Zuo, Si; Sigg, Stephan; Nguyen, Le; Beck, Nils; Jähne-Raden, Nico; Wolf, Marie Cathrine

CardioID: Secure ECG-BCG Agnostic Interaction-Free Device Pairing

Published in:
IEEE Access

DOI:
10.1109/ACCESS.2022.3226503

Published: 02/12/2022

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 October 2022, accepted 23 November 2022, date of publication 2 December 2022,
date of current version 14 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3226503

RESEARCH ARTICLE

CardioID: Secure ECG-BCG Agnostic Interaction-Free Device Pairing

SI ZUO[1], STEPHAN SIGG[1], LE NGU NGUYEN[2], NILS BECK[3], NICO JÄHNE-RADEN[4], AND MARIE CATHRINE WOLF[4]

[1]Department of Communications and Networking, Aalto University, 02150 Espoo, Finland
[2]Faculty of Information Technology and Electrical Engineering, University of Oulu, 90570 Oulu, Finland
[3]Institute for Natural Language Processing, University of Stuttgart, 70569 Stuttgart, Germany
[4]Peter L. Reichertz Institute, 30625 Hannover, Germany

Corresponding author: Si Zuo (si.zuo@aalto.fi)

ABSTRACT Usably secure ad-hoc device pairing fosters connectivity with hardware which is difficult to access (e.g., implanted) and grants convenience for ad-hoc short-term on-off pairing patterns (e.g. shared public domain). Examples are medical devices or fitness equipment. We present CardioID, an approach to extract features from heart rate variability for secure pairing keys that change with the randomness inherited in heart operation. Our processing chain is compatible with electrocardiogram (ECG, voltage), as well as ballistocardiogram (BCG, acceleration) type signals. Dissimilarities in locally generated sequences are accounted for using fuzzy cryptography exploiting Bose–Chaudhuri–Hocquenghem (BCH) codes. We propose a quantization to derive secure keys for cross BCG-ECG device pairing from heart-rate variability and analyze the performance in (inter- and intra-subject) BCG-to-ECG pairing. A secure communication protocol for Body Area Networks (BAN) is discussed. The attack surface of the protocol is analyzed, and we conduct a video-based attack study. In addition, two case studies with 5 (laboratory) and 20 (controlled in-field) subjects were conducted.

INDEX TERMS Ballistocardiogram (BCG), bioinformatic, body area network, devices pairing, electrocardiogram (ECG), healthcare, usable security.

I. INTRODUCTION

An electrocardiogram (ECG) is a diagnostic test to evaluate the heart's rhythm and electrical activity (i.e. voltage over time). ECG sensors are commonly found in medical and fitness equipment. On the other hand, common acceleration sensors may also obtain information on the heart's functioning when placed on the skin by measuring the body's response to ballistic forces related to cardiac contraction and ejection of blood into the vasculature (ballistocardiography (BCG), acceleration over time). Together, the number of devices capable of ECG or BCG is large, such as watches (wrist, ECG/BCG), glasses (temple, BCG), fitness chest straps (chest, ECG/BCG), hearing aids (ear, BCG), pacemakers (heart, ECG), implantable cardioverter defibrillators (heart, ECG) or ventricular assist devices (heart, ECG). Connecting these devices is often complicated, with impaired security, or even impossible due to limited accessibility or interfaces.

Prospective applications comprise pairing with devices that are interface-less or difficult to access, such as medical equipment (e.g. pacemaker, hearing aid, implantable cardioverter defibrillators, ventricular assist devices). In the fitness domain, an example is the pairing of chest-strap, smartwatches or smartphones with ECG-monitoring workout machines, such as treadmills, cycling, rowing, arc trainers, etc. (cf. Figure 1). This opens new usably secure application domains since de-authentication is automatic (when access to the BCG or ECG signal is interrupted) so that pairing lasts only for the context of use.

The associate editor coordinating the review of this manuscript and approving it for publication was R. K. Tripathy.

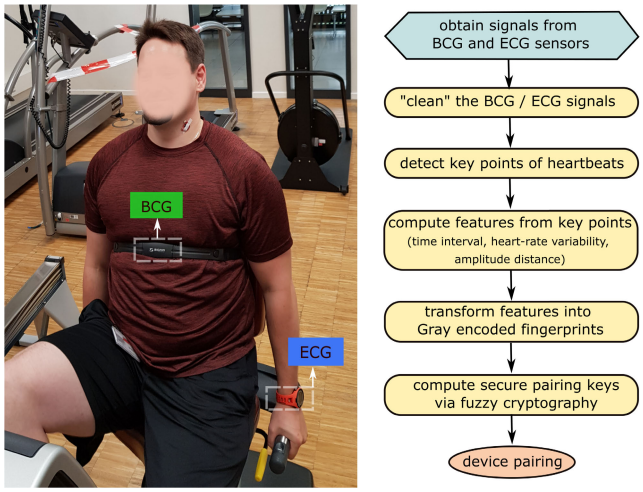
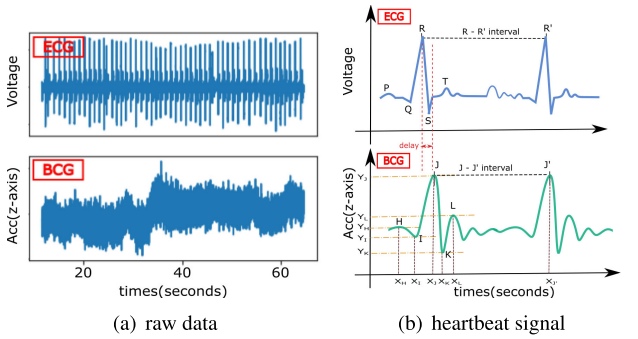


FIGURE 1. Exemplary scenario for ad-hoc device pairing from ECG and BCG readings. Right: operational principle.



(a) raw data (b) heartbeat signal

FIGURE 2. ECG and BCG data. Left: raw data. Right: ECG and BCG signals describing a heartbeat. The five key points in the ECG: P, Q, R, S, T and BCG: H, I, J, K, L. For ECG and BCG data from the same person, the R-R' and J-J' time interval durations are correlated. We utilize the time interval and amplitude related features for pairing.

Interaction-free device pairing generates body-implicit secure keys that exploit the randomness in the heart's operation (ECG or BCG signals). CardioID is the first algorithmic solution to compute implicit secure pairing keys across boundaries of sensing modalities (here: ECG-BCG), hence widening the application range for attention-free authentication. Meanwhile, Simon et al.'s work [1] shows that while cross-context attacks on ECG are less easy compared to eye movements, mouse movements, and touchscreen input, attacks are still more likely to succeed using more recent data. The introduction of BCG signals decreases the probability of successful attacks.

In contrast to traditional explicit pairing mechanisms, such as Bluetooth Secure Simple Pairing which requires comparison of PIN codes, CardioID does not expect explicit interaction and pairing will be maintained only for the context of use and does not require explicit de-authentication [2]. Compared to biometric authentication, CardioID does not have known issues (e.g., theft of biometric data, accumulation of evidence to extract secret biometric features over a longer observation period; etc.) [3]. Instead, it exploits the spontaneous randomness of the heart operation at the moment of pairing, thus taking advantage of the rich transient variability that is perceived as noise by biometric authentication schemes.

We collected both laboratory BCG and ECG data (from 5 healthy subjects) as well as noisy in-field data (from 20 healthy subjects) and used heart-rate variability for device pairing. The main research questions addressed regard:

Multi-modality implicit pairing: we identify features that support cross modality implicit key generation in secure device pairing from voltage or acceleration (section III).

Cross-modality usably secure pairing: with CardioID we present the first ECG-BCG capable implicit ad-hoc secure pairing scheme (section III).

Communication protocol: we present a secure communication protocol based on CardioID (section III).

Sourcecode and Datasets: we verify CardioID on two ECG/BCG datasets. The sources and the data are made available (section IV).

Entropy of ECG and BCG pairing keys: we report on the randomness contained in heart-rate variability based fingerprint sequences (section V).

Robustness against attacks of various strength: in our security analysis, we discuss the robustness of the protocol against attackers with different capabilities and resources, including spoofing as well as real-time video processing (section VII).

II. RELATED WORK

The cardiac cycle, i.e. the activity of the heart over a single heartbeat, can be divided into a systolic phase when the heart contracts and causes the blood to flow out, and a diastolic phase when the heart relaxes and refills with blood [4]. Likewise, ballistocardiography (BCG) measures the body's response to ballistic forces related to cardiac contraction and ejection of blood into the vasculature (cf. Figure 2) [5].

From Figure 2(a), observe that ECG is a graph of voltage over time, while BCG is measured by accelerometers.

