Author/s:
Zhang, M;Marin, E;Ryan, M;Kostakos, V;Murray, T;Tag, B;Oswald, D

Title:
OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels

Date:
2024-07-30

Citation:
Zhang, M., Marin, E., Ryan, M., Kostakos, V., Murray, T., Tag, B. & Oswald, D. (2024). OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels. ACM International Conference Proceeding Series, pp.1-13. ACM. https://doi.org/10.1145/3664476.3670876.

Persistent Link:
https://hdl.handle.net/11343/350567

OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels

Mo Zhang
mxz819@student.bham.ac.uk
The University of Melbourne
Melbourne, Australia
University of Birmingham
Birmingham, United Kingdom

Eduard Marin
eduard.marinfabregas@telefonica.com
Telefonica Research
Barcelona, Spain

Mark Ryan
m.d.ryan@bham.ac.uk
University of Birmingham
Birmingham, United Kingdom

Vassilis Kostakos
vassilis.kostakos@unimelb.edu.au
The University of Melbourne
Melbourne, Australia

Toby Murray
toby.murray@unimelb.edu.au
The University of Melbourne
Melbourne, Australia

Benjamin Tag
benjamin.tag@monash.edu
Monash University
Melbourne, Australia

David Oswald
d.f.oswald@bham.ac.uk
University of Birmingham
Birmingham, United Kingdom

ABSTRACT

Implantable Medical Devices (IMDs) are widely deployed today and often use wireless communication. Establishing a secure communication channel to these devices is challenging in practice. To address this issue, researchers have proposed IMD key exchange protocols, particularly ones that leverage an Out-Of-Band (OOB) channel such as audio, vibration and physiological signals. While these solutions have advantages over traditional key exchange, they are often proposed in an ad-hoc manner and lack a systematic evaluation of their security, usability and deployability properties. In this paper, we provide an in-depth analysis of existing OOB-based solutions for IMDs and, based on our findings, propose a novel IMD key exchange protocol that includes a new class of OOB channel based on human bodily motions. We implement prototypes and validate our designs through a user study (N = 24). The results demonstrate the feasibility of our approach and its unique features, establishing a new direction in the context of IMD security.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; **Usability in security and privacy**; • **Human-centered computing** → **Ubiquitous and mobile computing**.

KEYWORDS

Implantable medical device, Out-of-band channel, Key exchange, User perception

ARES 2024, July 30–August 02, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3670876

ACM Reference Format:
Mo Zhang, Eduard Marin, Mark Ryan, Vassilis Kostakos, Toby Murray, Benjamin Tag, and David Oswald. 2024. OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3664476.3670876

1 INTRODUCTION

The number of patients with an Implantable Medical Device (IMD), such as a pacemaker, an Implantable Cardioverter Defibrillator (ICD), or an insulin pump, has rapidly grown for decades [13]. Modern IMDs typically rely on a wireless interface to communicate with external devices such as programmers and device monitors. Programmers enable doctors to reprogram the patient's IMD wirelessly (e.g., to change the patient's therapy) and gather telemetry data while monitoring devices, typically located in the patient's house, are used solely to periodically collect patients' medical data and send it to the hospital. Another emerging trend is that off-the-shelf consumer devices are of increasing importance to give patients (some) access to their IMDs. For instance, Medtronic, a global leader in medical devices, has incorporated Bluetooth Low Energy (BLE) into IMDs [38, 39], and developed a smartphone app that allows the patient to view some basic characteristics of their IMDs over a BLE link [40].

However, wireless channels also introduce new security threats. Adversaries may eavesdrop on the wireless channel remotely and obtain sensitive patient information [50], or even worse, send malicious commands to the IMD to alter its settings [32]. The consequences of these attacks can be severe, as these commands can allow adversaries to deliver (or disable) a therapy with the goal of causing serious injury or even death. While no real-world attack against an IMD is known to date, past research has demonstrated that many IMDs available on the market today severely lack effective security mechanisms [18, 32–34, 50].

To overcome these issues, it is necessary to first establish a secure wireless communication channel between an IMD and an external device before any sensitive data or commands are transmitted. This can be achieved by running any secure *IMD key exchange* protocol that enables establishing a shared cryptographic key between the IMD and the external device. However, key exchange in this context can be challenging due to the characteristics of current IMDs: They have limited memory and computational power, and are operated by a single non-rechargeable and non-replaceable battery. Once the battery is depleted, the patient needs to undergo surgery to get a new IMD, which in itself introduces risks. Furthermore, IMDs have no physically accessible input or output interfaces (e.g., a keyboard or screen) once implanted. Hence, wireless communication with the IMD is "invisible" to the patient, and there are no means to physically allow communication (e.g., by pressing a button).

One potential approach to secure the connection between an IMD and an external device is by provisioning them with the same symmetric key during manufacturing [19, 32]. However, if this key is compromised (e.g., exposed online), an adversary could access the IMD indefinitely. Public key cryptography-based solutions, like those relying on digital certificates [1], are challenging to implement as they require a worldwide robust and costly Public Key Infrastructure (PKI). Moreover, because the external devices can be retired or compromised (e.g., stolen), the PKI must have proper mechanisms to revoke such illicit devices and update this information in the IMD. However, IMDs do not have an Internet connection to receive these updates.

Another solution relies on distance bounding protocols [48]. In this approach, both the external device and the IMD estimate their physical proximity as a criterion for key exchange, which is determined by calculating the Round-Trip Time (RTT) of an ultrasound signal—the time interval between sending a challenge and receiving the response. This solution, however, requires an ultrasound transceiver in the IMD and precise measurements of the RTT, a demanding task for resource-constrained IMDs. Furthermore, proxy device-based protocols [12, 15, 65] have been proposed, which delegate security to a proxy device that can be carried around by the patient (e.g., a bracelet). However, it requires 24-hour wearing of the proxy device, which places the security burden on the patient, and suffers in terms of usability and convenience. Moreover, some concrete solutions [12, 15] protect the IMD by using the proxy to jam the wireless channel, which can be illegal in many countries.

Therefore, conventional symmetric/public key-based key exchange techniques and other solutions are often unsuitable (or even not viable) in the context of IMDs [34]. Furthermore, some existing solutions can only be used in static contexts where the set of external devices the IMD can communicate with is very small and known at initialization time. Hence, there is a need for novel key exchange solutions that are secure, usable and deployable while simultaneously being compatible with future generations of IMDs. Over the last decade, the use of Out-Of-Band (OOB) channels (*i.e.*, any communication channels other than a wireless channel) has emerged as a promising way to bootstrap security between an IMD and an external device that do not share any prior secrets.

Contributions. In this paper, we provide an in-depth analysis of existing OOB-based solutions for IMDs, and propose a new IMD key exchange protocol. Our main contributions are:

- We systematically review previous IMD key exchange solutions based on OOB channels, and find that while these methods have unique advantages, they often come with limitations in security and deployability.
- We design a novel key exchange protocol, comprising a new class of OOB channel that leverages several simple bodily motions (body rotation or tap) for key exchange with IMDs. To the best of our knowledge, we are the first to propose using human bodily motions for IMD key exchange.
- We develop prototypes that use our proposed OOB channel, and evaluate them in a user study with 24 participants. The results demonstrate promising potential to use bodily motion for IMD key exchange.

Our research involving human subjects gained approval from the Human Research Ethics Committee in the related research institutions. The data and software from user study are available under the following link: https://github.com/MrZMN/OOBKey

2 ASSUMPTIONS AND REQUIREMENTS

2.1 Threat model

We consider a sophisticated adversary with full knowledge of the key exchange protocol and the following capabilities:

Channel/network attacks: We assume that the adversary has full control of the wireless channel. This implies that the adversary can either perform passive attacks by eavesdropping on the communication or carry out active attacks, e.g., launch a Man-in-the-middle (MITM) attack. Furthermore, depending on the characteristics of a specific OOB channel (elaborated more in Section 3), the adversary may also be able to either eavesdrop or tamper with the data sent over the OOB channel.
Hardware/software analysis: The adversary is able to gain access to examples of relevant hardware (e.g., by stealing a device programmer from hospital) and can profile and reverse-engineer them, obtaining all firmware and cryptographic keys (of that specific device). We however exclude the case that an adversary manipulates a target device (e.g., by replacing its firmware)—this issue can only be addressed through the use of secure hardware, which is orthogonal to the problem tackled in this paper.
Proximity: The adversary is able to stay within close proximity (such as a few meters) to the patient, and may even try physical contact without the patient's awareness, e.g., when the patient is in a public place, in a crowd, or asleep.

