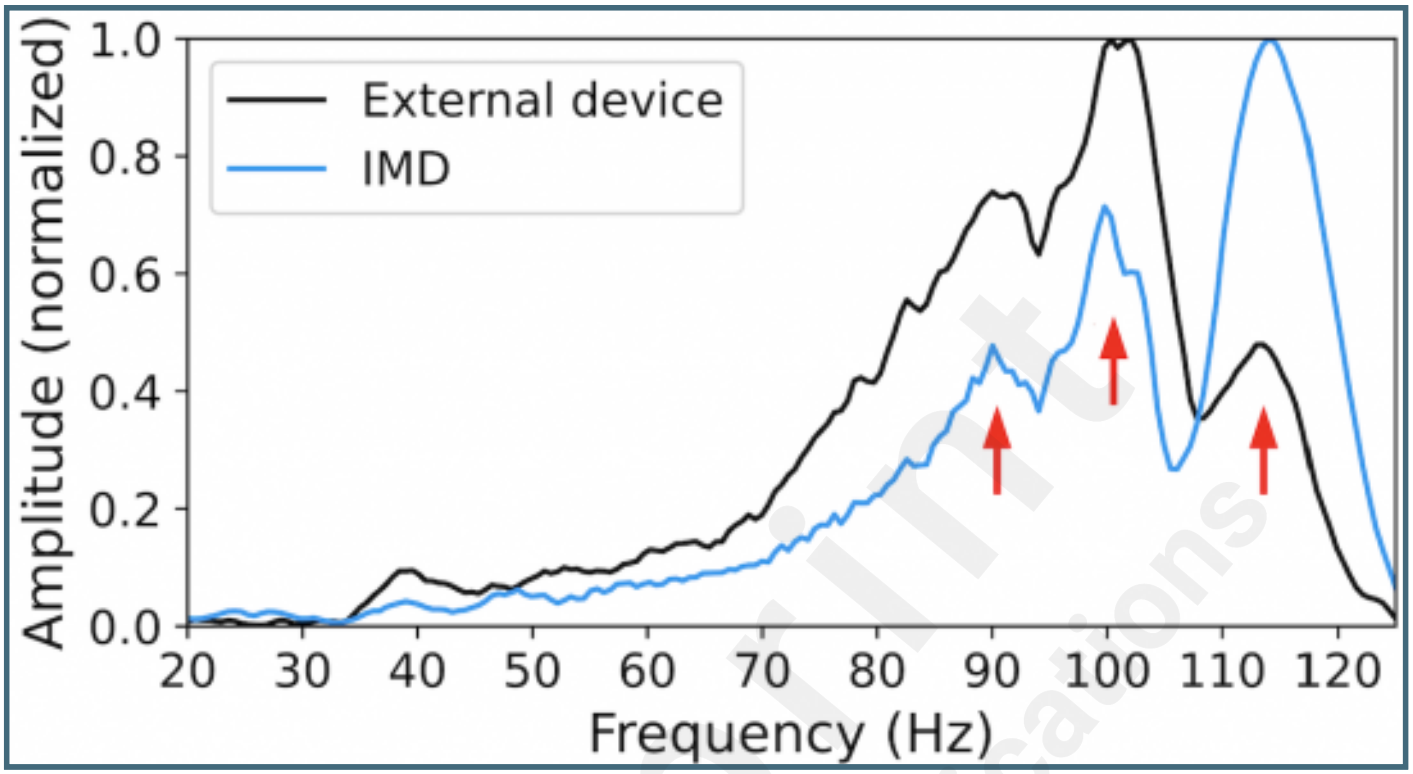
With one stable peak (72%).



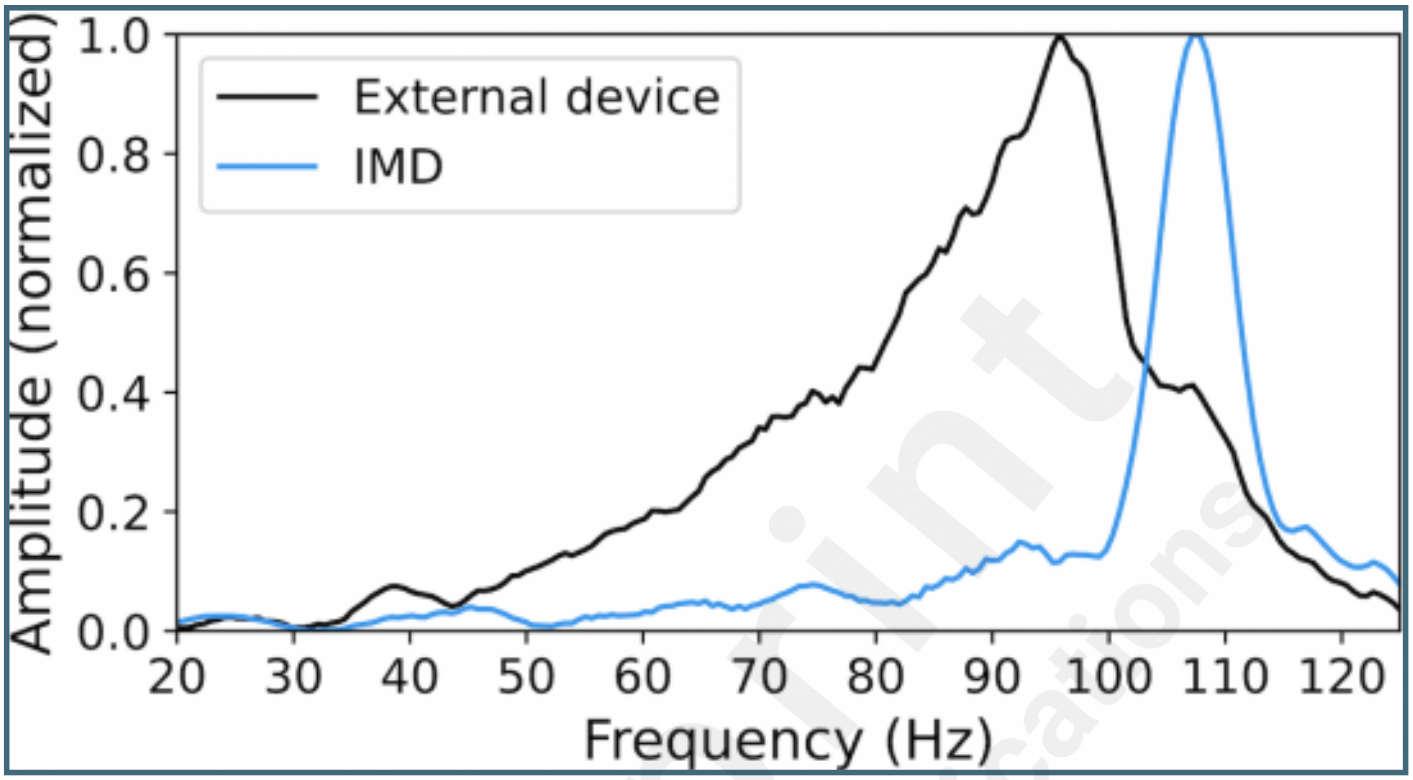
With two stable peaks (17%).