Distinguishing individual heartbeats from BCG and ECG is an active research topic [6], [7], [8], [9]. Detecting heartbeats from ECG exploits the Q-R-S complex (cf. Figure 2) [10]. In [6], an R-peak detector based on the Shannon energy envelope preprocessing and automated peak-finding is proposed. Due to the rapid development of Machine Learning, some neural network models have also been applied to denoise the ECG data and to obtain accurate Q-R-S complexes [11]. Gupta et al. [12] applied chaos theory for an accurate analysis of different ECG databases and uses the Short-time Fourier transform (STFT) to detect the R-peak. An adaptive threshold is used to detect the peak points of a BCG sequence in [13] and, similarly, after data filtering and transformation between time and frequency domains, basic peak detection is used [14]. In contrast, Liu et al. [9] filtered

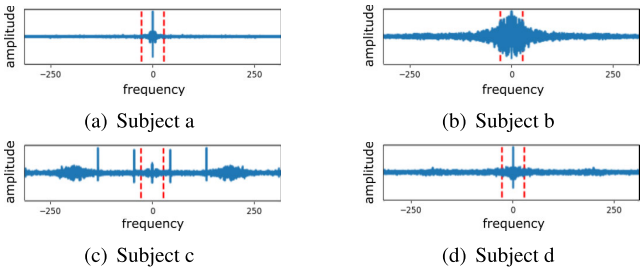


FIGURE 3. Frequency domain data from four subjects. For each subfigure, data between the red dashed lines is considered to contain both heartbeat and noise signals. The rest of the data is considered to be noise.

out the interval of the normal heartbeat range to obtain an accurate interval.

ECG measurement with medical equipment is reliable and accurate, but the need for disposable wet electrodes and device cost render medical measurement equipment unsuited for private continuous use. However, true ECG measurement capability has recently debuted in consumer smart watch equipment such as in smartwatch products from Apple, Fitbit, Samsung or Withings. Alternatively, ballistic forces caused by the contraction and expanding of the heart muscle as well as the pulse wave sent through the vascular system by this operation, can be used to obtain information on the functioning of the hearts from acceleration sensors on the body surface (ballistocardiography - BCG) [15], [16].

Traditionally, device pairing requires explicit input, for instance, by confirming or providing several integer digits [17]. Recently, implicit pairing schemes have been proposed, e.g. based on acceleration [3], [18], [19], [20], [21], audio [22], [23], magnetometer [24], or RF features [25]. Such schemes rely on similar patterns detected across these modalities for devices co-present in the same context to establish secure secrets. An example is gait-based pairing of devices that are jointly carried by a human subject [26], [27], [28]. These approaches exploit the correlation in acceleration signals when devices are worn on the same body [29], [30] or shaken together [18], [19], [20], [31].

Most related to our work are approaches that exploit signals obtained from the heart's functioning. Lin et al. [32] proposed a secure device pairing method based on the skin vibrations caused by heartbeat. The data is measured by piezo vibration sensors and the authors exploit the variation between consecutive J-peaks as their shared source of secrecy. However, the method can not establish a secure pairing between a pair of devices since the measured peak interval is shared between devices for comparison. In our protocol, there is no need to exchange information during the stage of fingerprint generation. We further exploit the noise in the decimal place of Gray encoded peak-to-peak time interval information.

Another related work is [33], which proposes a fuzzy-cryptography based device pairing for ECG data. However, the protocol is limited to ECG capable devices. In contrast, we derive features that allow cross-modality BCG-ECG pairing, which greatly increases the number of compatible device pairing combinations. In particular, smart watches and smart glasses usually possess acceleration sensors, while ECG sensing capability is not yet widely spread. Likewise, many fitness machines, such as treadmills, cycling, rowing, arc trainers, feature ECG sensors, but seldom other means to measure the heart operation.

III. RATIONALE AND METHODOLOGY

CardioID is a mechanism to pair previously non-acquainted devices without explicit user-device interaction. Instead, secure keys are generated from sensor readings of a jointly observed stimuli. In particular, CardioID extracts information about the variation in the operation of the heart muscle from ECG or BCG signals. The randomness (cf. section V) in the operation of the heart is exploited to generate a pattern which serves as the seed of a secure secret in a PAKE protocol (cf. section III-E). Since the BCG and ECG stimuli measured at various body positions are generated by the same process (the operation of the heart), BCG peaks experience a constant lag to ECG peaks and both signals can be used interchangeably with respect to the heart-rate variability. Through fuzzy cryptography, devices are capable of independently generating identical secrets from these similar, correlated ECG/BCG heart-rate variability patterns, by mapping these sequences into the key space of an error correcting code to correct errors with respect to the codes' legitimate codewords (cf. section III-D). In order to obtain the heart-rate variability, first, heartbeats are detected (section III-C) from pre-processed (section III-B) ECG and BCG data obtained through contact to the skin of the same subject (section III-A).

A. STIMULI OBTAINED FROM ECG AND BCG

An electrocardiogram (ECG) represents a signal of voltage over time of the electrical activity of the heart. It is measured using electrodes placed on the skin. In contrast, a ballistocardiogram (BCG) measures ballistic forces generated by the contraction of the heart muscle, captured by acceleration sensors in direct contact to the skin [34].

Conceptual ECG and BCG signals are shown in Figure 2. The ECG signal features five key points which can be found in every heartbeat. These are the **P, Q, R, S** and **T** [10]. A BCG measurement, on the other side, features different signal key points, which are referred to as **H, I, J, K** and **L** the in figure.

During the heart's operation, the electric stimulation (ECG) occurs first, closely followed by the muscle contraction (BCG). Consequently, the captured peaks from ECG and BCG signals do not occur in parallel, but BCG will be observed with several milliseconds delay.

However, the inter-peak intervals (e.g. the **JJ** intervals and **RR** intervals in Figure 2) experience small random variation over time, which are identical across BCG and ECG for a single heart-beat pair. We exploit the inherent randomness (the heart-rate variability) of BCG and ECG for cross-modality generation of secure keys for ad-hoc spontaneous device pairing.

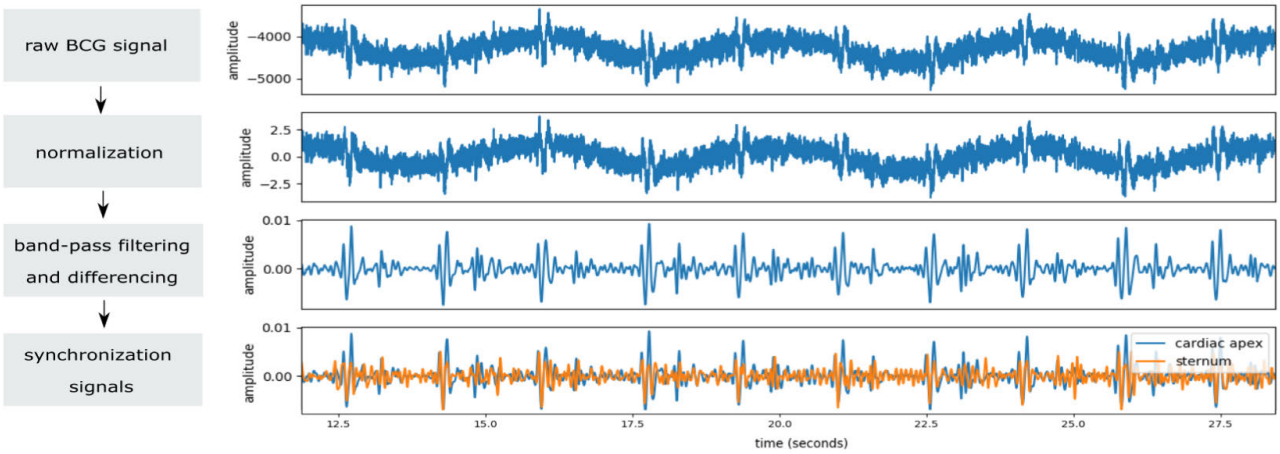


FIGURE 4. Data pre-processing. The raw BCG signal is normalized to zero means and unit variance, before band-pass filters and differencing are applied. The last row shows data from sternum (orange) and cardiac apex (blue) after synchronization.

B. DATA PREPROCESSING

We conducted two experiments to test CardioID. In particular, we collected data from 5 heart-healthy subjects under controlled laboratory conditions to be able to derive stable and robust features and further evaluated the approach on data collected during an in-field study from 29 heart-healthy subjects (cf. section IV). An issue we faced on the first day of the in-field measurements was a problem with the ECG hardware sensors, which resulted in various artifacts, such as 'noise-only' or 'signal absence', that rendered the data of 9 subjects unusable. After removing these measurements, we conducted all further processing with the remaining 20 subjects.

Figure 3(c) and 3(d) depict the noisy recordings. In these figures, the signals have a wider frequency range and the signal-plus-noise-to-noise ratio is smaller.

To address the oversampling in our data, we then resampled the data to the *de facto* sampling frequency of about 1750Hz.

The further processing is detailed in Figure 4 for cardiac apex (blue) and sternum (orange) data. In particular, the data was normalized with zero mean and unit variance (2nd row in Figure 4), band-filtered to disregard both low and high frequency noise with a third-order Butterworth bandpass filter with cutoff frequencies at 7 and 40Hz, as suggested by [36], [37], and [38].