The adversary may launch Denial-of-Service (DoS) attacks to manipulate the communication channel and disrupt the key exchange. However, if key exchange failures happen repeatedly, the external device can alert the user, who can take actions to investigate or report the suspected attacks.

2.2 Requirements for IMD key exchange

Given our review of relevant literature [15, 19, 32, 48, 53, 54, 65], and previously stated assumptions, we propose a set of core requirements one must consider for an IMD key exchange protocol:

Security: An adversary in our threat model cannot compromise the security of the key exchange. Specifically, we point out an

aspect often overlooked by prior works: for an adversary trying to perform key exchange with the patient's IMD in close proximity, it is crucial that the patient is able to recognize this malicious activity, enabling them to seek assistance or escape the scene (we assume the patient has fundamental cognitive and physical capabilities; otherwise, there are many more straightforward ways to cause severe impacts). Hence, the key exchange process should be highly perceptible. In line with prior works [19, 24], we argue that the degree of perception should exceed mere subtle body contact, and be impossible for the adversary to conceal, *i.e.*, the key exchange cannot function otherwise[1].

Usability: Users, primarily patients and doctors, should be able to easily understand, learn and execute the steps of the key exchange process. In an emergency situation—a serious incident where the patient may become unconscious and be unable to move, such as experiencing syncope symptoms in heart disease patients with cardiac implants [51]—medical practitioners should be able to access the patient's IMD without relying on Internet connection or other long-range communication links.

Deployability: The key exchange should be deployable to existing IMD products: It only utilizes the IMD's existing hardware components, and the energy consumption must be acceptable. Moreover, the key exchange should be time-efficient, as a long execution time (e.g., over half a minute) can negatively affect the user experience and even emergency availability. Furthermore, nowadays the types of external devices are becoming increasingly diverse and are not limited to dedicated, proprietary devices built by medical organization [40]. It would be advantageous for the key exchange to be compatible with readily available consumer devices, *i.e.*, smartphones or tablets.

3 RELATED WORK

The main intention to use OOB channels for IMD key exchange is that they are generally considered to be more secure than long-range wireless channels, and thus suitable for transmitting secret data [19, 24, 34, 53]. Moreover, compared to some conventional solutions (e.g., symmetric key-based ones), OOB channels do not rely on any prior shared information, which is especially advantageous in the IMD context. In addition, OOB channels might bring about additional benefits. For example, a vibration channel itself is perceptible to some extent, which might further enhance security as the user can sense when key exchange is taking place.

However, compared to wireless channels, OOB channels typically have more limited bandwidth, can be more costly for data transmission and reception (e.g., in terms of the energy consumption), and may require additional hardware components (e.g., vibration transceivers). Therefore, the OOB channels *cannot* replace wireless channels and are used only for transporting a small amount of data, *i.e.*, a session key (or a secret value from which a shared key can be generated). After a session key is agreed on, the parties can apply any standard encryption techniques and transmit the ciphertext through the wireless channel.

[1]For example, merely adding visual/audio cues to the external device is unsuitable, as an adversary could develop a proprietary external device that removes these cues.

3.1 OOB channels for IMD key exchange

Tattoo or bracelet as a visual channel. One way to establish a key between an external device and an IMD is to tattoo the IMD's key on the patient's skin or to print it on a bracelet worn by the patient [56]. This solution places little burden on the IMD, however, its applicability is debatable. Tattoos can become unreadable after an accident, disclose the patient's condition to others, or be refused due to the religious, aesthetic, or cultural concerns. Equally, a bracelet can be damaged or lost, which can lead to severe consequences.

Audio channel. Halperin et al. [19] proposed that the IMD broadcasts a key as a modulated sound wave (4 kHz signal generated by a piezo element embedded in the IMD) such that only an external device a few centimeters away can demodulate it correctly. One major advantage is that due to the nature of audio signals, patients may notice when a key exchange occurs. However, Halevi and Saxena [17] showed that the sound can be captured using an off-the-shelf microphone from several meters away. Siddiqi et al. [60] proposed a method where the IMD transports the key using MHz-range ultrasound. The security is based on the assumption that the MHz ultrasound waves can only be received by devices that touch the patient's body. However, the authors only verified this security assumption in an acoustic software simulation but not in a real hardware set-up. Also, an ultrasound is not perceptible.

Vibration channel. Saxena et al. [55] and Kim et al. [24] proposed to use vibration for key exchange with IMDs. The transmitter device (typically the external device) encodes the key into a vibration signal via a vibration motor, while the receiver (typically the IMD) uses an accelerometer to receive it. Similarly, the key exchange process is to some extent perceivable by the patient. Crucially, unlike the audio channel, a strong advantage of this channel is that sending a vibration to an IMD requires the sender device to directly touch the patient's body. However, the vibration is essentially a low-frequency audio signal, which also inevitably emits acoustic side-channels and may be compromised [17].

Human body as a conductive channel. The human body also acts as an OOB channel for IMD key exchange due to its conductivity [34, 52]. The key transmission can be achieved via, e.g., galvanic coupling techniques [62, 63]: The external device injects the key as a low alternating current (e.g., 0.5 mA) into the skin, while the IMD detects the voltage across two receiving electrodes. The security assumption is that the current is absorbed by the tissue and emits little side-channel information outside the body [34, 62]. Nevertheless, whether this method can totally defend against eavesdropping attacks requires more investigations. Importantly, this method assumes that injecting a low-enough current is harmless for a patient carrying implants. However, medical device companies, such as Boston Scientific, have claimed that such current injection might interfere with the IMD's therapy [57].

Physiological signal as a channel. Besides the above solutions where one device generates and transmits the secret to another via an OOB channel, there are also solutions that rely on a shared entropy source like the patient's body [28, 46, 53]. As opposed to biometrics that is person-specific and to a large extent invariant [35], physiological signals (e.g., heartbeats) are random signals

Table 1: Evaluation of deployability properties.

	Hardware Components (IMD)	Energy Consumption (IMD)	Time Efficiency
Audio channel	piezo element [19]; MHz-ultrasound transceiver [60]	claimed negligible [19]; < 15 mJ [60]	320 bps [19]; 50K bps (theoretical) [60]
Vibration channel	accelerometer	< 4.5 mAh [24] (over IMD's 90-month lifetime)	1.5 bps (zero error rate mode) [55]; 20 bps [24]
Human body	a pair of electrodes	≤ 2.75 mJ [62]	85.3 bps [34]; 50K bps [62]; 4.8K bps [63]
Physiological signal	biosensor (e.g., ECG sensor)	≤ 19.68 mJ [28]	3.2 bps [28]; 4 - 5.3 bps [31, 53]

varying over time. A standard approach consists of two devices independently and synchronously taking a measurement of the physiological signal, and establish a key based on it. Yet, the security of physiological signal-based cryptographic protocols is questionable. For example, numerous works [28, 53] proposed to use the Inter-Pulse-Interval (IPI), *i.e.*, the time interval between two consecutive R-peaks of the Electrocardiogram (ECG) signal, to realize key exchange. However, Ortiz-Martin et al. [44] and Seepers et al. [58] have shown that IPI is not an appropriate selection. Currently, there is no known suitable physiological signal that meets all the requirements for being a qualified entropy source [30].

3.2 Analysis of previous approaches

We analyze previous OOB channel-based approaches against the requirements that we identified in Section 2.2.

Security. Previous attacks [4, 17, 30, 58] have exposed vulnerabilities of visual, audio, vibration and physiological signal-based OOB channels, to eavesdropping using microphones or cameras from several meters away. To defend against these threats, certain countermeasures have been suggested. For instance, to safeguard audio and vibration channels, Kim et al. [24] and Anand and Saxena [4, 6] proposed using Gaussian white noise or masking signals to obscure the acoustic leaks. These approaches have shown promise in thwarting side-channel vulnerabilities against sophisticated eavesdropping techniques.

On the other hand, all prior works do not require the protection of examples of relevant hardware/software to ensure security because the exchanged key is not shared by multiple devices, *i.e.*, it is either re-initialized in each key exchange session or uniquely assigned to a specific device.