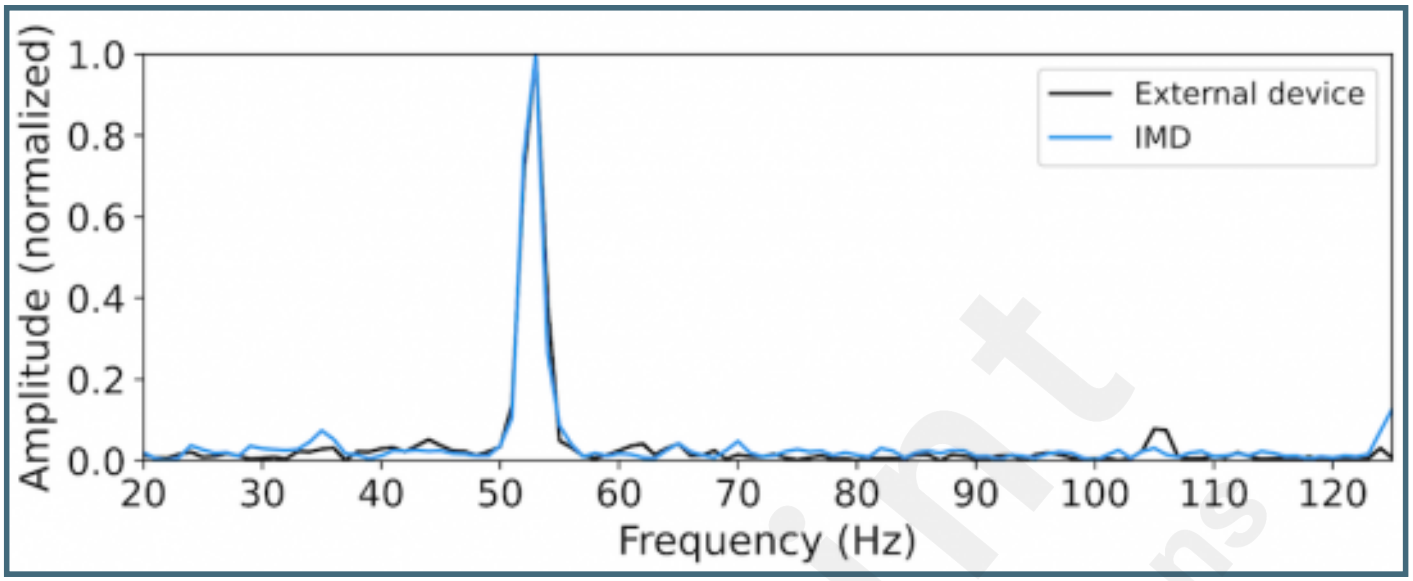
With three stable peaks (2%).



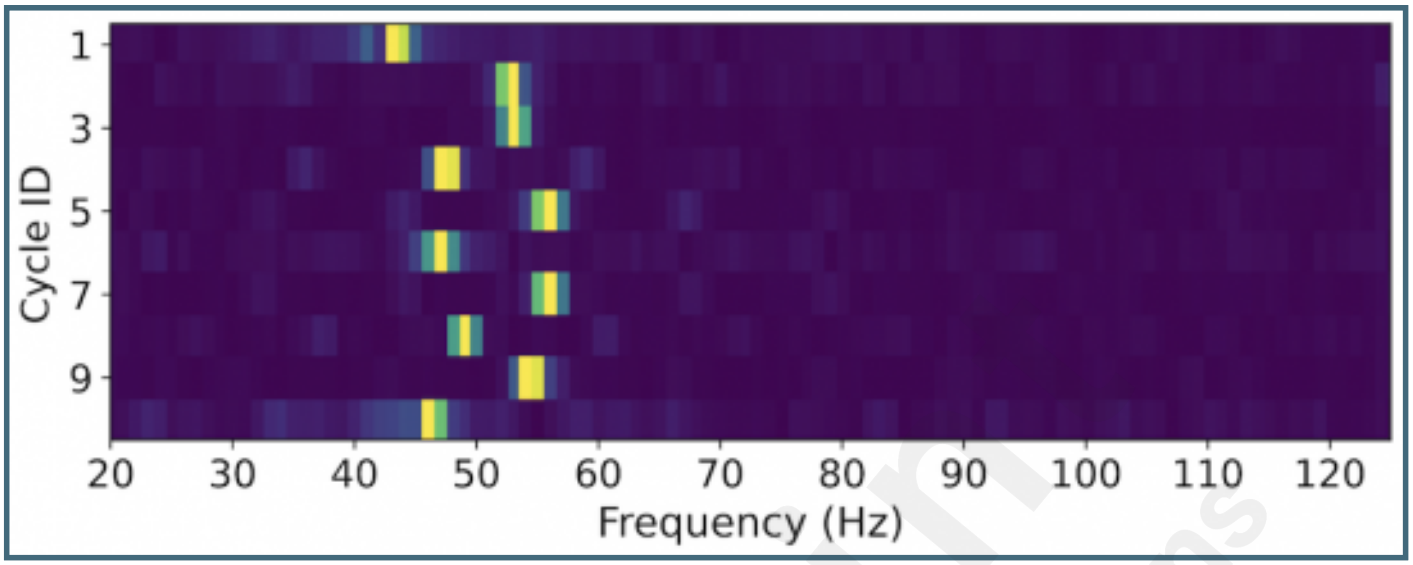
Noisy data (9%).