To stabilize the mean of the data, we applied differencing which removes changes in the level of the data, thereby eliminating (or reducing) trend and seasonality (3rd row in Figure 4). Since the data is recorded from different body locations, it might show delay. Therefore, in the final step, we synchronized the data based on the public prototype-pattern-based alignment approach proposed in [38] and fast dynamic time warping (DTW) [39] (4th row in Figure 4). In particular, we utilize a pre-defined, few seconds long fingerprint sequence (we utilize a characteristic, synthetic sequence) which is not actually extracted from ECG/BCG data, compute (via DTW) and share the time-offset to the best match with the local sequence with the remote device, where the same procedure is conducted. While the synthetic sequence is not extracted from the observed sequences, its best match is with high probability identical for sequences that are related, such as the ECG or BCG sequences computed by the remote devices. By shifting the fingerprint sequences according to the observed best match from the DTW with the synthetic sequence, the data from the remote devices is brought into agreement without the need to exchange actual information on the ECG or BCG data. It takes around 0.8 seconds for preprocessing data with a length of 30 seconds (CPU: 11th Gen Intel(R) Core(TM) i5-1135G7@2.40GHz 1.38 GHz; RAM: 16.0 GB).

After synchronization, fingerprints are computed from **JJ** and **RR** peaks after the end of the sequence that has been used for the synchronization on the respective devices (cf. section III-D).

C. HEARTBEAT DETECTION

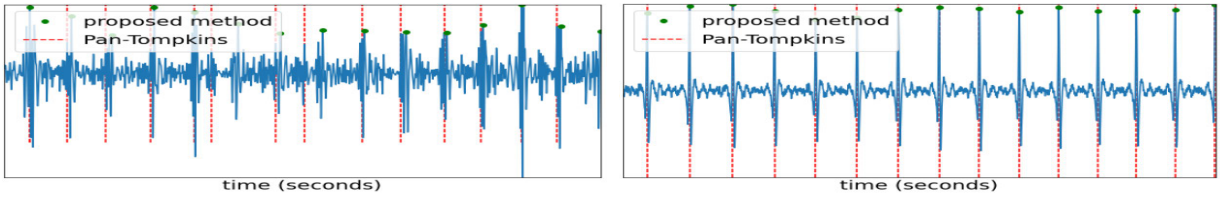
Both BCG and ECG signals feature a recognizable waveform with distinctive peaks and valleys [34]. Considering the properties of heartbeat and peak points from previous research [40], [41], [42], we set up the rules for peak point filtering. Specifically, the detection of BCG key points starts from the detection of **J** peaks [43], [44]. Local minima and maxima (candidate peak points) are filtered:

Distinctive peak rule The maximum is located between two minima, which is considered to be one of the peaks **J**.

Appropriate timing rule (1) The time interval of the selected two minima is within 0.06 to 0.12 seconds.

For all **J** peaks found, we detect and remove outliers based on Hampel filter [45]. The filter calculates the median time over a **JJ** peak interval and its six surrounding intervals, three on each side. A peak that differs from the median absolute deviation by more than three standard deviations is replaced.

In our case, for each pair of adjacent **J** peaks, if the time interval exceeds 1.6 times the average, a new peak **J** is



(a) BCG (b) ECG

FIGURE 5. R peak detection performance. Points in green represent the peak detected by CardioID; dashed red lines represent peaks detected by Pan-Tompkins algorithm.

inserted (by detecting a new local maximum from the clip sequence as a peak). On the other hand, for time intervals 0.4 times below the average, the peak **J** is removed.

Peak **H** and peak **L** are found as:

Peak order rule (1) For each heartbeat, the index of the peak **H** is in front of the index of peak **I**.

Appropriate timing rule (2) Time interval of corresponding peaks **H** and **J** is within 0.12 to 0.20 seconds. The selected values are based on the previous work of other researchers and can be applied on any subjects.

Peak order rule (2) For each heartbeat, the index of the peak **L** will be larger than the index of valley **K**.

Appropriate timing rule (3) The time interval of peak **L** and valley **I** is within 0.35 to 0.43 seconds. Similarly, the selected values are based on the previous work of other researchers and can be applied on any subjects.

ECG peak detection works analogously. Figure 5 shows examples of detected **R** peaks in BCG and ECG data. Compared to state-of-the-art ECG peak detection [46], we achieved a root-mean-square error (RMSE) in the range of 0.0303 sec to 0.1621 sec which confirms that our key point detection is satisfactory.[1]

After obtaining the key points, the time interval features are computed from these key points. Given the peaks **J** and **R**, lists of time intervals are obtained as $t_{J'} - t_J$ and $t_{R'} - t_R$, where **J** and **J'** (as well as **R** and **R'**) are adjacent peaks, and t is the corresponding timestamp. After computing time interval lists $T_{BCG} = \{t_{interval_0}, t_{interval_1}, \ldots, t_{interval_n}\}$ and $T_{ECG} = \{t_{interval_0}, t_{interval_1}, \ldots, t_{interval_n}\}$, we are able to encode the features.

D. PAIRING BASED ON ECG AND BCG SIGNALS

To generate fingerprints for device pairing based on ECG and BCG signals, we exploit the inherently random variance in **JJ** and **RR** peak intervals (heart-rate variability).

We use variation in the second last digit of its hexadecimal encoding, while throwing away higher order digits (low variance) and lower order digits (noise).[2] This value is then encoded to give a 4-digit binary representation of each **RR** or **JJ** interval (Gray Coded) and a fingerprint f constitutes a concatenation from 8 consecutive intervals (32 bits). The procedure of encoding the time interval for pairing is shown in Figure 6. The transformation to hexadecimal representation is necessary to ensure that all bits in the 4-bit Gray encoding are equally likely in the resulting key sequence.

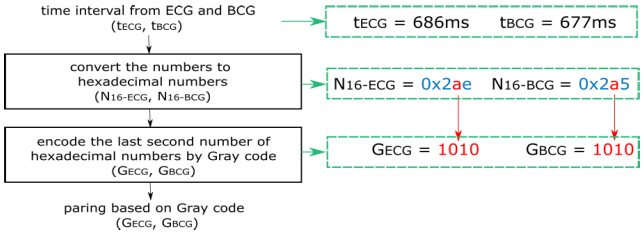


FIGURE 6. The procedure for encoding the time interval for pairing: the green boxes show an example of the procedure.

After independent generation of the fingerprints f, f' on two devices, pairing is achieved via fuzzy cryptography. In particular, the fingerprint (concatenation of 8 gray-encoded 4-digit sequences from two consecutive **J** (**R**) peaks) can be mapped into the code space $\mathcal{C}$ of a BCH error correcting code. Since the timing of BCG and ECG signals are identical but shifted (BCG is triggered by the ECG pulse), both BCG and ECG timings can be used interchangeably. To apply the error correction, one device chooses a codeword $c \in \mathcal{C}$ as anchor point and derives the distance d between c and its fingerprint f in the codespace $\mathcal{C}$. d is a vector to transform f into $c = f \bigoplus d$. d is then shared with the second device, which may be overheard by an adversary. Any device with access to a fingerprint f' of sufficient similarity to f (distance in the codespace smaller than the error correction distance δ of the employed BCH error correcting code) will achieve $DEC(c') = DEC(c) = DEC(f' \bigoplus d)$ (e.g. simultaneous ECG/BCG measurements from the same subject). Fingerprints f'' with distance to f larger than δ, yield $DEC(c'') = DEC(f'' \bigoplus d)$ with $DEC(c'') \neq DEC(c)$. A separation between inter- and intra-person pairings is therefore possible with CardioID.

[1] Pan-Tompkins algorithm is considered as a reference and is not error-free. It is infeasible to acquire an error-free ground truth through BCG or ECG measurement.

[2] We chose hex encoding to ensure that, after transforming to gray-coded 4 digit binary representation, all binary sequences are equally likely.

E. PAIRING PROTOCOL

Various key agreement protocols are compatible with CardioID. We suggest the use of a protocol which reduces the adversary to a one-shot man-in-the-middle attacker in a two-party adversarial model, for instance, by constraining the attacker to only one try by extending a Diffie-Hellman key exchange. Possible implementations include a hash commitment before revealing public values (cf. Vaudenay [47]). Similarly, Password Authenticated Key Exchanges (PAKE) restrict the success probability of an attacker on the interaction during protocol execution (e.g. Bluetooth Secure Simple Pairing (SSP), IPSec, and ZRTP [48], [49], [50]). Since either device may initiate the protocol, a ''balanced'' PAKE should be used. We assume a two-party adversarial model. A modern PAKE provides resilience to dictionary attacks, replay attacks, unknown Key-Share attack, and Denning–Sacco attacks [51] and provides mutual authentication, key control, known-key security and forward secrecy. Note that CardioID does not require passkey secrecy of a previous authentication attempt, since an attacker is not able to exhaust the key-space via multiple repeated attacks, because the key changes with each attempt (cf. section V). Previously learned parts are not reused as the protocol prevents the use of heart-rate variability data from the same **RR** or **JJ** interval in different pairing attempts. In particular, we forbid parallel protocol runs so that an attacker may not boost her success probability by pretending to be multiple devices.

For the integration of CardioID into real-world applications, we suggest an integration of an additional Out-of-Band mode besides NFC, providing the Bluetooth passkey. This is considered secure under the PE(i) model in [17].