Of all the approaches, the audio (not ultrasound) and vibration channel-based solutions offer a degree of audible/tactile feedback to the patient. Nonetheless, the signal amplitudes were subdued in their initial designs [19, 24]. For instance, the vibration amplitude in [24] is only around 0.2 g, which is confirmed to produce a limited level of perceptual intensity to humans [21]. Similarly, the effectiveness of the audio channel is also questioned by previous research [55]. While amplifying the signal might address this, it presents challenges as it could lead to more acoustic leakage and potential discomfort for patients. Furthermore, these techniques were not validated on real users. Thus, it is uncertain if they can genuinely achieve significant user perception in practice.

Usability. The previous works commonly asserted the proposed techniques to have high usability (*i.e.*, simple to learn and easy to execute): The visual channel-based solution requires the user to retrieve the secret from a patient's tattoo or personal item, while other solutions merely require the user to hold the external device near the patient or attach it to the patient's body. Notably, such claims were seldom substantiated with user studies. Moreover, all methods are plug-and-play and the key exchange process in emergency situations is identical to the one employed in hospitals.

Deployability. We present the deployability data given by prior works in Table 1. Note that the data is not always complete, e.g., energy consumption was not widely provided. Here we omit the visual channel-based method as it only requires a symmetric key to be pre-installed and places little burden on the IMD.

All OOB channels require specific hardware components in the IMD: The audio-based solutions require a piezo element [19] or a MHz-ultrasound transceiver [60]. Current IMDs lack these components, and no indications suggest their integration in the foreseeable future. The vibration channel demands an accelerometer within the IMD, a feature existing in cutting-edge IMDs. For example, the Medtronic pacemakers and ICDs already contain accelerometers for medical purposes [37, 42, 47]. In contrast, the technique based on current transmission through the body needs a pair of electrodes/wires in the IMD to receive the current. To our knowledge, there is no evidence of their existence in IMDs (though their integration may be feasible). Moreover, physiological signal-based solutions leverage a biosensor, which can be inherently present in IMDs for medical use, e.g., the ECG sensor in cardiac implants.

Among the energy consumption values in prior works, the physiological signal-based method reports the most energy with 19.68 mJ per execution. To evaluate this, we first estimate an IMD's battery capacity using advanced pacemakers as an example: The energy density of a pacemaker's Li/I_2 battery can reach 210 Wh/kg [3]. Hence, assuming the battery constitutes 80% of the total weight of the pacemaker, a 20 g pacemaker battery—approximated using the Medtronic Azure pacemaker [41] as an example—would have an energy capacity of roughly 4 Wh (14400 J). Therefore, the energy consumption of prior works should generally be acceptable.

We use bit rate (*i.e.*, bit per second) to represent time efficiency of each method. We observe that solutions based on audio channels and human body present high data rates, while the vibration and physiological signal-based methods yield considerably lower speed. If a 128-bit cryptographic key is to be exchanged, these methods may result in a key exchange duration of half a minute or more.

For the visual, audio, and vibration channels, commercial devices like smartphones suffice as external devices, given their inherent features like keyboard, microphone, and vibration motor. However, human body channel is incompatible as it demands the external device to emit a current. The compatibility of physiological signal-based solutions depends on the type of physiological signal.

Limitations of existing work. As we have discussed so far, existing OOB channels offer features well-suited to the IMD key exchange context; however, they also exhibit certain limitations:

Vulnerable to injection attacks. Current OOB channels generally lack strong safeguards against adversaries in proximity of the patient, which try to exchange a key with the IMD without the patient noticing. This is a crucial aspect that has regularly been neglected: Most previous works attempt to make the IMD key exchange as unobtrusive as possible to the patient, rendering the key exchange process almost *imperceptible*. To our knowledge, many advanced IMDs in the market [11, 39, 40] currently also follow this guideline.

Such a design principle is admittedly prevalent in many everyday security systems, e.g., when surfing the Internet, users do not notice the key exchange with a remote server using the Transport Layer Security (TLS) protocol. However, this heavily relies on the assumption that the key exchange is sufficiently secure and is initiated by the legitimate user (both of which are true for TLS in the browser, but not necessarily for an OOB key exchange). As this assumption is often not met [4, 17, 30, 58], we question if this guideline fits the IMD context, where the device is part of the patient and its security is life-critical.

We emphasize that this vulnerability is especially evident in the public spaces of everyday life. For example, on a crowded bus, it may be difficult for the patient to recognize if a nearby person is trying to pair with their IMD. In such scenarios, proximity to the patient, or even brief physical contact with them (a necessary step in many previous IMD key exchange techniques [24, 28, 52, 53, 62]), could potentially be overlooked by the patient.

Vulnerable to eavesdropping attacks. OOB channels also face threats from sophisticated side-channel eavesdropping using microphones and cameras. Fortunately, over the last decade, such threats have been largely mitigated with various defense strategies [4, 6, 16, 24]. However, we identify another issue in previous works: they commonly propose using an OOB channel to *directly* exchange a session key. This simplifies an attack, as the adversary does not have to recover the secret in real-time during its transmission over the OOB channel. Instead, they can record the traffic and launch offline brute-force analysis, potentially increasing the likelihood to compromise the security [17].

Deployability issues. Many proposed solutions cannot be deployed on existing modern IMD products, and are also not compatible with off-the-shelf consumer devices as external devices. Another concern is the potential for a prolonged key exchange time due to the relatively low data rates for some OOB channels. For example, vibration and physiological signal based channels can take dozens of seconds to exchange a 128-bit key.

4 OUR KEY EXCHANGE PROTOCOL

To address these limitations, we introduce a novel IMD key exchange protocol, which largely mitigates both injection and eavesdropping attacks, is compatible with state-of-the-art IMDs and prevalent consumer devices, and completes within several seconds.

Figure 1 shows the full details of our protocol. The external device first initializes the key exchange—this can be any existing wake-up process adopted by current IMD products [38]. Subsequently, two steps are executed:

① **OOB key exchange:** The user (*i.e.*, patient or doctor) is required to hold the external device and perform several bodily motions on the patient's body. The IMD and the external device measure these motions as a shared basis to exchange an ephemeral and low-entropy Short-Term Key (STK). Due to the potential inherent noise between the motion measurements, a fuzzy cryptographic primitive [67], such as a fuzzy commitment [22], is utilized to rectify such noise (that is within a certain threshold) without revealing the secret.

② **PAKE:** Two devices run a Password-authenticated Key Agreement (PAKE) method [23] to further exchange a robust and high-entropy Long-Term Key (LTK) as the session key. Here, the STK plays the role of the "password" in the PAKE. A concrete example of PAKE is Diffie-Hellman Encrypted Key Exchange (DH-EKE) [8]. This step can be completed only if both devices share an identical STK, meaning their measured motions must be sufficiently similar.

We will elaborate the design of these two steps in this section. Note that since the fuzzy cryptographic primitive [67] and PAKE [23] are well-established algorithms in the cybersecurity community, we will not include a step-by-step breakdown of them.

4.1 Bodily motion as an OOB channel

4.1.1 Motivation. We propose using human bodily motion as an OOB channel to mitigate the injection attacks. This is inspired by previous works that leverage user motion for pairing with (not implanted) Internet-of-Things (IoT): Mayrhofer and Gellersen [36] and Hinckley [20] suggested key exchange between two IoTs by holding them together and shaking. Xu et al. [66] and Revadigar et al. [49] facilitated key exchange between two wearables with the user walking for dozens of steps. Li et al. [26, 27] introduced key exchange between an IoT device and a smartphone through user-generated events, like random button presses. Zhang et al. [68] and Ahmed et al. [2] asked the user to pat/move the device in specific patterns according to instructions on another device's screen. Sethi et al. [59] proposed key exchange between two devices with tangible screens by simultaneous drawing on both devices.