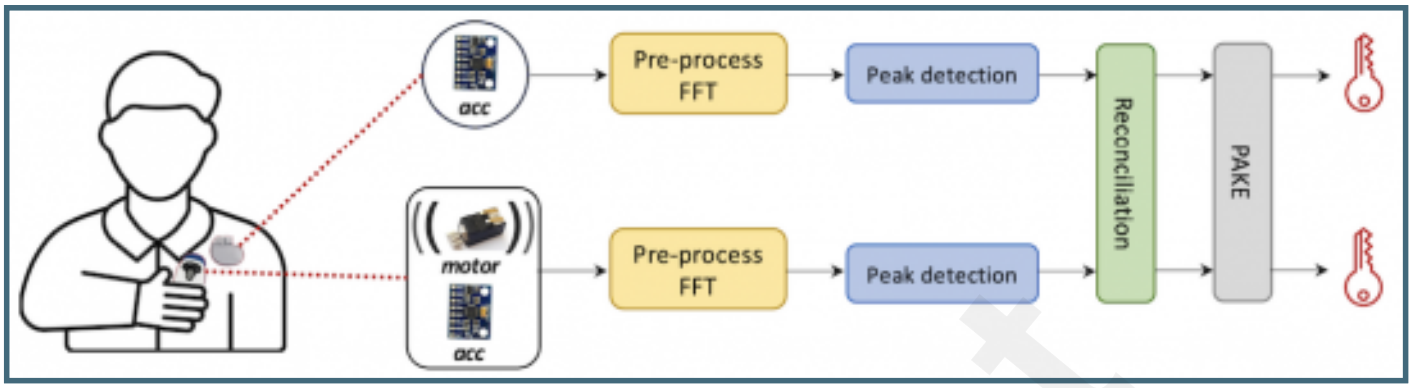
Frequency spectrum given a constant vibration (50 Hz, 1 s) in one cycle.



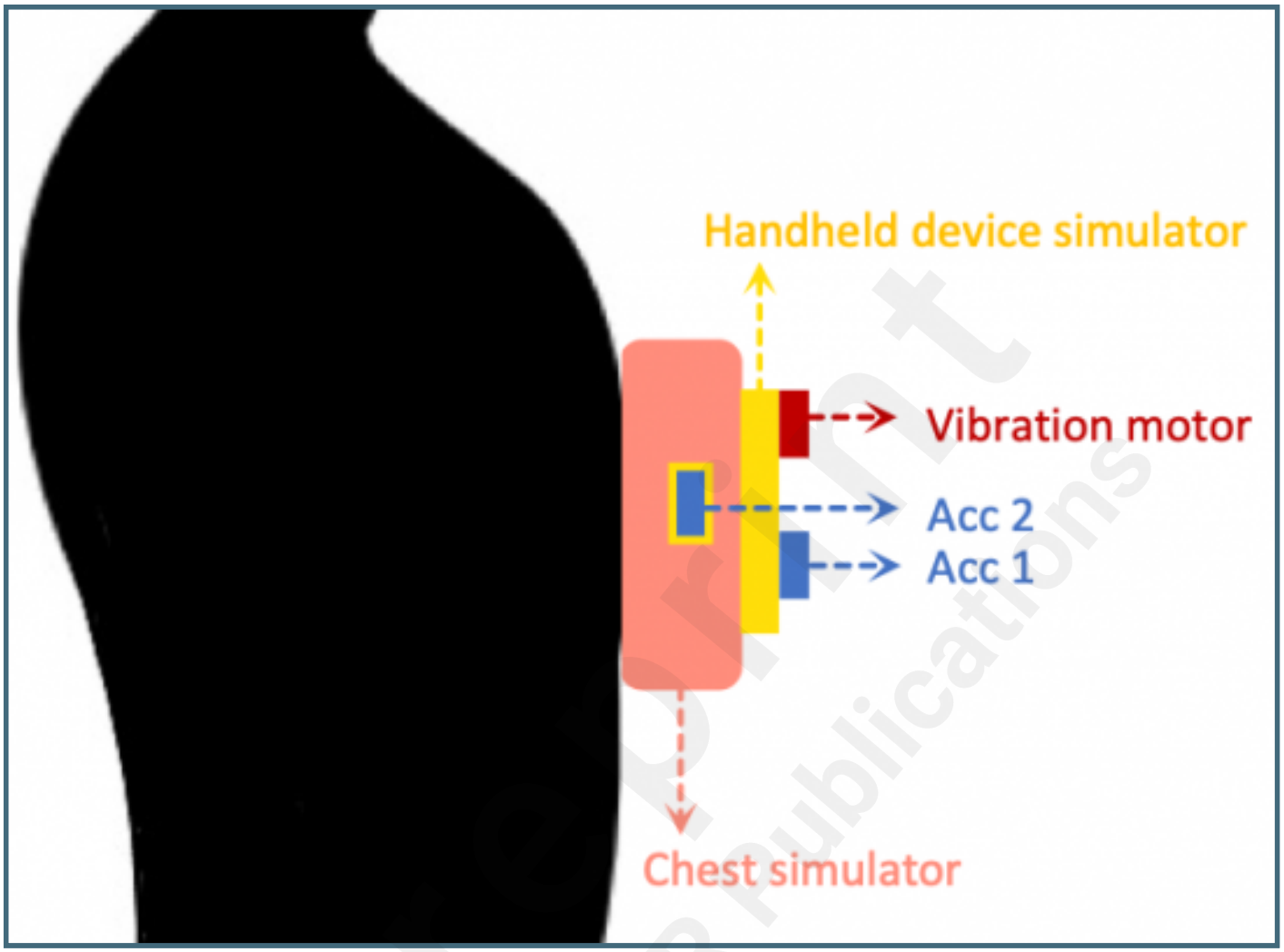
Frequency spectrum of IMD, given a constant vibration (50 Hz, 1 s) in ten consecutive cycles.