As sketched in Fig. 7, CardioID utilizes fuzzy cryptography, which shortens the extracted bit sequence so that the final key length is smaller. Threat models, such as [17], choose a relatively high key length of 24. Bluetooth (and ZRTP) have a similar margin of 20 identical bits for PIN (word) comparison. Since the key is generated automatically, we can keep a tighter margin and propose a target a bit size of 16 for a one-shot success probability of 2^{-16}.

IV. EXPERIMENTAL EVALUATION

In this section, we present the results for both laboratory and in-field studies. The data collection plan was evaluated and approved by the ethics committee at our university. All participants were informed about the nature of the study, how data was anonymized and stored, and about the possibility to withdraw their written consent at any time.

For the laboratory experiment, we used the Movesense[3] motion sensor as the acceleration sensor and a four-lead Shimmer3 ECG Unit as ECG sensor.[4] The subjects were asked to lie still with stable breath and to avoid any body movement. For each subject, we took 5 measurements and each measurement lasted 3 minutes. The acceleration sensor

[3]https://www.movesense.com/specifications/

[4]http://www.shimmersensing.com/

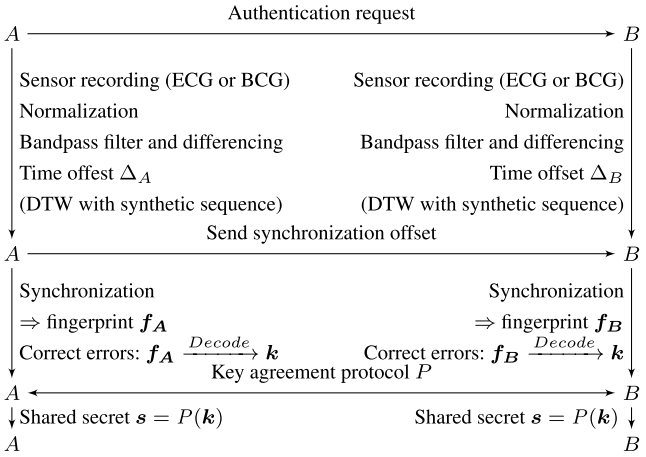


FIGURE 7. CardioID pairing protocol for devices *A* and *B* with access to ECG or BCG signals from the same body.

was placed on position B with a belt (as shown in Fig. 1) while the ECG data was collected simultaneously with electrode pads at positions R, L, N, F as shown in Figure 8. In a real-world implementation, wireless sensors (or wearable) will be chosen for both BCG and ECG data collection (cf., Fig. 1).

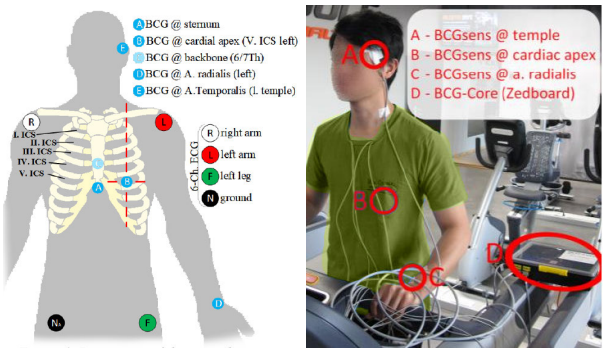
For the in-field study, we used the KX122-1037 acceleration sensors (sensitivity: 16-6384 counts/g, noise: 0.75mg@50Hz). As ECG sensor, we employed a 6-channel ECG OLIMEX shield with 3 electrodes and 10-bit data resolution for each channel.

The measurement started with an initial assessment including a 12-Channel rest and exercise ECG and a questionnaire to check heart healthiness. We excluded participants with current or former diseases or surgeries. Two setups with different sensor positions are used. For the first, sensors are placed at the BCG positions on the sternum, the apex of the heart and the spine (see Figure 8(a) positions A-C). For the second setup, two BCG positions are selected on larger vessels on the temple and wrist with an additional BCG position on the sternum (see Figure 8(a) positions B, D, E).

Data was collected via a Xilinx Zynq-7020 system-on-chip (SoC) that combines a dual-core ARM processor with a Virtex 7 FPGA. For synchronous parallel data readout of the four sensors (3x accelerometers and a 6-Channel-ECG), all SPI controllers use a common clock and each sample is hardware-timestamped.

A. ECG AND BCG SIGNAL PAIRING

For each sensor position, consecutive eight **R-R** (**J-J**) intervals are gray encoded into fingerprints of 32 bits and to obtain identical keys across devices, we utilize fuzzy cryptography (described in section III-D). In a nutshell, fingerprints can be mapped to their closest key in the key space of a BCH error correcting code so that similar fingerprints map to the same (identical) key. The aim for two devices on the same body is to independently generate key sequences from ECG and BCG data which have a high bit similarity.



(a) Positioning of the sensors (b) Subject performing the study

FIGURE 8. Measurement setup in a gym during the user study.

1) PAIRING – CONTROLLED LABORATORY STUDY

Figure 10(a) depicts the percentage of bit errors between pairs of fingerprints from the 5 subjects. The average scores are above 0.6 and some exceed 0.85. Note that a similarity of 0.5 represents the expected similarity to a random binary sequence, for instance, in an uninformed attack. A higher similarity translates to a higher robustness to separate matching keys from non-matching ones via fuzzy cryptography. In particular, the similarity for same-subject BCG-ECG fingerprints needs to be higher than for inter-subject fingerprints so that matching keys can be created for same-subject pairings via fuzzy cryptography while for inter-subject pairing, the generated keys differ.

TABLE 1. Average time difference between matching ECG (R-R) and BCG (J-J) intervals.

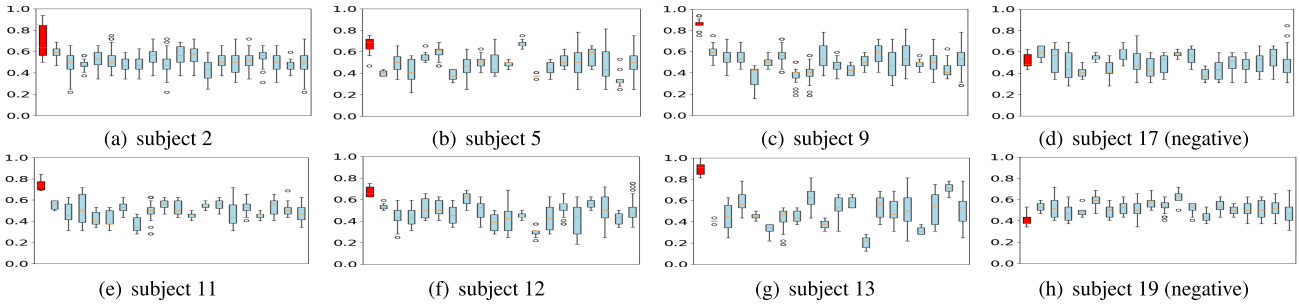
subject	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
offset	0.0192	0.0151	0.0213	0.0481	0.0258	0.0240	0.0103	0.0140	0.0003	0.0219	0.0277	0.0587	0.0005	0.0030	0.0841	0.0365	0.0917	0.0075	0.3689	0.0754

2) PAIRING – IN-FIELD STUDY

We test the robustness of CardioID on the more noisy data collected in the in-field study. Figure 10(b) shows the similarity score over all 20 subjects. The values shown in red are the median of the similarity score. For 19 subjects, the average similarity scores are higher than 0.5.

For both case, most of the subjects achieve acceptable scores for pairing. Based on these scores, we are able to set a threshold to evaluate whether the pairing successes or not.

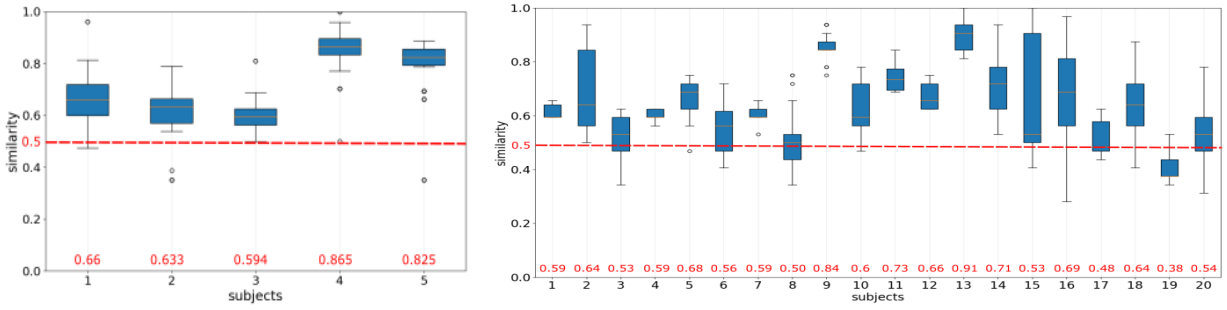
In particular, we report the average difference in the heart-rate variability across **J-J** and **R-R** intervals in Table 1. For subject 17 and subject 19, the distances are highest, which explains their low similarity score. This indicates that it would be possible to detect device combinations with low pairing success probability, and hence could help to assist a wearer of the devices in adjusting misalignment of sensors.