These solutions are not directly transferable to the IMDs as they generally require physical contact with IoTs, whereas IMDs are implanted. They also do not consider emergency scenarios. Nevertheless, these methods have demonstrated notable potential: They provide users a heightened awareness of their devices. Moreover, the physical motions interacting with IoTs are indispensable. Assuming that the device is an IMD implanted in the patient's body, these motions must be executed on the patient's body. The above implies that the key exchange can be designed highly perceptible. Consequently, patients hold the authority to decide whether to

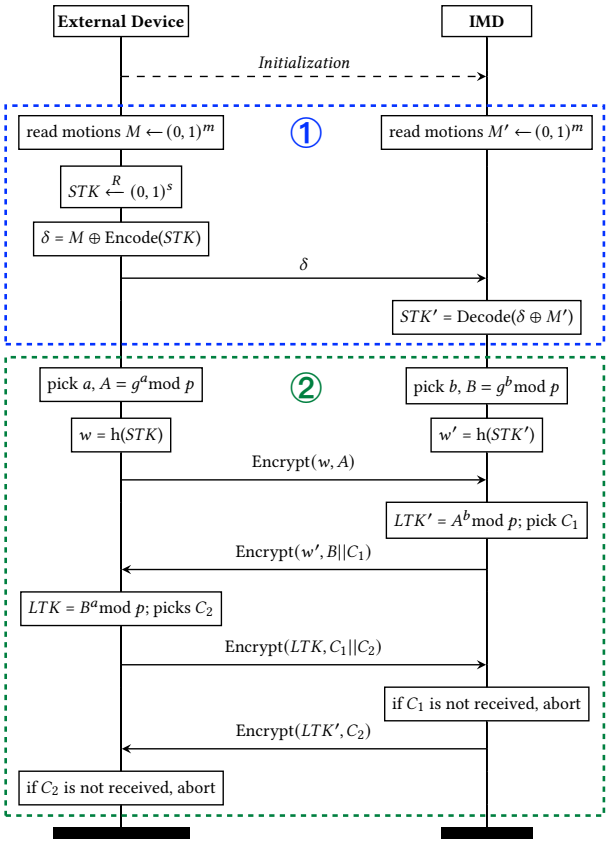


Figure 1: Our key exchange protocol. ① is OOB key exchange, which involves measuring bodily motions and applying a fuzzy commitment scheme [22] to remove noise from these measurements. *R* stands for random number generation and ⊕ is XOR operation. The Encode/Decode processes are part of an error correction code. ② is PAKE (using DH-EKE [8] as an example). g and p are public parameters. h() is a secure hash function, and Encrypt(key, msg) refers to the encryption of the message msg with key. Note that although we use fuzzy commitment and DH-EKE, many other fuzzy primitives or PAKE methods may also be applicable.

execute the key exchange, acting as an *additional* robust countermeasure against unauthorized access. This way, an adversary may not succeed merely by being in close proximity.

Another promising aspect of bodily motions is that they can be measured using inertial sensors, e.g., accelerometer and gyroscope [14]. Nowadays, inertial sensors are becoming more miniaturized and energy efficient, which makes them appropriate for advanced IMDs. For instance, Medtronic has incorporated these sensors into their cardiac IMD products to enable a "Rate Response feature", which adapts the pacing rate of IMDs to changes in the patient's physical activity [37, 42, 47]. Furthermore, inertial sensors have been prevalent on consumer devices like smartphones.

However, as acknowledged by many previous studies [2, 26, 27], using bodily motions as a means for key exchange can inevitably lead to potential visual and/or auditory side-channel leakage. We will discuss these risks in Section 7.1.

4.1.2 Design of Our OOB Channels. We design our OOB channel in two strategies: (i) One device generates the secret (*i.e.*, M in Figure 1) and transmits it to another device by guiding the user to perform specific motions (each motion is mapped from a portion of M). This strategy aligns with [2, 52, 55, 68]. (ii) The user acts as an entropy source for M, which resembles the approaches proposed by [27, 36, 53, 59].

The selected motion should meet several criteria: First, it should be simple and executable to patients. Second, when the patient is unable (e.g., in emergencies) or unwilling to perform the motions, the motions can be done by medical staff on the patient's body. Third, it is reliably detectable by inertial sensors either inside (IMD) or outside (external device) the patient. Forth, it should potentially contain high entropy, reducing the need for repetitive moves over an extended period. Fifth, the motions must be highly perceptible to the patient.

After collaborative brainstorming and tests in a pilot study group (see Section 5.2), we select rotation and tap as the motions for (i) and (ii) respectively. The details of the OOB key exchange processes are outlined below. For simplicity, we assume the IMD is a pacemaker and the external device is a smartphone, but note that the device types can be easily varied, e.g., an insulin pump as the IMD.

Rotate and Pair. In this system, patients are guided by a smartphone app to execute a series of left or right full-body rotations, with the angle (ranging from 30 to 180 degrees) randomly determined by the app. This angle range is chosen empirically after our pilot study: angles less than 30 degrees are difficult to perform and angles above 180 degrees risk causing dizziness. Each rotation is required to be completed within a uniform ten-second window[2], irrespective of the angle, to prevent potential information leakage (e.g., smaller angles take shorter time). Visual cues such as a progress bar guide the patients on the remaining time. The patient must reach and hold the target heading (*i.e.*, the degree shown on the app) when time expires, or the instruction must be repeated—this rule safeguards against potential non-compliance with the instructions. The app dynamically displays the patient's current heading with a precision of one degree. A minor deviation, *i.e.*, plus or minus two-degree variation from the target heading, is allowed for the patient's convenience.

Tap and Pair. In this system, patients are directed to gently tap the smartphone against their chest area for several times. Before starting, they are advised by the system to tap with a random rhythm instead of a consistent, periodic pattern. As the patient performs these taps, the smartphone recognizes each tap in real time and emits an immediate sound as feedback (this sound only serves as an acknowledgment and can be removed). The key exchange ends upon collection of sufficient taps.

After the patient performing the motions, a fuzzy cryptographic primitive is applied to eliminate any mismatches (that are within a certain threshold) between the two devices' measurements, e.g., those caused by sensor noise. We detail this process in Section 6.1.

[2]The ten second window is an intuitive design to ensure that sufficient time is provided.

We believe that our OOB channel can effectively mitigate injection attacks. The key exchange can only be conducted by a legitimate patient or doctor. If an adversary rotates the patient's body or taps a device on it for a few times, this would be readily perceptible to the patient. Our user study further substantiates our claim, as elaborated in Section 6.3.

4.2 Use of a PAKE

4.2.1 Motivation. We propose employing a Password-authenticated Key Agreement (PAKE) method [23] to mitigate eavesdropping attacks and enhance the time efficiency of the key exchange. In our protocol, the external device and IMD only use the bodily motions to exchange a short STK. Subsequently and instantly, they execute the PAKE and exchange an LTK. The prerequisite for successful PAKE execution is that both parties share the exact same STK; otherwise, the legitimate devices can detect a failure, thus abort the current session and require a restart (*i.e.*, a new STK exchange).

The involvement of a PAKE has two major advantages. First, the protocol execution time can be reduced. Instead of exchanging the entire session key (most likely a 128-bit key), the OOB channel is used solely to bootstrap a short STK, e.g., one with about 20 bits of entropy [2]. The PAKE employs the normal wireless channel and is thus usually faster compared to the OOB exchange.

Second, the PAKE can also significantly reduce the potential for eavesdropping: (i) It rules out offline brute-force attacks (*i.e.*, record the traffic and perform offline exhaustive search) on the OOB channel. The STK is short-lived and only valid until the start of the PAKE, which means that the adversary must obtain the STK online in a usually short timeframe. (ii) The adversary cannot endanger the patient by passive observation alone. For example, assume DH-EKE is used as the PAKE, then the underlying Diffie-Hellman scheme naturally prevents the adversary from obtaining the LTK by eavesdropping only. (iii) It restricts the time of attempts of a MITM adversary. Through proper implementation of a PAKE, the adversary is confined to a single attempt to run the PAKE with a legitimate device [8]. The adversary's failure (e.g., due to possessing a wrong STK) will lead to the abortion of the current session.

4.2.2 Security Analysis with PAKE. In our protocol, the adversary is forced to wait for the patient or the doctor to perform the STK exchange. Concurrently, they need to eavesdrop/guess (but not inject) the STK and execute the PAKE with one legitimate device. Here, we quantify the success probability of the adversary, denoted as P_{adv}. For simplicity, we assume that the adversary aims to impersonate the external device and connect with the IMD (which is normally the worst case), but note that the situation is similar if the target is the external device.

The key exchange protocol might fail under some circumstances, thus, should tolerate a certain number of rounds (*i.e.*, restarts). The maximum tolerable number of rounds can be fixed by design, denoted by n. In each round, let P_c denote the adversary's success probability to eavesdrop/guess the STK. We assume that if the adversary can obtain the STK, they can use it to complete the PAKE, and thus, the adversary's success probability is also P_c. Let Q_c be the probability that the legitimate external device succeeds in completing the PAKE with its exchanged STK. Given this, since the successes of the external device and the adversary are *exclusive* but not independent, the probability that neither of them obtains STK (and hence the PAKE fails) is $1 - P_c - Q_c$. There are three possible outcomes per round:

- The external device succeeds.
- The adversary succeeds.
- Both fail and the protocol proceeds to the next round.