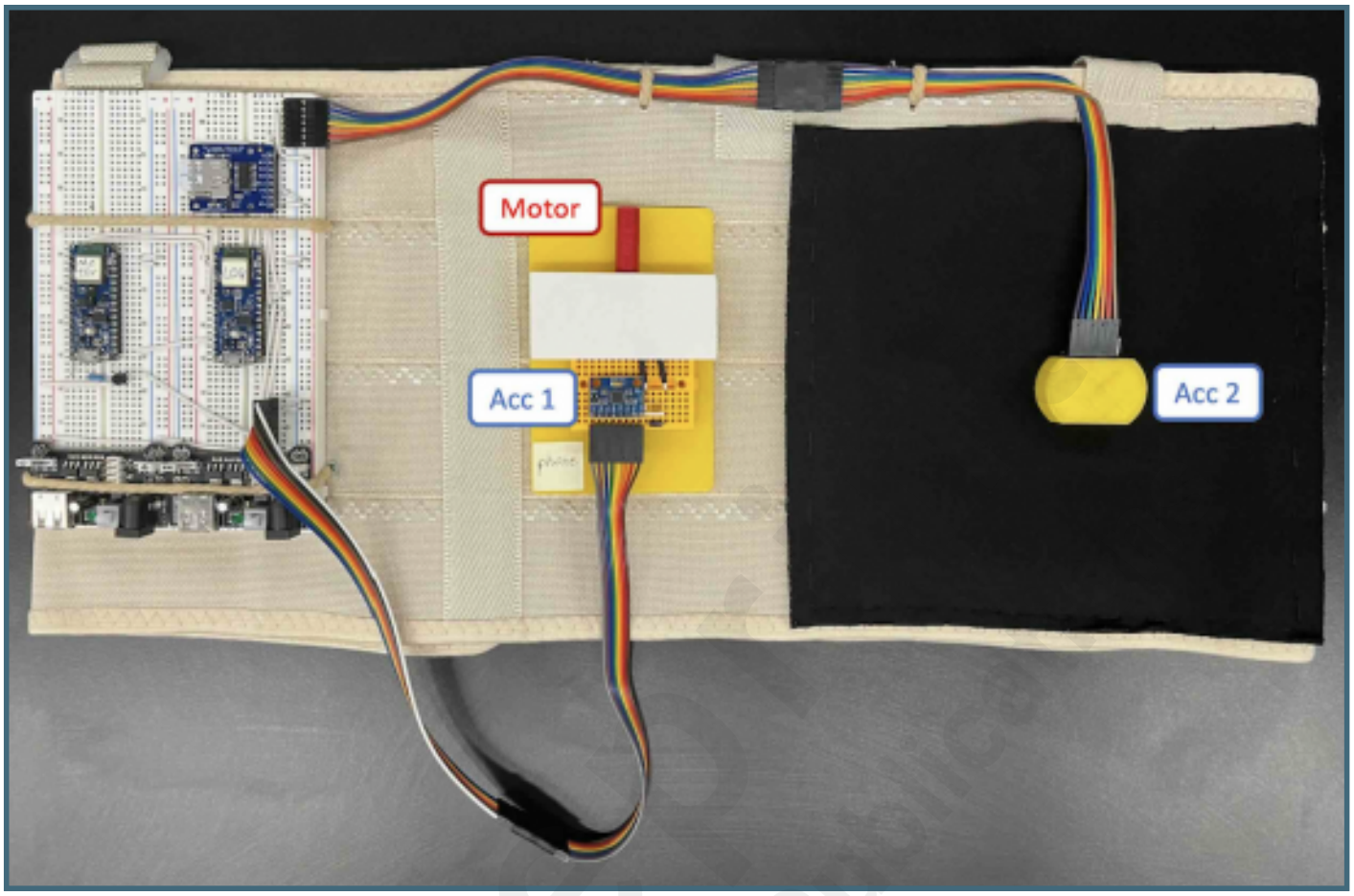
An overview of our pairing technique.



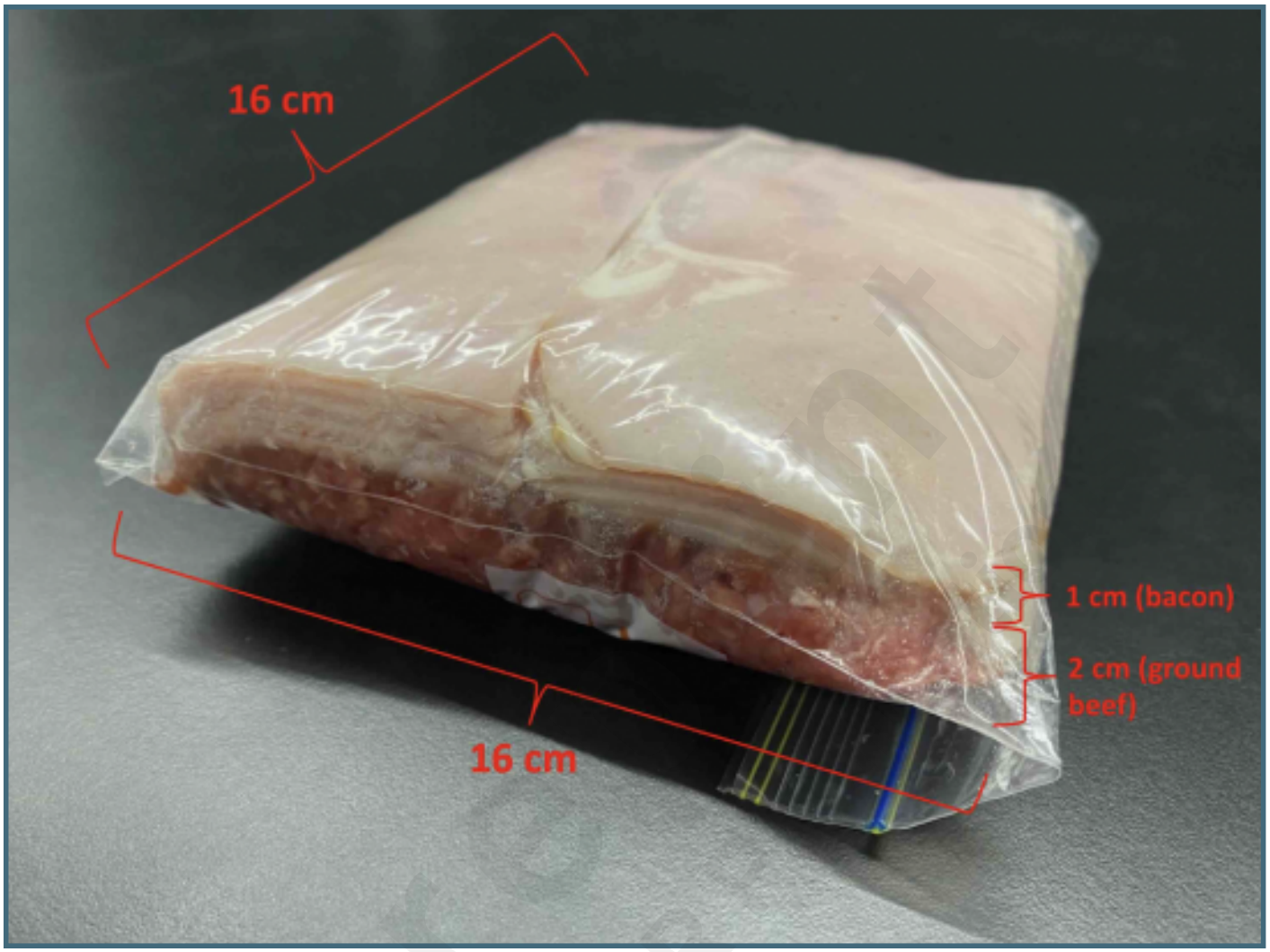
Prototype overview.