(a) subject 2 (b) subject 5 (c) subject 9 (d) subject 17 (negative)

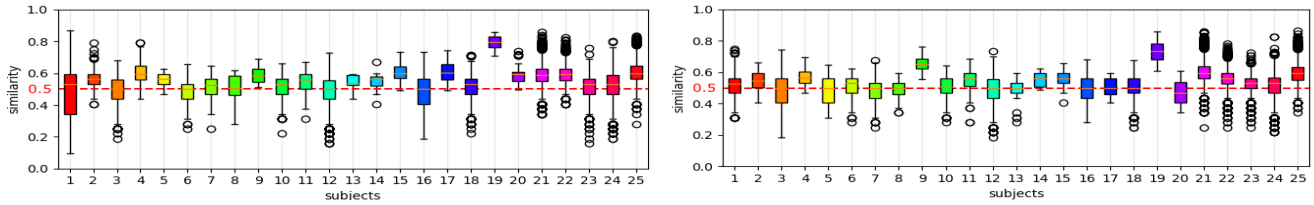
(e) subject 11 (f) subject 12 (g) subject 13 (h) subject 19 (negative)

FIGURE 9. Examples of same-subject (red) and inter-subject (blue) similarity score on data from noisy measurements.



(a) Same-subject similarity from laboratory dataset. (b) Same-subject similarity from noisy measurement.

FIGURE 10. Same-subject similarity of the laboratory dataset (left, 5 subjects) and the data from noisy measurement (right, 20 subjects): the values shown in red represent the median of similarity scores of subjects. In laboratory dataset, the average similarity scores of all subjects are higher than 0.5 and in the meanwhile with a rather small variance. For data from noisy measurement, 95% of the subjects achieved average similarity scores higher than 0.5. The scores of subject 2, 15 and 16 have higher variance.



(a) BCG (b) ECG

FIGURE 11. Similarity score of fingerprints generated from different times of the same subject for both BCG and ECG signals. The scores are computed for 25 subjects (5 from controlled laboratory study and 20 from in-field study). The similarity scores that around 0.5 (random guess) shows that spoofing can not be successful since the method exploits the randomness of the heart operation over time.

TABLE 2. FP, TP, FN, and TN rates for different thresholds.

Similarity THR	FPR	TPR	FNR	TNR
0.5	0.421	0.894	0.106	0.571
0.6	0.133	0.565	0.435	0.866
0.7	0.026	0.312	0.688	0.973
0.8	0.002	0.173	0.827	0.997

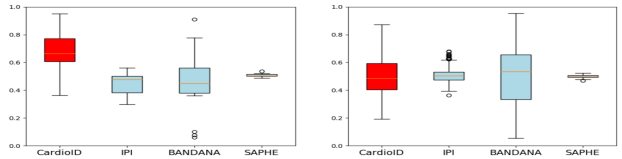
Exemplary inter-subject similarity scores are depicted in Figure 9. The red box represents the similarity score of the same-subject case (BCG and ECG from same subject), while the blue boxes show the score of inter-subject (BCG and ECG from different subjects). In most cases, same-subject similarity exceeds inter-subject similarity, which satisfies our requirements for secure pairing. Since outliers are seldom for inter-subject cases, for continuous pairing, pairing attempts which are not from same-body worn devices can be detected after a few iterations. For subjects 17 and 19, same-subject similarity is not sufficient so that pairing will fail.

We compute the False Positive Rate (FPR), True Positive Rate (TPR), False Negative Rate (FNR) and True Negative Rate (TNR) in table 2 when given different values for the threshold of similarity score.

We also compute the similarity score of fingerprints generated from measurements taken at different times of the same subject. Figure 11(a) and 11(b) show the scores of 25 subjects (5 from the controlled laboratory study and 20 from the in-field study) for both ECG and BCG. For most subjects, the similarity scores are around 0.5 (random guess). This shows that spoofing can not be successful since the method exploits the randomness of the heart operation over time (cf. section VII-B).

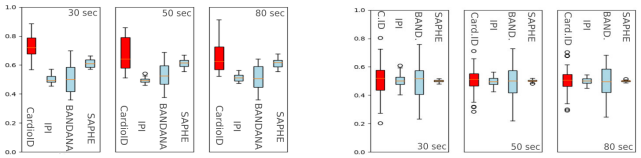
B. COMPARISON TO OTHER PAIRING SCHEMES

We compare CardioID with state-of-the-art implicit secure pairing schemes on both datasets. In particular, we implemented IPI pairing (acceleration gait/BCG) [32], [52], BANDANA (acceleration gait) [3] and SAPHE (acceleration) [20]. The IPI protocol utilizes a random offset by which individual heartbeats deviate from the mean heartbeat cycle in time domain. In BANDANA, the generated fingerprints are based on the difference between the mean and instantaneous acceleration of the heartbeat data. In SAPHE, the generated fingerprints are based on the comparison of random points and corresponding data points.



(a) Same subject (b) Different s.

FIGURE 12. BCG-to-ECG subject similarity on laboratory data.



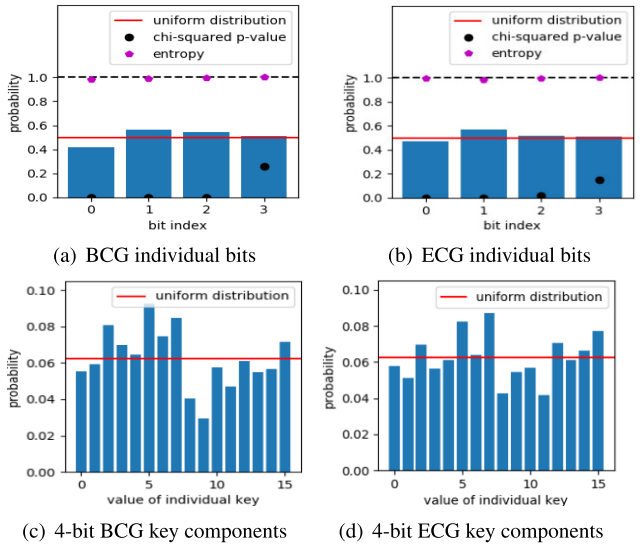
(a) Same subject (b) Different subjects

FIGURE 13. BCG-to-ECG subject similarity on noisy measurements, from 30, 50, 80 sec. of data.

For a fair comparison, and since some schemes were originally developed with different input data in mind, we preprocessed the BCG and ECG data identically for all schemes and only applied the quantization part of the protocols to obtain fingerprints from the ECG and BCG inputs. The performance of each scheme is depicted in Figures 12(a), 12(b), 13(a) and 13(b). Based on the performance in Figures 13(a), we can see that longer pairing time does not improve the similarity score. It also means that 30 seconds is already sufficient for the implicit pairing, without any human interaction.

These figures show the comparison results between CardioID and other quantization schemes in both same-subject and inter-subject cases. They indicate that although affected by outliers, CardioID achieves a higher similarity score in all datasets. In laboratory data, CardioID achieves a similarity of 0.651. BANDANA features the lowest average score (0.423). Also, for noisy measurements, the fingerprint pairs generated by CardioID are most similar in all cases with 0.716 (0.639, 0.624) similarity for 30 (50, 80) seconds of BCG/ECG data. BANDANA achieves the lowest average score (0.491, 0.493, 0.509). Figures 12(b) and 13(b) show the inter-subject similarity score, which is centered around 0.5 (i.e., the similarity expected when compared to random binary fingerprints) for all approaches. The variance is smallest for IPI and SAPHE.

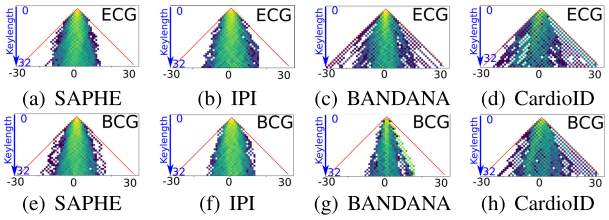
Summarizing, CardioID outperforms the state-of-the-art implicit secure pairing schemes for cardiograph data.



(a) BCG individual bits (b) ECG individual bits

(c) 4-bit BCG key components (d) 4-bit ECG key components

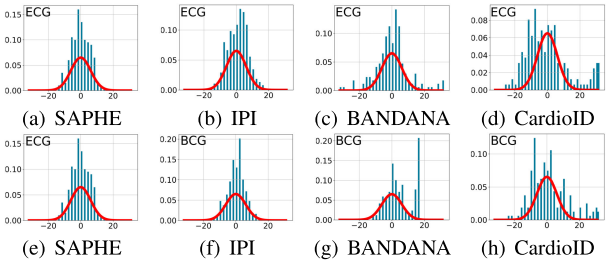
FIGURE 14. Analysis on 4-bit key component.



(a) SAPHE (b) IPI (c) BANDANA (d) CardioID

(e) SAPHE (f) IPI (g) BANDANA (h) CardioID

FIGURE 15. Heatmaps of random walks for 32-bit keys (0 → left; 1 → right).