We estimate P_{adv} in the following.

Proposition 4.1. Given an adversary that conducts attack for at most n times,

$P_{adv} \leq P_c + \phi P_c + \cdots + \phi^{n-1} P_c = \frac{P_c(1-\phi^n)}{1-\phi}$, where $\phi = 1 - P_c - Q_c$.

Proof. The first term corresponds to the case that the adversary succeeds in the first round; the second term corresponds to the case that the adversary succeeds in the second round; and so on. Note that these cases are exclusive, and therefore can be summed. The adversary succeeds in the nth round if they fail in the first $n-1$ rounds (with probability ϕ^{n-1}) and succeed in the round after that (with probability P_c). □

Furthermore, we propose that P_{adv} is always less than some constant multiple of P_c.

Proposition 4.2. There is a constant k representing the legitimate external device's ability that is independent of P_c, such that:

$$P_{adv} \leq k \cdot P_c, \text{ when } k = \frac{1}{Q_c}.$$

Proof. Since $1 - (1 - P_c - Q_c)^n \leq 1$ (remember that these are probabilities, hence in the interval $[0, 1]$), we have $P_c(1 - (1 - P_c - Q_c)^n) \leq P_c$; also $P_c + Q_c \geq Q_c$, and therefore

$$P_{adv} \leq \frac{P_c(1 - (1 - P_c - Q_c)^n)}{P_c + Q_c} \leq \frac{P_c}{Q_c} = k \cdot P_c$$

when we put $k = \frac{1}{Q_c}$. □

To understand this proposition, let us assume that the legitimate device is likely to succeed ($Q_c > 0.9$) and the adversary is likely to fail ($P_c < 0.05$), then we have $P_{adv} < 0.056$. This shows that the advantage the adversary gets of being able to force a restart of the protocol is fundamentally limited. Note that if the adversary interferes with the legitimate external device (*i.e.*, reducing Q_c) and causes repeated protocol restarts, the user can easily detect this.

5 EVALUATION WITH HUMANS

To validate our protocol, we develop prototypes that use our proposed OOB channel and evaluate their performance through a user study. Note that as fuzzy primitives and PAKE are well-established cryptographic algorithms and their applicability on resource constrained devices has been widely verified [27, 67], we did not implement them in our study.

5.1 Prototype implementation

IMD. To simulate a pacemaker, we employ a Bosch BNO055 inertial measurement unit [10], which we house within a 3D-printed casing (the pink component in Figure 2a). An Arduino Nano 33 BLE board is used to interface with the sensor and store data.

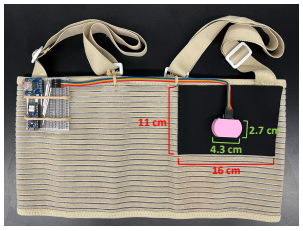
In the *Rotate and Pair* prototype, tilt-compensated heading data in degrees is calculated using a Kalman filter based on accelerometer and gyroscope readings [29]. For the *Tap and Pair* prototype, we implement a real-time peak detection algorithm that recognizes tap events. This algorithm processes the norm of 3-axis accelerations ($\sqrt{a_x^2+a_y^2+a_z^2}$) as individual samples, each checked for potential peaks based on pre-set thresholds of signal amplitude, peak width, and distance between consecutive peaks. Subsequently, the IMD computes the time interval between two successive peaks in milliseconds.

Smartphone. We use a Google Pixel 6 smartphone for our study and develop two Android applications to guide the user through the key exchange process based on rotation and tap.

As in Figure 2c, the rotation app implements a classic electronic compass design that features a 360-degree compass rose with the current heading dynamically displayed at its center (we refer to the graphic layout design in [9]). Instructions are presented at the top to guide the user to rotate either left or right to a specified degree. At the bottom, a progress bar visualizes the remaining time to complete the current instruction, and a numerical display indicates overall progress (*i.e.*, the number of rotations towards the completion of key exchange). The tap app (Figure 2d) guides the user with text instructions and a start button. When the button is pressed, its color changes and the user begins tapping the phone against the chest area. As taps are made, the smartphone acknowledges each tap with a short sound that resembles the brief, soft "beep" of a text message notification.

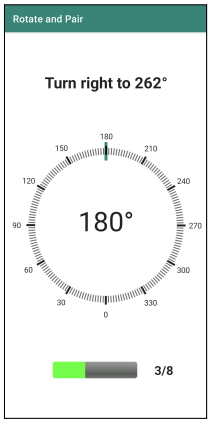
At the beginning of each key exchange, the smartphone establishes an (insecure) BLE channel with the IMD (*i.e.*, the Arduino board). For *Rotate and Pair*, the smartphone utilizes Java's SecureRandom API [43] to initialize each rotation instruction. The tilt-compensated heading is obtained in real-time via Android OS 'game rotation vector' virtual sensor and dynamically updated on the compass. When the user completes each rotation (*i.e.*, reaches the target heading when the progress bar is filled), the smartphone records its current heading and signals the IMD to do the same. Moreover, the smartphone records the time the user first arrives at the target heading as the estimation of actual rotation duration. For *Tap and Pair*, the smartphone synchronizes with the IMD at the beginning and end of the key exchange. Throughout the tapping sequence, the smartphone employs a peak detection algorithm (similar to that in the IMD) to measure the time intervals between successive taps in milliseconds.

Chest simulator. As pacemakers are implanted within the body, it is crucial that our experiments simulate an environment similar to the human chest. We adopt the design in [19, 24, 34] and use 5 mm layer of bacon and 10 mm layer of lean ground beef to mimic the chest's physical properties, as in Figure 2b. The 5 mm depth is a standard depth for pacemaker implantation [45]. During the experiments, the "pacemaker" was embedded within the meat layers contained in a food bag under room temperature. This meat bag was then placed in a pocket sewn onto an elastic chest strap, positioned around the area of the human heart (see Figure 2a). Participants were asked to wear this strap throughout the study to mimic the conditions of pacemaker users. The meat was replaced at the beginning of each day to prevent spoiling.

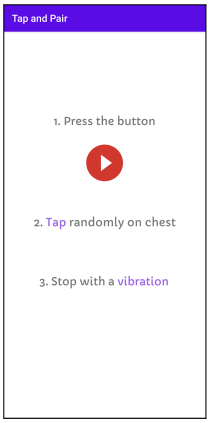


(a) IMD prototype.

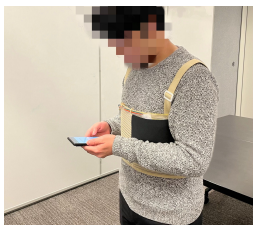
(b) Chest simulator.



(c) App for rotation.



(d) App for tap.



(e) Rotate and Pair.

(f) Tap and Pair.

Figure 2: Experimental setup

5.2 Data collection

We first conducted a pilot study with 6 individuals to study their attitudes of different motions, and identify and resolve any problems with our experiment setup. Then, we recruited 24 participants for our study: 11 males and 13 females with ages ranging from 21 to 52. Participant recruitment happened via online advertisements, and each participant was offered $30 for their time. During the user study, each participant used both key exchange methods, and the order in which they used the methods was counterbalanced.

For *Rotate and Pair*, we instructed each participant to stand, hold the smartphone, and perform eight consecutive full-body rotations (Figure 2e), referred to as a run. We advised participants to use both hands and refrain from twisting their wrist while rotating. We asked each participant to perform three such runs for data collection. The number of rotations is designed with caution to avoid potential dizziness. For *Tap and Pair*, we instructed participants to gently tap the smartphone against the black pocket area on the chest strap

(Figure 2f), executing 15 successive taps as a run. Each participant carried out ten runs in total.

For both methods, prior to data collection, we requested the participants to try our smartphone app to get familiar with the task. This process took less than one minute for all people. After data collection, participants were asked to complete a standard System Usability Scale (SUS) questionnaire [25] to evaluate the usability of the key exchange. At the end of the user study, we asked each participant a few interview questions about their experiences. Full details of the questionnaire and interview are given in Table 2 and Table 3, respectively.

Table 2: Our SUS questionnaire consists of ten questions and provides respondents 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 [25]) suggests good system usability. We used the term "pair" as opposed to "key exchange" to avoid confusion among individuals without a cybersecurity background.