Hardware setup.

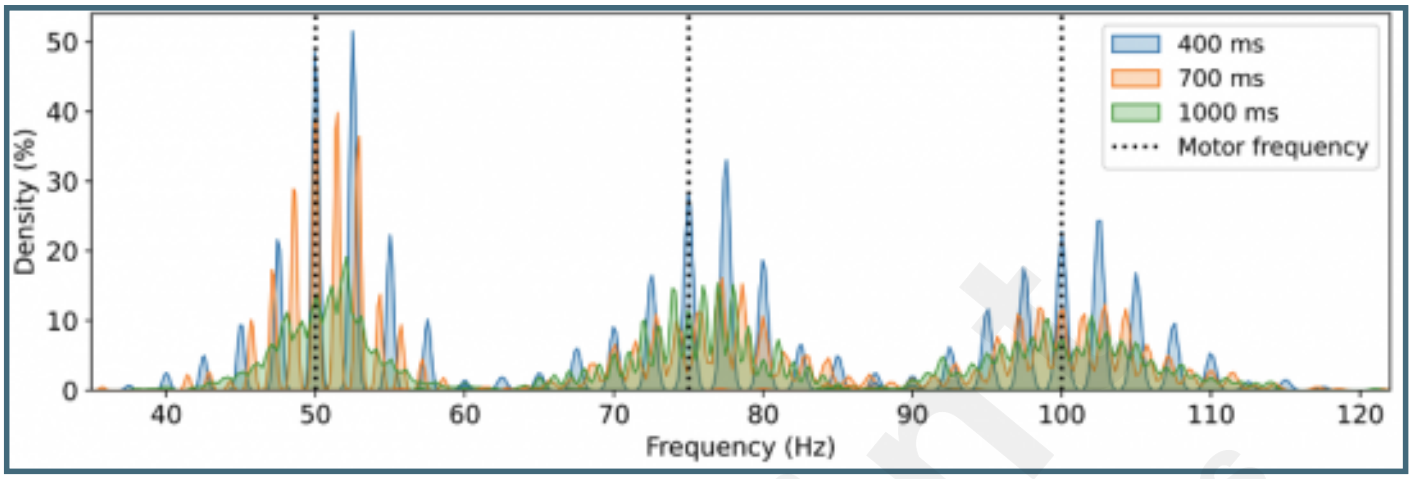


Chest simulator.

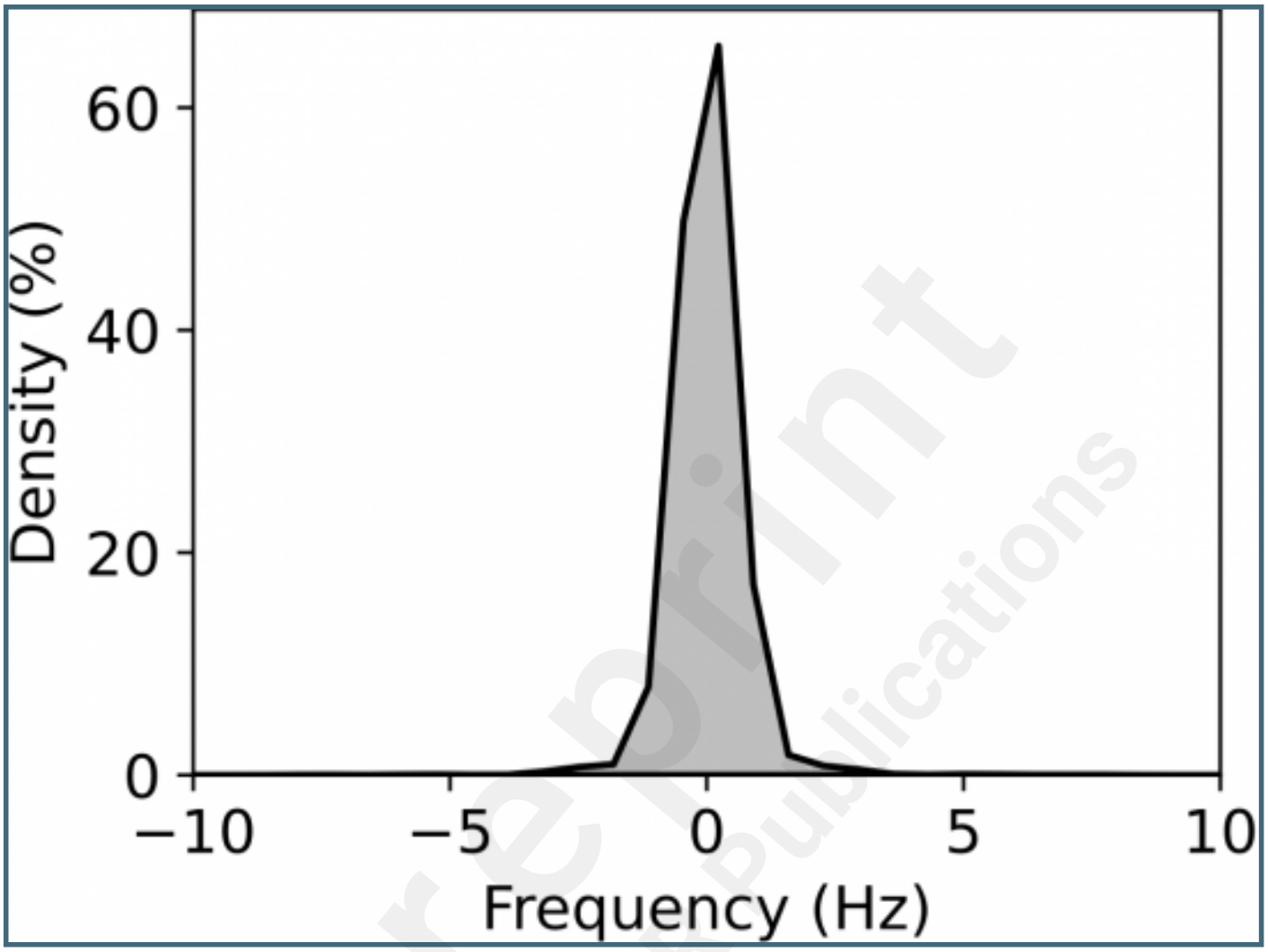


Participant in user study.