(a) SAPHE (b) IPI (c) BANDANA (d) CardioID

(e) SAPHE (f) IPI (g) BANDANA (h) CardioID

FIGURE 16. Cumulative sums distribution for 32-bit keys (last rows in Figure 15). Expected binomial distribution in red.

V. RANDOMNESS OF THE KEYS

We investigated whether keys generated by CardioID, IPI, BANDANA and SAPHE protocols are *sufficiently unpredictable*, to withstand computationally reasonable attacks from an adversary. We analyze the randomness of keys and present results from the DieHarder suite of statistical tests, as well as from the ENT Pseudorandom Number Sequence Test.

A. BIT DISTRIBUTION

To describe the randomness of keys, we look at every single bit of the key component (4 bits). Figure 14 shows the bits' behavior of keys generated from BCG and ECG signals. Figure 14(a) and 14(b) show that an individual bit is not behaving exactly like a uniformly distributed random variable, but still, the probabilities of bits are roughly around 0.5.

We also compared the randomness of keys generated by different protocols by visualizing the structure of random walks on a Galton board. Plotting a sufficient number of truly random key sequences will eventually show a binomial distribution. Figure 15 shows heatmaps of random walks corresponding to the sequences generated by different approaches (0→ left (−1), 1→ right (+1)). While their spread over the probability space differs, the spread follows the expected distribution in all cases. Based on the last row of each heatmap, Figure 16 depicts the cumulative sum distribution.

Summarizing, SAPHE and CardioID exhibit reasonable randomness, while BANDANA and IPI show biases.

B. STATISTICAL TESTS

To evaluate the schemes against bias in the random keys produced, we ran the DieHarder set of statistical tests. Figure 17 shows the p-values computed from 20 runs of the tests. Note that, for purely random sequences, the p-value distribution resembles a normal distribution with mean around 0.5. For IPI and BANDANA, we notice weaknesses for several tests where the mean significantly deviates from 0.5 and the spread of values is too concentrated around the mean, while SAPHE suffers especially regarding the "count the 1s stream" test (9). CardioID shows no clear bias.

TABLE 3. Frequency of special characters.

max width=

	Encoded sequence
Sequence size	73354
Optimum compression rate	14%
Chi square distribution	112409.32
Arithmetic mean (random=0.5)	0.2825
Monte Carlo Pi value	4
Serial correlation coefficient (uncorrelated=0)	0.000379

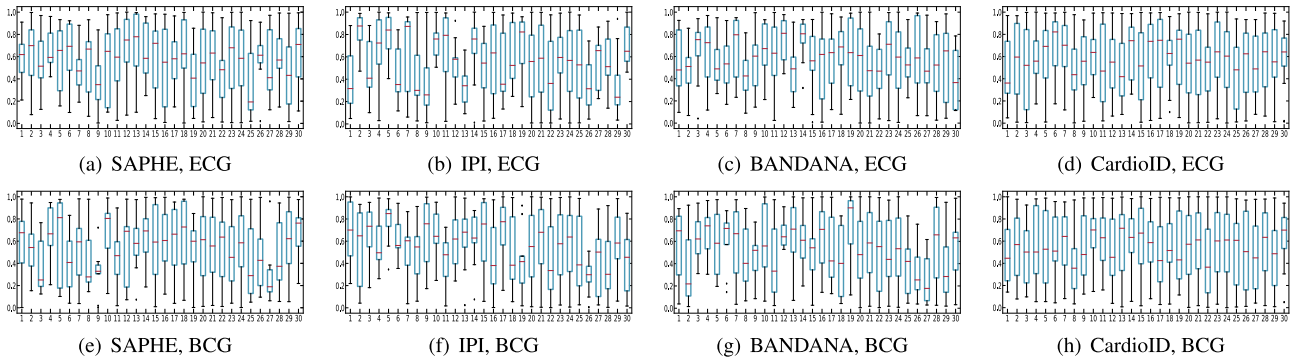
C. PSEUDORANDOM NUMBER TEST

For the sequences generated by CardioID, we further ran the *ENT Pseudorandom Number Sequence Test Program*.[5] It computes the information density of bit sequences, reduction through optimal compression, chi-square distribution, arithmetic mean value of data bytes as well as serial correlation coefficient (shown in Table 3). For instance, a lower compression rate is better and for the serial correlation, values close to 1 or -1 indicate a problem. For the arithmetic mean, a value of 0.5 is desired.

D. ENTROPY ANALYSIS

We extracted more than 4000 key components originating from 20 subjects' BCG and ECG data, and analyzed them for their average Shannon Entropy 18. On average, one person's BCG key components - which are 4 bits long - exhibit a Shannon Entropy of 3.04 bits, outperforming Lin et al.'s

[5]https://www.fourmilab.ch/random/



(a) SAPHE, ECG (b) IPI, ECG (c) BANDANA, ECG (d) CardioID, ECG

(e) SAPHE, BCG (f) IPI, BCG (g) BANDANA, BCG (h) CardioID, BCG

FIGURE 17. Distribution of p-values achieved for keys after 20 runs of the DieHarder set of statistical tests. Tests are: (1) birthdays (2) operm5 (3) rank32 × 32 (4) rank6 × 8 (5) bitstream (6) opso (7) oqso (8) dna (9) count-1s-str (10) count-1s-byt (11) parking (12) 2D circle (13) 3D sphere (14) squeeze (15) runs (16) craps (17) marsaglia (18) sts monobit (19) sts runs (20) sts serial [1-16] (21) rgb bitdistr. [1-12] (22) rgb min dist. [2-5] (23) rgb perm. [2-5] (24) rgb lagged sum [0-32] (25) rgb kstest (26) dab bytedistr. (27) dab dct (28) dab filltree (29) dab filltree 2 (30) dab monobit 2.

approach in a similar setting, with a reported entropy value of 2.9 [32]. This entropy value means that an average 4 bit long BCG key contains the randomness of 3.04 completely random bits. We consider this an acceptable value. In analogy to passwords, even imperfect passwords are fine if they are long enough. By chaining multiple 4 bit sequences, a more robust key can be formed.

VI. CardioID IN A COMMUNICATION PROTOCOL

We envision the key generation from CardioID within a communication protocol for medical devices in a local Body Area Network. Considering trends towards wearable devices and wireless communication between medical devices, this is a realistic scenario. We consider a BCG and ECG-based implicit secure communication protocol, exploring ways to use CardioID's cryptographically robust fingerprints and their 4-bit components. It uses them not just for confidentiality - i.e. encryption - but also as a means to provide data integrity and continuous authentication, leading devices to "unpair" once they are not anymore on the same body, i.e., observing the same BCG or ECG signal [53].

In contrast to similar proposals for such a communication protocol, we do not require asymmetric cryptography to be set up, thus do not require a central trusted authority. This reduces the exposure of any data that was exchanged. In that sense, the protocol is decentral and suitable for the medical domain, where privacy is of great concern.

A. CONFIDENTIALITY

Assume two devices, Bob and Alice. Placed on the same person's body and registering a corresponding signal, e.g., BCG or ECG, Bob uses CardioID to retrieve a cryptographic fingerprint f_b, extracting binary key components from heart-rate variability. Alice is also capable of using CardioID to derive a matching fingerprint f_a. To establish secure communication only with devices co-present on the same body, Bob generates a random challenge (e.g., $12-8$) and concatenates it to a 'Hello' message, encrypted using f_b, and wirelessly broadcast. After receiving Bob's message, Alice decrypts it using f_a, and broadcasts her encrypted 'Hello' concatenated with the solution to Bob's challenge. Alice now uses f_a as a symmetric encryption key for future communication with Bob. Bob receives Alice's message and successfully decrypts it using f_b. Bob verifies that the response from Alice was correct and remembers f_b as a symmetric encryption key.

1) CASE ANALYSIS: BENEFITS FROM CONFIDENTIALITY

The wireless communication between the patient's medical devices and the doctor's reader is shielded against brute-force or dictionary attacks, intended to guess the cryptographic keys that are used, providing security. This is critical, since doctors hold a moral and often legal obligation to protect their patients' medical data from exposure.

In addition, the randomness of the keys prevents the doctor's wrist reader from re-identifying a person. This holds even if the device was to be physically hijacked by a malicious third party. Devices in our scheme are "memory-less", i.e., even if the same patient visits her office multiple times there is no way for the wrist reader to tell, strengthening privacy. A specific ASIC which only allows a device to read random bits in the BCG or ECG signal, thus providing guaranteed privacy even if the device were physically compromised, could be envisioned.

In a situation where a doctor only needs temporary read access to that data, exposure is kept to a minimum.