I think that I would like to use this pairing method frequently.
I found the pairing unnecessarily complex.
I thought the pairing method was easy to use.
I think that I would need the support of a technical person to be able to pair.
I found the various functions in this pairing method were well integrated.
I thought there was too much inconsistency in this pairing method.
I would imagine that most people would learn how to pair very quickly.
I found the pairing method very cumbersome to use.
I felt very confident using the pairing method.
I needed to learn lots of things before I can get going with this pairing.

Table 3: Our semi-structured interview questions.

In general, can you share your preference between the two pairing techniques based on rotation and tap, and why?
Have you noticed anything uncomfortable in the pairing processes?
(Given the context of how Medtronic implements the pairing between an external device and a pacemaker [11, 41]) would you prefer the convenient, but invisible solutions currently adopted by state-of-the-art medical companies, or would you prefer the more interactive, yet demanding solutions that we propose?

6 RESULTS

6.1 Accuracy

We use False Rejection Rate (FRR) and False Acceptance Rate (FAR) to measure the accuracy of the OOB key exchange. FRR represents the frequency at which the OOB key exchange between a legitimate IMD and smartphone is rejected. A low FRR is crucial for usability. FAR indicates the frequency that the key exchange between the user's IMD (resp. smartphone) and an illegitimate smartphone (resp. IMD) is incorrectly accepted. A low FAR is essential for security.

Due to the noise inherent in sensor measurements and user behavior (e.g., hand wobbles), the data (angle or time interval) collected by the IMD and the smartphone may not be identical but only similar. To enable exchange of an identical STK, a fuzzy cryptographic primitive [67], e.g., the fuzzy commitment scheme [22, 27], is utilized to correct the mismatch without revealing the secret. At the core of this method is the definition of a distance d between a pair of data and the selection of a threshold (Thr): the mismatch can be rectified (and thus the key exchange succeeds) if $d \leq Thr$; otherwise, the key exchange fails. A false rejection occurs when $d > Thr$ for a legitimate data pair, and false acceptance when $d \leq Thr$ for an illegitimate pair. As in [27], we define d as the sum of the absolute differences between corresponding elements in a pair of data from IMD and smartphone.

Table 4: NIST statistical test results for taps.

Test	p-value	Test	p-value
Frequency	0.806	Block Frequency	0.855
Runs	0.723	Longest Runs	0.088
Binary Matrix Rank	0.706	FFT	1.000
Non-overlap Template	0.716	Overlapping Template	0.620
Serial	0.424	Linear Complexity	0.725
	0.442	Approximate Entropy	0.130
Cumulative Sums	0.854	Random Excursions	0.738
	0.629	Random Excursions Var.	0.582

For *Rotate and Pair*, we build two sets to evaluate FRR and FAR.

- **Set I** comprises 72 (= 24×3) pairs of rotation angles, each with a length of eight (since we collect eight angles in one run). All the pairs in Set I come from legitimate key exchange sessions between an IMD and a smartphone.
- **Set II** has 72 pairs of rotation angles (the same size as Set I), where each pair is created by randomly combining data from the IMD and the smartphone originating from different sessions.

Note that not all eight rotations in one run are necessarily needed. We can adjust the length, ranging from one to eight, by truncating the initial elements.

Similarly, for *Tap and Pair*, we build Set I with 240 (= 24×10) legitimate pairs, each with 15 time intervals, and Set II of the same size by randomly selecting illegitimate pairs from different sessions.

For a given number of motions, the smaller the Thr, the lower the FAR (better security), but the higher the FRR (worse usability). Because security is of utmost importance for the context of IMDs, we set a smaller Thr to guarantee FAR = 0, and use the corresponding lowest FRR to represent accuracy. Figure 3 shows the performance of *Rotate and Pair* and *Tap and Pair* across various numbers of motions. As expected, an increase in the number of motions leads to higher accuracy. Considering that an FRR below 2% signifies good usability (note that a much more lenient FRR threshold of 10% was used in previous works [27, 36]), we observe that as few as 3 rotations, or 4 taps, are sufficient in terms of accuracy, with (FAR, FRR)=(0, 1.4%) and (FAR, FRR)=(0, 1.1%), respectively.

6.2 Security

Randomness analysis. The randomness of rotations is guaranteed by the Java SecureRandom API that is widely acknowledged as a reliable random number generator for cryptographic purposes [43]. The randomness of human-generated taps is evaluated using the same approach as in previous works [27, 53, 64]. We concatenate the six least significant bits of the time intervals from all participant runs (maintaining experiment order) and examine if the resulting

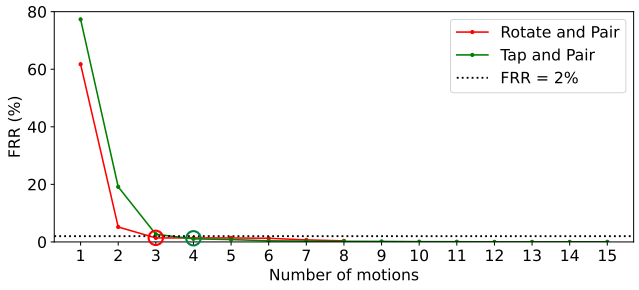


Figure 3: FRR *vs.* number of motions (FAR = 0). The circles indicate the minimum motions to ensure FRR < 2%.

bitstring of 21.6k bits is randomly distributed according to the NIST statistical test suite [7]. The results are shown in Table 4. The outputs of the NIST statistical tests are p-values that represent the probability the tapping dataset is generated by a legitimate random number generator. If a p-value is smaller than a threshold (usually 0.01 [7]), the randomness hypothesis is rejected. Table 4 shows that all p-values are larger than 0.01 and hence *pass* the NIST tests.

Entropy analysis. The entropy of each motion event quantifies the capability of an adversary in guessing the STK. As in prior works [28, 36, 64], we use Shannon entropy [61] to quantify the entropy of each type of motion. A single rotation is uniformly distributed over 300 degrees (in one degree precision) and thus contains an entropy of 8.2 bits. In contrast, a single tap in our study has an entropy of 9.4 bits.

However, the entropy is diminished due to fuzzy cryptographic primitives that rectify mismatches between the two devices. If we use the binary encoding method presented in [27] on our dataset, the maximum bit mismatch rate for *Rotate and Pair* and *Tap and Pair* would be 4.3% and 1.9%, respectively. This can be addressed by e.g., a fuzzy commitment scheme with (20, 15) binary BCH code with a 5% error tolerance [67], potentially leading to an entropy loss of 25%. We emphasize that this is a preliminary estimation, and more rigorous calculations are necessary in real-world implementations, which is beyond the scope of this paper. In this way, each rotation and tap carries an entropy of 6.2 and 7.1 bits, respectively.

6.3 Efficiency and usability

We next use our results to estimate the time for users to perform one rotation[3] or tap. We find that the mean time is 4.6 s (SD = 2.4) and 0.9 s (SD = 0.6), respectively. The corresponding average bit rates for rotation and tap are 1.3 bps and 8.0 bps.

The mean SUS scores for *Rotate and Pair* and *Tap and Pair* are 62.8 (SD = 21.17) and 70.7 (SD = 17.25). While both scores are around the typical benchmark value of 68 for "good usability" [25], we note that they serve only as a reference: the data collection process for each participant is intensive, and our prototype uses a basic design and leaves plenty of room for usability improvements, e.g., the compass in the rotation app could be replaced by more intuitive animations. We expect that users carrying out a more realistic task would report even higher usability scores.

We gain further insights into usability from the interviews. The majority of participants agreed that both tasks were easy to learn and complete, and they found them to be highly noticeable and engaging. We find a fairly equal preference between rotation and tap, each having its own pros and cons. Rotations were often liked for their simplicity—users do not need to think much, but merely follow the instructions. However, almost all participants suggested that the compass should be better designed (e.g., remove extraneous information). Taps, on the other hand, were found to be more convenient by other people as they do not require constant visual attention to the phone. Yet, some participants thought it is challenging to perform randomly, and some found it less engaging than rotation, which felt more like a game. Furthermore, two participants reported slight dizziness at the end of the user study, but also mentioned that this was due to the repetition of 24 rotations and that less rotations will alleviate this issue.