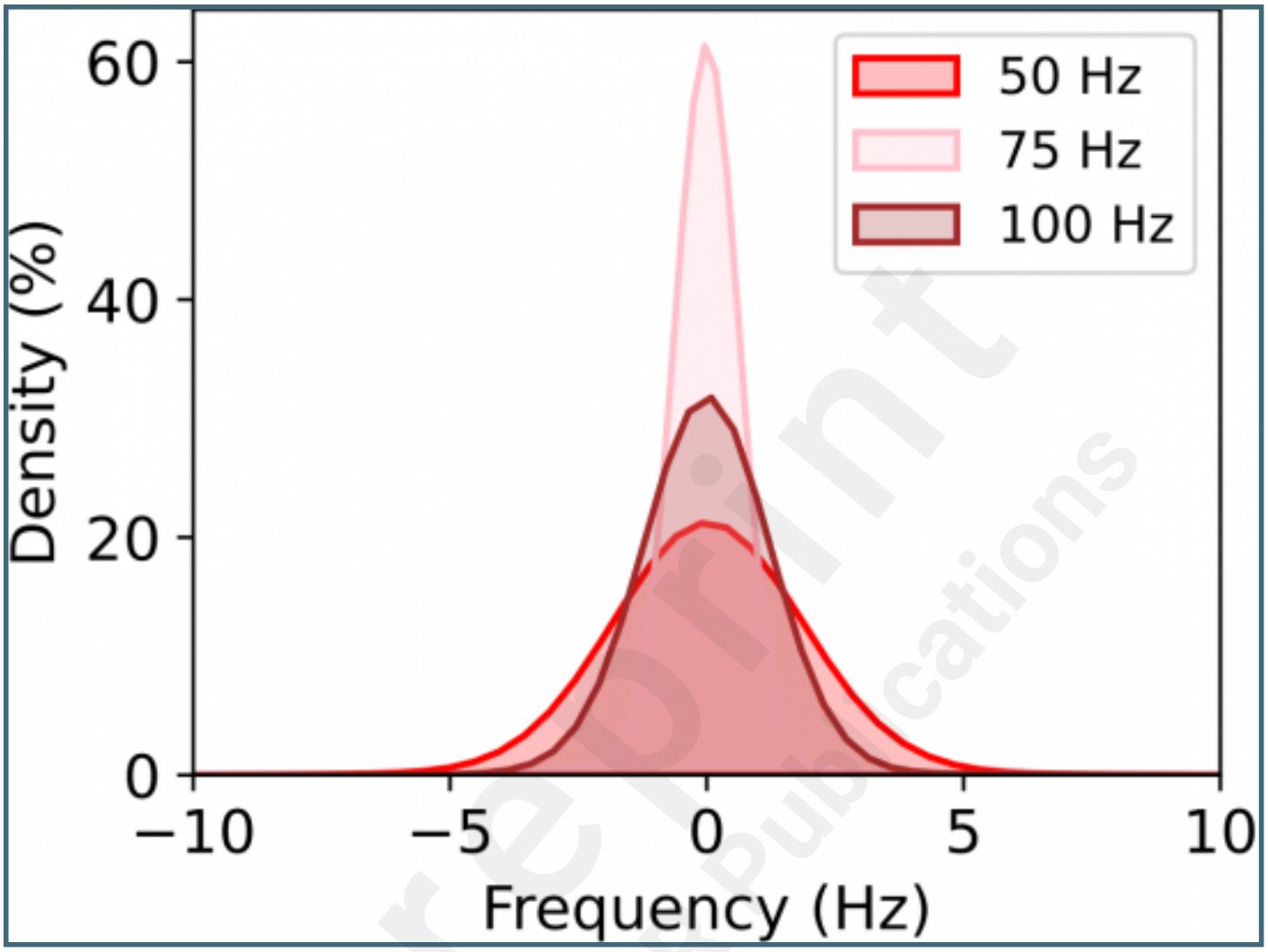
Distribution of peak location measured by the IMD among 24 participants. The black dashed lines indicate frequencies of the vibration motor.



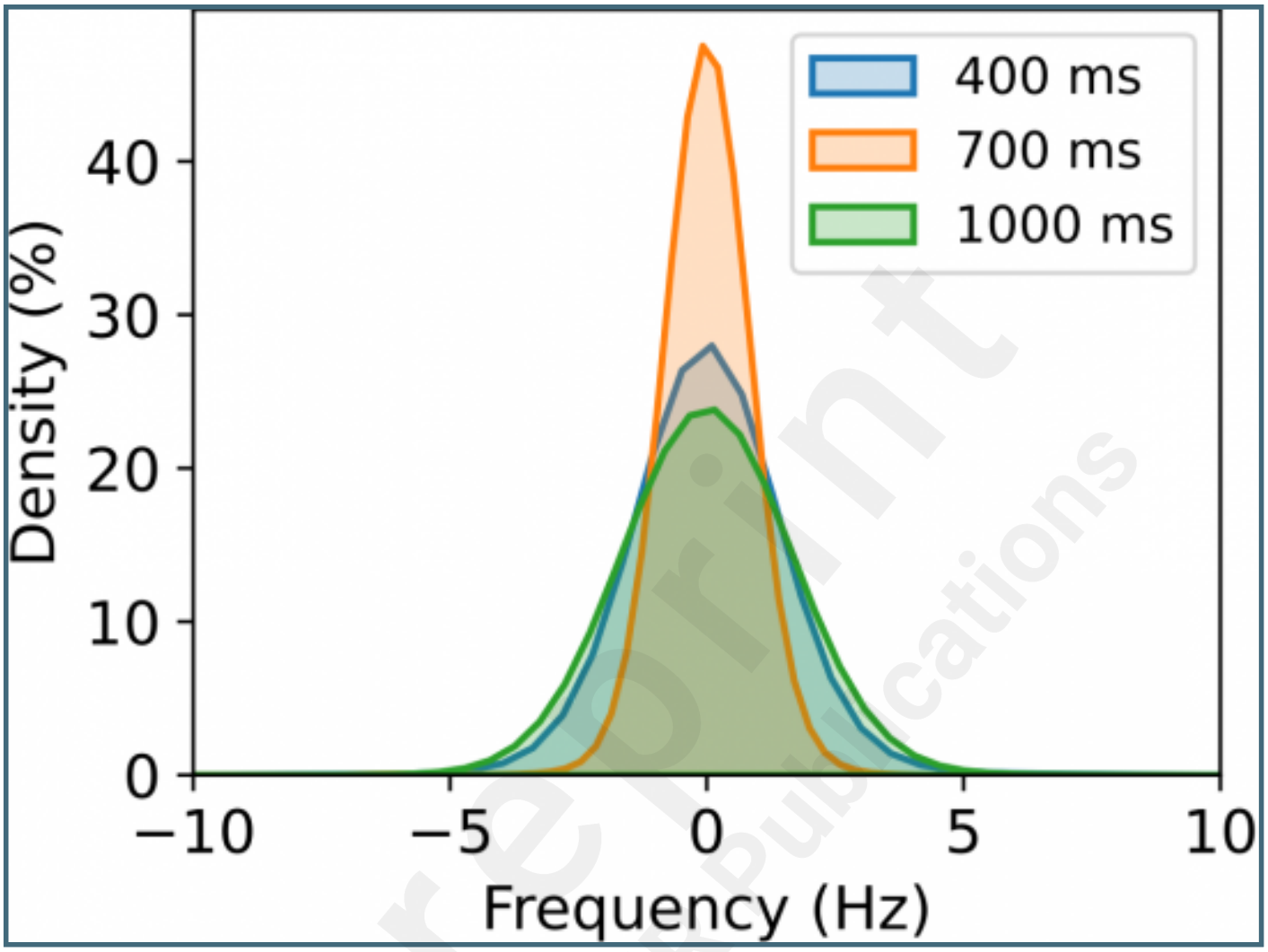
Mismatch of all data among 24 participants.