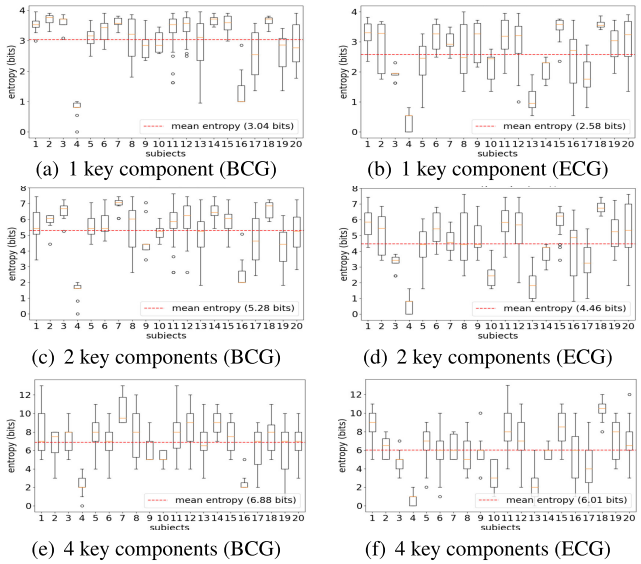
B. INTEGRITY

To prevent data tampering, the protocol further integrates sequence numbers and digital signatures.

Bob concatenates any message *msg* that he sends via the secure channel with a sequence number *seqNr* and signs it with the common secret fingerprint f. The resulting signature s is appended to the message. Knowing f, Alice is able to verify the signature s and discards the message in case the signature is incorrect. Missing messages trigger a resend request, messages with already received *seqNr* are discarded.

1) CASE ANALYSIS: BENEFITS FROM INTEGRITY MEASURES

The protocol's integrity measures shield communication against blind manipulation or replay attacks, since a device



(a) 1 key component (BCG) (b) 1 key component (ECG)
(c) 2 key components (BCG) (d) 2 key components (ECG)
(e) 4 key components (BCG) (f) 4 key components (ECG)

FIGURE 18. BCG and ECG entropy in 4-bit key components.

is able to tell whether a message has been tampered with by verifying that message's digital signature. This includes transmission errors. A doctor may appreciate this, since it lowers the risk of a faulty diagnosis as a result of faulty data.

C. CONTINUOUS AUTHENTICATION

After having established a secure communication channel, Bob and Alice confirm their co-presence at repeated intervals by retrieving and exchanging authentication requests including time-sensitive key components kc_b and kc_a from the body signal. In the case of BCG or ECG signals, these key components correspond to the most recent heart beat. These 4-bit key components are significantly shorter than the fingerprints from CardioID, making continuous authentication energy-efficient.

The communication is closed by either side if kc_b or kc_a can not be confirmed with a sufficiently low error rate.

Building in large part on top of CardioID, the proposed protocol inherits its desirable properties. The randomness in individual fingerprints implies that while at a given point of time, devices on different bodies can be told apart, over time, the devices are not able to identify persons, preserving their privacy by design. In other words, each new session when a device is worn restarts its memory and identification capabilities. The proposed protocol can thus be considered an implicit, robust and secure communication protocol, that is also privacy-preserving, allowing for anonymous usage.

1) CASE ANALYSIS: BENEFITS FROM CONTINUOUS AUTHENTICATION

The continuous authentication mechanism allows the doctor to implicitly switch her wrist reader between patients. When it is moved to a new patient, the change in the BCG or ECG signal is detected, triggering a new pairing attempt with devices that observe the same BCG or ECG signal. This mechanism also serves to avoid gathering faulty data, implicitly cutting communication with devices off once they are perceived not to be on the same body anymore.

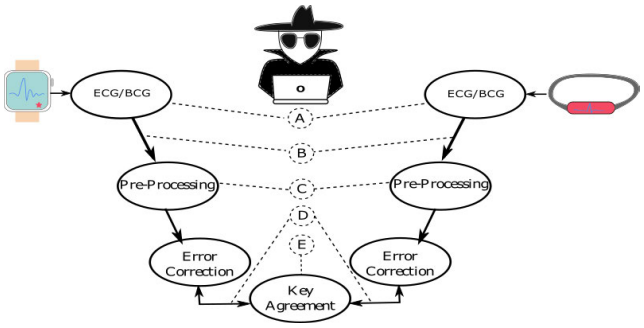


FIGURE 19. Conceptual view of our ECG/BCG-based pairing with attack vectors.

VII. SECURITY ANALYSIS

Figure 19 sketches the conceptual design of our ECG/BCG-based pairing scheme and potential attack vectors, following the conceptual approach proposed in [29] and [55]. Both ECG/BCG devices sample the signal, pre-process the sampled sequence, apply error correction and agree on a key.

Protection against MitM attacks can only be achieved if all parts of the system are resilient. The discussed attacks are associated with the attack vectors A-E in Figure 19. As perfect security does not exist and every system can be broken if only the effort is sufficiently high, we attempt to report feasible attacks for each attack vector. For the classification of the severity of these attacks, we refer to [55] (Section 4: Classifying adversary models), which distinguishes zero effort, minimal effort, advanced effort and guaranteed success cases. Their classification scheme distinguishes these attack cases by the capabilities (C1:user, C2:developer, C3:manufacturer) of the attacker and by her resources (E1:individual, E2:organization, E3:nation state).

A possible attack surface is introduced by the sensors (A), for instance, because an adversary could force incorrect ECG/BCG readings by playing back recorded audio of an ECG at sufficient loudness, as detailed in [56] (C2,E1, advanced effort). Furthermore, data acquisition could be bypassed (B) by an adversary capable of injecting historical data into the device (C2,E2, advanced effort). In addition, a potential bias in the preprocessing (e.g., filtering, fingerprint generation), which had not been identified during protocol design, could allow a naive brute force attack (C) (C2,E1, advanced effort). The protocol also shares the distance δ during the fuzzy cryptography part and before the actual key agreement (cf. section III-D). A vulnerability of fuzzy cryptography, not known as of today, might exploit this to potentially leak information (D) (C2,E3, guaranteed success). Additionally, a key agreement that is weak or based on false assumptions could open the attack windows for an adversary (C2,E2, advanced effort). This is especially the case if the agreement is not based on established standards (E)

(we suggest utilizing a PAKE based protocol). Finally, as for any security protocol, a compromised device poses a significant threat (C3,E2, guaranteed success).

A. IMPACTS OF USING ERROR CORRECTION

In any biometric authentication system, noise of the biometric information is an intrinsic property (here: heart-rate variability extracted from ECG/BCG measurements). Fuzzy cryptography has been proposed to employ error correcting codes to mitigate such noise. Error correcting codes encode messages from a message space $m \in \mathcal{M}$ into codewords of the (larger) codespace $c \in \mathcal{C}$ introducing redundancies. This process allows correcting errors introduced to c by decoding it back to m. In fuzzy cryptography, the biometric information contains noise or errors that can be corrected after mapping into $\mathcal{C}$. The redundancy introduced in the encoding process, however, dictates that an adversary also does not have to guess all bits in the fingerprint correctly, but can be sloppy. For instance, assume a key length of K and an error correcting code able to correct a fraction of u bits from the total fingerprint length N. This means that the success probability of a single randomly drawn fingerprint is not 2^N, but instead only

$$\sum_{k=0}^{u} \binom{N}{k} / 2^N = \frac{\sum_{k=0}^{u} \left(\frac{N!}{(N-k)!\cdot k!} \right)}{2^N} \tag{1}$$

since up to u errors are allowed at an arbitrary position in the fingerprint. Careful choice of the parameters is therefore demanded to limit the advantage gained by an adversary through fuzzy cryptography. For instance, in our case, using BCH codes capable of correcting 8 bits, the actual length of the binary sequence after decoding it into $\mathcal{M}$ is 16 bits.

B. ONE-SHOT SUCCESS PROBABILITY (E)

Without additional knowledge about the victim's ECG or BCG signal, an attacker may decide to exhaust the key space $\mathcal{C}$ of all keys $\boldsymbol{k}$ to execute a MitM or impersonation attack (E).

However, the proposed method is based on the heart rate variability that changes over time. The changes also affect the generated fingerprints as well as the mapping to the code space. For each pairing attempt, a completely new authentication process (new $\boldsymbol{k}$ independent from the previous one) is started. Thus, it is impossible to exhaust $\mathcal{C}$, making this a one-shot attack. For instance, assume a length of 16 bit for $\boldsymbol{k}$ (after error correction (cf. section VII-A)). Note that 16 bits provide sufficient entropy since we suggest implementing a PAKE protocol as in [57], which prevents offline attacks and can thus provide a sufficiently large security margin even with short key lengths K.

C. PRE-PROCESSING-SPECIFIC ATTACKS (C)

An attacker with insight to preprocessing might be able to exploit this knowledge to boost her one-shot success probability. This is especially critical if the preprocessing should be biased. Our analysis of the fingerprints after preprocessing in section V did not reveal any such biases.

D. SPOOFING ATTACK (D)

A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage [58].

As shown in Figure 14(c) and 14(d), the overall distribution of values is fairly even. The best guess among the BCG samples (the most frequent value 5 in figure 14(c)) only has a chance of approximately 9% of being correct. The optimal probability for all values would be 6.25%, corresponding to a uniform distribution amongst 16 values. For a key comprised of, e.g., 32 key components (i.e., 128 bits long), the chance of guessing it using a dictionary-based method would thus be $0.09^{32} < 4 \cdot 10^{-34}$.