As for the preference between Medtronic's solution and ours (see Table 3), 21 out of 24 participants favored our proposed methods. Many participants mentioned that they felt in *control* of their IMD using our key exchange techniques, even though we never explicitly used the word "control" during the interview. A common sentiment was the desire for higher transparency during the key exchange process. For example, participant p21 stated, "I think I have the right to know immediately and directly, who can pair my pacemaker, who's pairing and how it's going to be paired". In contrast, the remaining three participants prioritized convenience and did not think somebody would ever attack them. Overall, these observations validate the significance of our design. *i.e.*, using human motion as an OOB channel for IMD key exchange.

7 DISCUSSION

This paper proposes a novel IMD key exchange protocol that involves the user performing several simple bodily motions, aiming to enhance both security and deployability compared to previous OOB-based IMD key exchange techniques. Overall, we find that as few as 3 rotations, or 4 taps, yield an FAR of 0 and an FRR below 2%, signifying low threats from adversaries and high reliability for legitimate users. The entropy values for these motions—18.6 or 28.4 bits—are comparable with previous work [2] (20 bits) and conventional six-digit PIN codes (19.9 bits) that are commonly employed in Bluetooth technologies and other security systems. We believe that these motions serve as adequate input of a PAKE [2]. Note that if needed, higher entropy can be easily achieved by performing more motions. Additionally, like many other OOB channels mentioned in Section 3.1, our key exchange protocol works on an ad-hoc basis and does not require protection of specific external devices.

Our user study validates that the key exchange process is easy to understand, learn, and execute, even in their current simplistic prototype form. Theoretically, if the patient is unable or unwilling to perform the motions, medical staff can conduct the taps on the patient's body, and rotations could be performed on a wheelchair (or stretcher) with their assistance (to be tested empirically as future work). This can take the pressure off the patient but still retains the

[3]In our study, participants often completed the rotations in a duration much shorter than the 10-second window set by our prototype. Thus, future design can consider shortening the window.

high perception level. Further investigations are needed to validate the feasibility.

For deployability, our methods only require an inertial sensor that already exists in modern IMDs [37, 42, 47]. Three rotations take roughly 13.8 s to complete, and four taps require about 3.6 s. We argue that such durations strike a good balance: they are long enough to be noticeable by the patient, yet short enough to maintain usability and safety in emergencies. Moreover, our prototype algorithms (and cryptographic algorithms such as fuzzy primitives [67] and PAKE [27]) can operate effectively on 32-bit Cortex-M microcontrollers, which closely resemble the capabilities of an IMD [41]. The energy consumption for OOB key exchange based on 3 rotations and 4 taps is about 16.6 and 4.3 mJ on our Arduino prototype, respectively. Furthermore, our methods are compatible with consumer devices like smartphones and tablets.

7.1 Security against side-channel attacks

The above security analysis assumes that the adversary is limited to guessing only. Due to the use of bodily motions as secrets, our proposed OOB channels inevitably emit a degree of visual and/or auditory (for motion generated noises) side-channel information. Hence, our protocol is vulnerable to advanced eavesdropping attacks based on camera (using computer-vision techniques) or microphone. As a result, the entropy of the bodily motions may be compromised to some extent.

Certainly, this vulnerability is not exclusive to our work; it is a common issue in previous approaches on motion-based key exchange with IoT devices [2, 26, 27, 36, 59, 68], and OOB key exchange with IMDs, such as those using audio [19], vibration [24, 55], and physiological signals [28, 46, 53].

Various defense strategies have been proposed for these works [4–6, 16, 24, 27], and such strategies can also be adapted to our protocol. For instance, attacks using microphones can be significantly attenuated by adding auditory masking signals to the external device using an integrated speaker [4, 6]. Camera-based attacks can be mitigated by conducting the key exchange in private settings, like the clinic or patient's home [26, 27]. Additionally, visual obfuscation techniques, e.g., those using infrared light [16], could be added into the external device to impair camera visibility of the user.

We emphasize that for our protocol, in the worst case, adversaries capable of launching advanced side-channel attacks can compromise the security *only while* the legitimate parties are present and conducting the key exchange. In contrast, a potentially greater threat is the possibility of an adversary silently injecting a key into the patient's IMD in daily life, a common vulnerability in previous OOB-based IMD key exchange methods (see Section 3.2). Our use of bodily motions inherently provides a robust defense against injection attacks. This way, patients in public areas (like crowded buses) can feel more secure, as the risk of an adversary nearby attempting to pair with their IMD is fundamentally restricted.

7.2 Main insights from our work

Our work can offer valuable insights for both research community and medical device industry. Firstly, to our knowledge, we are the first to point out a frequently overlooked issue in both academic and industry circles: the lack of patient perception during the IMD key exchange process. Traditional methods often at most require subtle body touch or soft sound/vibration, which may be vulnerable particularly when the patient is in public places.

Secondly, our research suggests that using bodily motions can effectively address this concern. Our empirical studies show that the workload required for key exchange is minimal, and people may be willing to engage with security measures for their IMDs. Note that our work in this paper is preliminary, and there is significant potential to further enhance the key exchange before considering it in real life. For instance, future research could explore more efficient methods for human involvement, such as completing the tapping process by attaching the external device to the body and tapping it with fingers. Furthermore, our prototypes (especially the smartphone apps) can be refined to enhance usability.

7.3 Limitation

Our experiment did not recruit participants who were IMD patients due to ethics constraints of the institutions where the study was conducted. Nevertheless, we believe our results already show promise and provide insights into bodily motion-based IMD key exchanges. Future work could involve collaboration with medical domain experts, such as doctors, emergency workers, and medical company representatives, to refine the key exchange process and validate the techniques with actual IMD patients.

8 CONCLUSION

In this paper, we systematize previous approaches that use OOB channels to exchange keys with IMDs, and show that they generally have security limitations and other issues. We then develop a novel IMD key exchange protocol, utilizing human bodily motions as a new OOB channel. We further evaluate our protocol through a user study. We hope that our work serves as a reference to reason more systematically about the use of OOB channels together with cryptographic protocols for key exchange in body area networks.

ACKNOWLEDGMENTS

This research was partially funded by the UK Engineering and Physical Sciences Research Council (EPSRC) under grants EP/R012598/1 and EP/R007128/1, NHMRC grants 1170937 and 2004316, AUSMURI grant 13203896, and CISCO grant 2021-2327463696. Mo Zhang is funded by a joint Priestley PhD Scholarship from the University of Birmingham and the University of Melbourne.

REFERENCES

[1] Carlisle Adams and Steve Lloyd. 2003. *Understanding PKI: concepts, standards, and deployment considerations.* Addison-Wesley Professional.

[2] Imtiaj Ahmed, Yina Ye, Sourav Bhattacharya, N. 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.

[3] Achraf Ben Amar, Ammar B Kouki, and Hung Cao. 2015. Power approaches for implantable medical devices. *Sensors* 15, 11 (2015), 28889–28914.

[4] 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.

[5] S. Abhishek Anand and Nitesh Saxena. 2017. A Sound for a Sound: Mitigating Acoustic Side Channel Attacks on Password Keystrokes with Active Sounds. In *Financial Cryptography and Data Security*. 346–364.

[6] S Abhishek Anand and Nitesh Saxena. 2018. Noisy vibrational pairing of IoT devices. *IEEE Transactions on Dependable and Secure Computing* 16, 3 (2018), 530–545.

[7] Lawrence Bassham, Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Stefan Leigh, M Levenson, M Vangel, Nathanael Heckert, and D Banks. 2010. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.

[8] S.M. Bellovin and M. Merritt. 1992. Encrypted key exchange: password-based protocols secure against dictionary attacks. In *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy*. 72–84.

[9] Philipp Bobek. 2022. Compass. https://github.com/Kr0oked/Compass.

[10] Bosch. 2014. *BNO055, Intelligent 9-axis absolute orientation sensor.* https://cdn-shop.adafruit.com/datasheets/BST_BNO055_DS000_12.pdf Rev. 1.2.

[11] Cybersecurity and Infrastructure Security Agent. 2020. Medtronic 2090 Carelink Programmer Vulnerabilities (Update C). https://www.cisa.gov/uscert/ics/advisories/ICSMA-18-058-01.

[12] 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*. Article 5, 7 pages.

[13] GlobeNewswire. 2019. Global Active Implantable Medical Devices Market is Expected to Reach USD 30.42 Billion by 2025. https://www.globenewswire.com/news-release/2019/08/08/1898922/0/en/Global-Active-Implantable-Medical-Devices-Market-is-Expected-to-Reach-USD-30-42-Billion-by-2025-Fior-Markets.html.