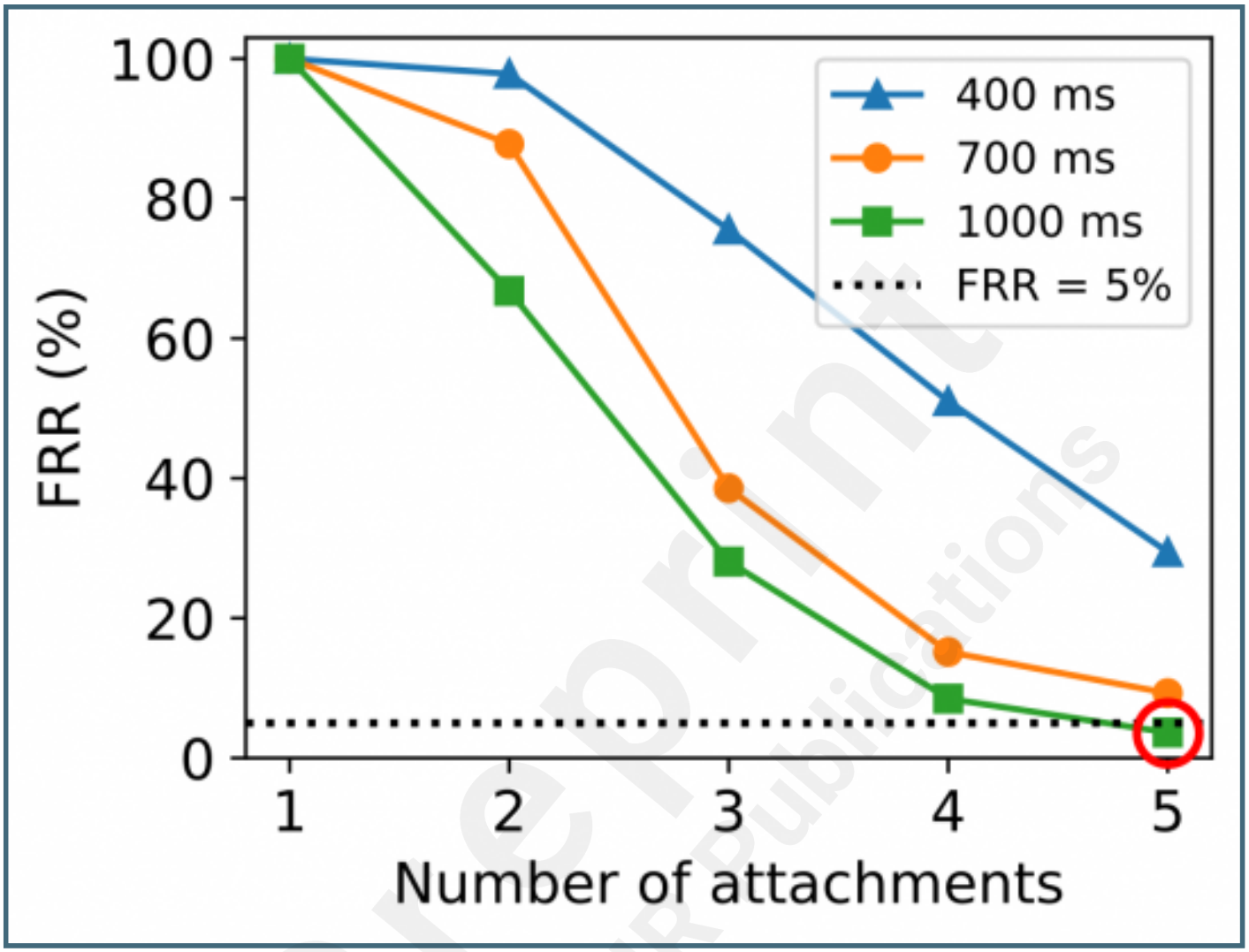
Mismatch with vibration frequency among 24 participants.



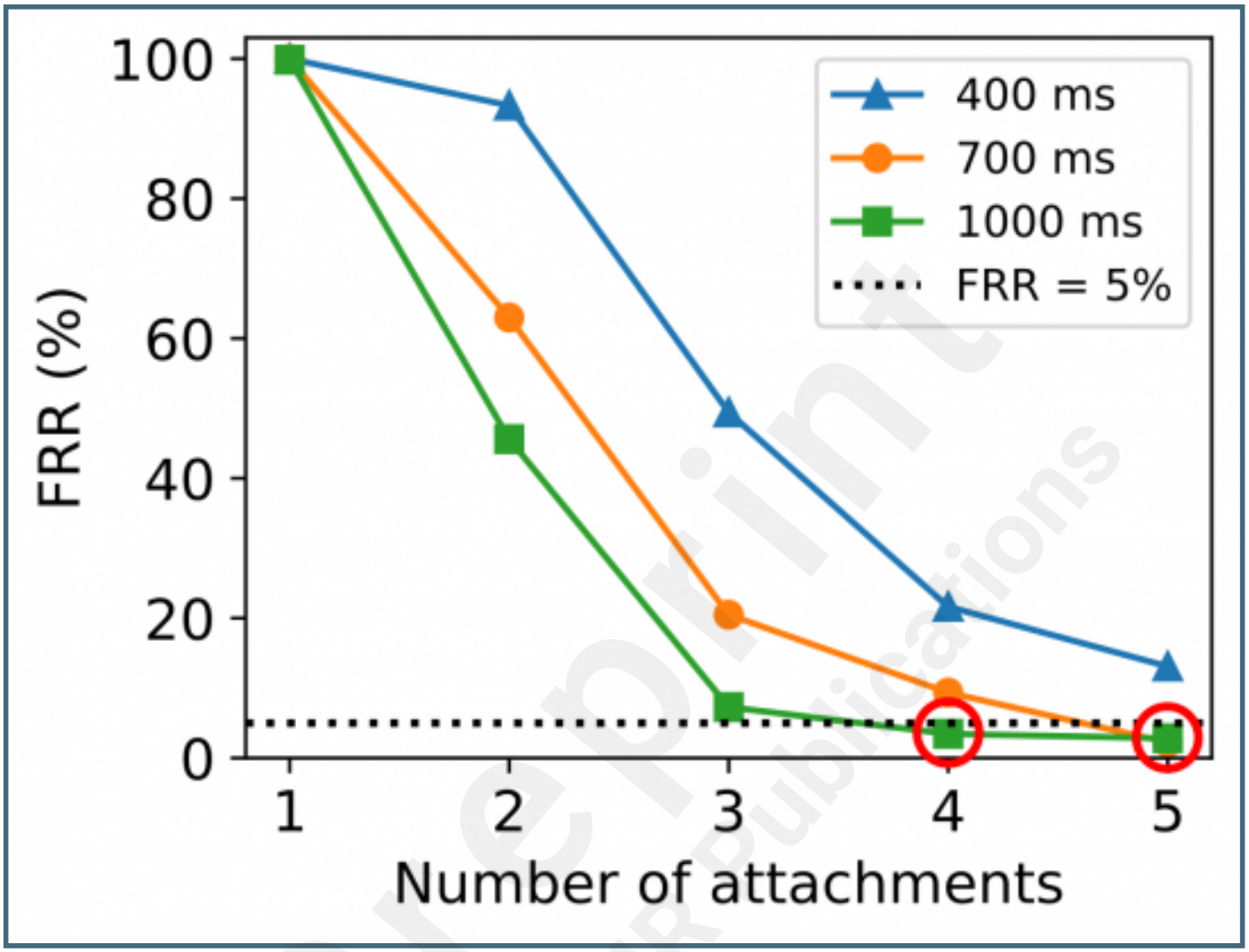
Mismatch with vibration time among 24 participants.



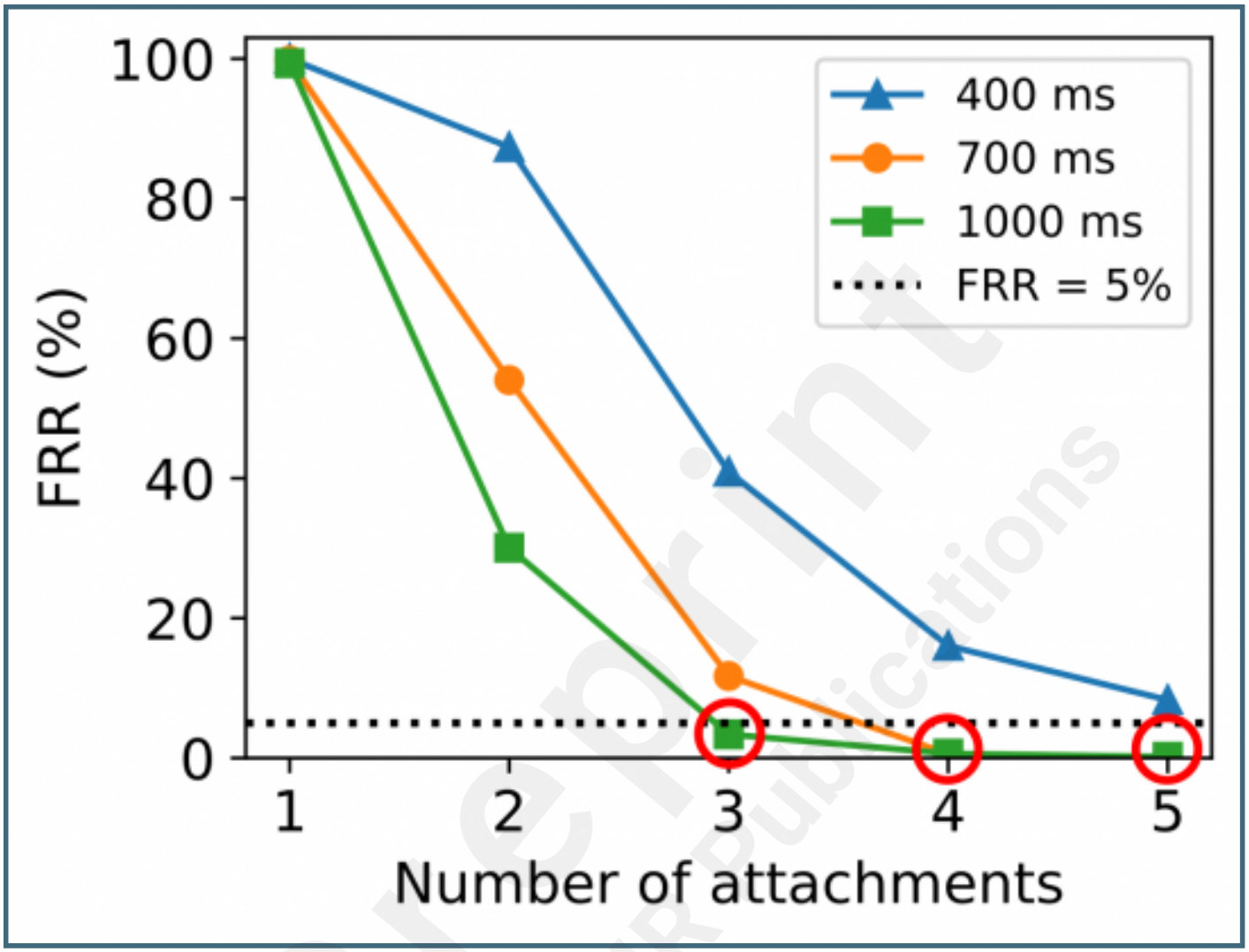
FRR vs. number of attachments, under 50 Hz vibration frequency.



FRR vs. number of attachments, under 75 Hz vibration frequency.



FRR vs. number of attachments, under 100 Hz vibration frequency.



Multimedia Appendixes

Questionnaire and Interview Design.
URL: http://asset.jmir.pub/assets/a5fcb2fe5535aaa0c54ae7ab21c60e0b.docx