[14] Alan Godfrey, AK Bourke, GM Olaighin, P Van De Ven, and J Nelson. 2011. Activity classification using a single chest mounted tri-axial accelerometer. *Medical engineering & physics* 33, 9 (2011), 1127–1135.

[15] 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.

[16] HACKADAY. 2020. Using IR LEDS to hide in plain sight. https://hackaday.com/2020/02/28/using-ir-leds-to-hide-in-plain-sight/.

[17] 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.

[18] 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 (2008), 30–39.

[19] 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 (sp 2008)*. 129–142.

[20] Ken Hinckley. 2003. Synchronous Gestures for Multiple Persons and Computers. In *Proceedings of the 16th Annual ACM Symposium on User Interface Software and Technology*. 149–158.

[21] Inwook Hwang, Jongman Seo, Myongchan Kim, and Seungmoon Choi. 2013. Vibrotactile perceived intensity for mobile devices as a function of direction, amplitude, and frequency. *IEEE Transactions on Haptics* 6, 3 (2013), 352–362.

[22] Ari Juels and Martin Wattenberg. 1999. A Fuzzy Commitment Scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security* (Kent Ridge Digital Labs, Singapore) *(CCS '99)*. Association for Computing Machinery, New York, NY, USA, 28–36.

[23] Jonathan Katz, Rafail Ostrovsky, and Moti Yung. 2003. Forward Secrecy in Password-Only Key Exchange Protocols. In *Security in Communication Networks*, Stelvio Cimato, Giuseppe Persiano, and Clemente Galdi (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 29–44.

[24] 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 (DAC)*. 1–6.

[25] James R Lewis. 2018. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction* 34, 7 (2018), 577–590.

[26] 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* (Los Cabos, Mexico) *(MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, Article 33, 17 pages.

[27] 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* (Virtual Event, USA) *(CCS '20)*. Association for Computing Machinery, New York, NY, USA, 309–323.

[28] 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* (Montreal, Quebec, Canada) *(IPSN '19)*. Association for Computing Machinery, New York, NY, USA, 265–276.

[29] Zhirong Lin, Yongsheng Xiong, Houde Dai, and Xuke Xia. 2017. An Experimental Performance Evaluation of the Orientation Accuracy of Four Nine-Axis MEMS Motion Sensors. In *2017 5th International Conference on Enterprise Systems (ES)*. 185–189.

[30] 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* (Toronto ON, Canada) *(SACMAT '19)*. Association for Computing Machinery, New York, NY, USA, 113–122.

[31] Eduard Marin, Mustafa A. Mustafa, Dave Singelée, and Bart Preneel. 2016. A Privacy-Preserving Remote Healthcare System Offering End-to-End Security. In *Ad-hoc, Mobile, and Wireless Networks*, Nathalie Mitton, Valeria Loscri, and Alexandre Mouradian (Eds.). Springer International Publishing, Cham, 237–250.

[32] 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* (Los Angeles, California, USA) *(ACSAC '16)*. Association for Computing Machinery, New York, NY, USA, 226–236.

[33] 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* (New Orleans, Louisiana, USA) *(CODASPY '16)*. Association for Computing Machinery, New York, NY, USA, 113–120.

[34] Eduard Marin, Dave Singelée, Bohan Yang, Vladimir Volski, Guy A. E. Vandenbosch, Bart Nuttin, and Bart Preneel. 2018. Securing Wireless Neurostimulators. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy* (Tempe, AZ, USA) *(CODASPY '18)*. Association for Computing Machinery, New York, NY, USA, 287–298.

[35] Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin, and Gene Tsudik. 2017. Authentication using pulse-response biometrics. *Commun. ACM* 60, 2 (2017), 108–115.

[36] Rene Mayrhofer and Hans Gellersen. 2007. Shake Well Before Use: Authentication Based on Accelerometer Data. In *Pervasive Computing*, Anthony LaMarca, Marc Langheinrich, and Khai N. Truong (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 144–161.

[37] Medtronic. 2016. Rate Response (RR) Feature. https://www.medtronicacademy.com/features/rate-response-rr-feature.

[38] Medtronic. 2020. BlueSync Technology Within Implantable Cardiac Devices. https://europe.medtronic.com/xd-en/healthcare-professionals/therapies-procedures/cardiac-rhythm/cardiac-device-features/bluesync-technology.html.

[39] Medtronic. 2021. Insulin pump systems. https://www.medtronic.com/us-en/healthcare-professionals/products/diabetes/insulin-pump-systems.html.

[40] Medtronic. 2021. MyCarelink mobile app. https://global.medtronic.com/xg-en/mobileapps/patient-caregiver/cardiac-monitoring/mycarelink-heart-app.html.

[41] Medtronic. 2022. Azure Pacing System. https://europe.medtronic.com/xd-en/healthcare-professionals/products/cardiac-rhythm/pacemakers/azure.html

[42] Medtronic. n.d.. Medtronic Sensor. https://www.cardiocases.com/en/pacingdefibrillation/specificities/programming-exercise/medtronic/medtronic-sensor.

[43] Oracle. 2023. Java Class SecureRandom. https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html.

[44] Lara Ortiz-Martin, Pablo Picazo-Sanchez, Pedro Peris-Lopez, and Juan Tapiador. 2018. Heartbeats do not make good pseudo-random number generators: An analysis of the randomness of inter-pulse intervals. *Entropy* 20, 2 (2018), 94.

[45] 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.

[46] Carmen CY 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.

[47] 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 (2020), 1–11.

[48] 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.

[49] Girish Revadigar, Chitra Javali, Weitao Xu, Athanasios V Vasilakos, Wen Hu, and Sanjay Jha. 2017. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. *IEEE Transactions on Information Forensics and Security* 12, 10 (2017), 2467–2482.

[50] Luca Reverberi and David Oswald. 2017. Breaking (and Fixing) a Widely Used Continuous Glucose Monitoring System. In *Proceedings of the 11th USENIX Conference on Offensive Technologies* (Vancouver, BC, Canada) *(WOOT'17)*. USENIX Association, USA, 18.

[51] 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.

[52] Marc Roeschlin, Ivan Martinovic, and Kasper Bonne Rasmussen. 2018. Device Pairing at the Touch of an Electrode.. In *NDSS*, Vol. 18. 18–21.

[53] Masoud Rostami, Ari Juels, and Farinaz Koushanfar. 2013. Heart-to-Heart (H2H): Authentication for Implanted Medical Devices. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. 1099–1112.

[54] 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*. 524–539.

[55] 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 (PerCom)*. 181–188.

[56] 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 (HealthSec 10)*. USENIX Association, Washington, DC.

[57] Boston Scientific. 2017. Boston scientific electromagnetic (EMI) compatibility table for pacemakers, transvenous ICDs, S-ICDs and heart failure devices. *Tech Guide* (2017).

[58] 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.

[59] Mohit Sethi, Markku Antikainen, and Tuomas Aura. 2014. Commitment-based device pairing with synchronized drawing. In *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 181–189.

[60] Muhammad Ali Siddiqi, Robert HSH Beurskens, Pieter Kruizinga, Chris I De Zeeuw, and Christos Strydis. 2021. Securing implantable medical devices using ultrasound waves. *IEEE Access* 9 (2021), 80170–80182.

[61] MTCAJ Thomas and A Thomas Joy. 2006. *Elements of information theory*. Wiley-Interscience.

[62] 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 INFOCOM 2019 - IEEE Conference on Computer Communications*. 1135–1143.

[63] Marc Simon Wegmueller, Sonja Huclova, Juerg Froehlich, Michael Oberle, Norbert Felber, Niels Kuster, and Wolfgang Fichtner. 2009. Galvanic coupling enabling wireless implant communications. *IEEE Transactions on Instrumentation and Measurement* 58, 8 (2009), 2618–2625.

[64] Wang Wei, Lin Yang, and Qian Zhang. 2018. Resonance-based secure pairing for wearables. *IEEE Transactions on Mobile Computing* 17, 11 (2018), 2607–2618.

[65] 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.

[66] Weitao Xu, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. 2016. Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure on-Body Device Communication. In *Proceedings of the 15th International Conference on Information Processing in Sensor Networks*. Article 3, 12 pages.

[67] 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*. 289–309.

[68] Tengxiang Zhang, Xin Yi, Ruolin Wang, Yuntao Wang, Chun Yu, Yiqin Lu, and Yuanchun Shi. 2018. Tap-to-pair: associating wireless devices with synchronous tapping. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–21.