Figure 11 shows that although the fingerprint is obtained from BCG or ECG of the same person but at different time, the similarity is around 0.5. Hence, spoofing is not possible.

E. VIDEO CAPTURING PHYSIOLOGICAL STIMULI (E)

Cameras are omnipresent in these days, for instance, as CCTV systems, personal camcorders, or mobile phones, or through remote meetings. The quality of the captured videos is often sufficient to discriminate subtle movements. It has been shown in [59] that it is possible to extract atrial fibrillation from video. Consequently, an adversary with camera-support might therefore be advantaged in extracting instantaneous pairing keys with the help of such recorded video (E). In the best case, impersonation from video might potentially be possible when the adversary would succeed in extracting accurate BCG information from the video with low delay ($<$ 1 sec) since the keys are based on instantaneous heart-rate variability. Such attack would require the capabilities of a developer and involve access to sufficient quality video footage, for instance, through the access of an organization's CCTV installation, or from a remote video meeting with the victim (C2,E2, advanced effort). For this attacking strategy, one potential approach is pulse extraction from the variation of skin tone [60].[6] The hue channel values of pixels in skin regions are filtered through a 3rd-order Butterworth band-pass filter of 0.8-3Hz to retain the frequency range of heartbeats. The resulting signal is in the form of photoplethysmography (PPG) signals, as shown in Figure 20. Another method with a more complicated set-up is imaging-BCG [61], [62]. It uses the Lucas-Kanade tracker to estimate the trajectories of facial features. Based on these trajectories, BCG can be reconstructed. Video-based attacks may reveal heart-related signals, however, are computationally demanding in real-time.

F. SUMMARY OF SECURITY ANALYSIS

CardioID is resilient to the most usual threats of non-targeted (zero effort: e.g., random success or brute-force attacks) or non-sophisticated (minimal effort: e.g. targeted attack from peers with non-developer capabilities) attacks. CardioID is though not able to withstand advanced effort or guaranteed

[6] https://github.com/habom2310/Heart-rate-measurement-using-camera

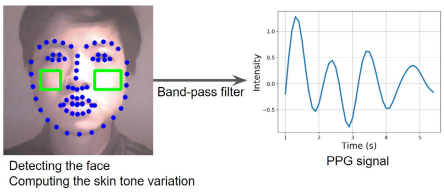


FIGURE 20. Photoplethysmography (PPG) from video.

success level attacks that involve developer, manufacturer, operator or owner capabilities as well as resources available to organizations or nation states. Furthermore, being able to place a malicious sensor on the subjects body unnoticed poses a significant threat against the system. However, this is a property that is shared by all on-body implicit device pairing protocols, such as SAPHE, IPI or BANDANA and in general a trade-off that comes with pairing schemes that do not rely on explicit attention for their key input.

VIII. LIMITATIONS

In contrast to other pairing mechanisms, CardioID requires some seconds to observe the operation of the heart in order to extract a fingerprint and secure key with sufficient entropy. We found that 30 seconds are sufficient.

During our experiments, we noticed that the noise in the acceleration sensing is increasing with body movement. While static states provide sufficient quality measurements, for BCG and ECG signals recorded during movement or at remote positions on the body, it is possible that noise significantly degrades the signal quality.

A further limitation of CardioID is posed by an attacker capable to place a device physically on the body of the victim. In this Trojan horse attack, CardioID provides no protection against the spontaneous pairing with the device of the attacker.

IX. DISCUSSION

We have exploited sequences of peak intervals (**J-J'** and **R-R'** intervals) to compose fingerprints. As described in section III-D, we arrive at ad-hoc pairing keys by applying fuzzy cryptography on these fingerprints.

Alternative encodings may inherit greater robustness and we propose a specific BCG encoding. The construction of a matching ECG encoding is straightforward.

The features include two types: time interval and the amplitude distance. Based on previous research, the effective time interval features extracted from BCG are shown in Figure 2, Table 4. The proposed features (amplitude distance) are shown in Table 5.

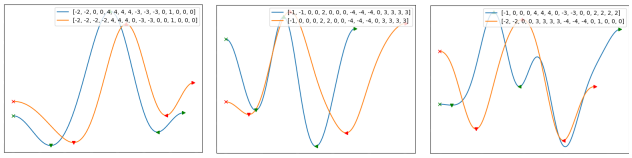
We propose to employ the shape of the BCG signal. Each sub-curve is represented by 4 digits, so that a heartbeat described by 4 sub-curves is encoded into 16 digits out of *[-4, -3, -2, -1, 1, 2, 3, 4]*. First, we sort amplitude distance features. The largest absolute amplitude distance value is assigned "4" or "-4"; the smallest is assigned "1" or "-1". If the sampled value is smaller than zero, a negative sign will be assigned to the subcurve, otherwise a positive.

TABLE 4. Time interval features from detected key points.

Extracted Time Interval Features		
1. $\lvert X_H - X_I \rvert$	2. $\lvert X_I - X_J \rvert$	3. $\lvert X_J - X_K \rvert$
4. $\lvert X_K - X_L \rvert$	5. $\lvert X_H - X_J \rvert$	6. $\lvert X_I - X_K \rvert$
7. $\lvert X_J - X_L \rvert$	8. $\lvert X_H - X_L \rvert$	9. $\lvert X_J - X'_J \rvert$

TABLE 5. Amplitude features from detected key points.

Extracted Amplitude Distance Features	
1. $Y_H - Y_I$	2. $Y_I - Y_J$
3. $Y_J - Y_K$	4. $Y_K - Y_L$



(a) Similarity: 0.75 (b) Similarity: 0.875 (c) Similarity: 0.1875

FIGURE 21. Examples of heartbeat encoding results. The signal shapes in (a) and (b) are similar, resulting in a higher similarity score. In (c), the different shapes result in lower similarity.

For example, in Figure 2, the subcurve **JK** will be encoded by "4".

The absolute value of the time interval determines how often an encoded value is repeated (0 to 3). For example, as shown in Figure 2, the smallest absolute time interval is $|X_J - X_K|$. Therefore, this value ('4') will repeat 0 times. The curve **JK** will therefore be represented by *[4, 0, 0, 0]*.

Non-zero values represent amplitude distance features while the repetition count represents the time interval.

Iterating the previous steps for every sub-curve, the heartbeat will be encoded into a sequence with 16 digits out of *[-4, -3, -2, -1, 1, 2, 3, 4]*.

We test our coding approach on BCG data from 16 healthy subjects in a resting position. Given two encoding sequences, the similarity is computed by:

$$similarity = \frac{\#\text{ of identical encodings}}{\#\text{ of all encodings}} \tag{2}$$

Example encodings are shown in Figures 21(a), 21(b) and 21(c). In the former two figures, the heartbeat extracted from the BCG data looks similar and the encoding accuracy is higher than 0.7. Figure 21(c) exemplifies a negative example in which heartbeat shapes differ, which results in a low similarity score.

X. CONCLUSION

In this paper, we proposed CardioID, a secure device pairing method based on ECG and BCG data, and evaluated the performance of CardioID based on the similarity score. We compared CardioID with other quantization schemes, including IPI, BANDANA and SAPHE on both laboratory data and data from noisy measurements. The results show that CardioID clearly outperforms the state-of-the-art implicit secure pairing schemes for cardiograph data. In terms of security, we discuss a secure communication system based on CardioID and potential attacks on it. We introduce improved fingerprints from ECG and BCG, which encodes the heartbeat with both time interval and amplitude distance.

In our future work, we will first focus on the quality extraction of heartbeat from the BCG data. We will try to filter the BCG data from different subjects differently, based on the data itself. Besides, more features will be added for encoding heartbeat. Currently, we only used the heart-rate variability, time interval and amplitude distance from the peak points of heartbeat. There are still other statistical features and features in frequency domain. These information also contributes to the uniqueness of heartbeat.

REFERENCES

[1] S. Eberz, G. Lovisotto, A. Patané, M. Kwiatkowska, V. Lenders, and I. Martinovic, "When your fitness tracker betrays you: Quantifying the predictability of biometric features across contexts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 889–905.

[2] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[3] A. Bruesch, L. Nguyen, D. Schürmann, S. Sigg, and L. C. Wolf, "Security properties of gait for mobile device pairing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 3, pp. 697–710, Mar. 2019.

[4] A. M. Katz, *Physiology of the Heart*, 5th ed. Philadelphia, PA, USA: Wolters Kluwer Health, 2011.

[5] L. Giovangrandi, O. T. Inan, R. M. Wiard, M. Etemadi, and G. T. A. Kovacs, "Ballistocardiography—A method worth revisiting," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2011, pp. 4279–4282.

[6] M. Manikandan and S. Kp, "A novel method for detecting R-peaks in electrocardiogram (ECG) signal," *Biomed. Signal Process. Control*, vol. 7, no. 2, pp. 118–128, Mar. 2012.

[7] N. Jähne-Raden, M. Marschollek, U. Kulau, and L. Wolf, "Heartbeat the odds: A novel digital ballistocardiographic sensor system," in *Proc. 15th ACM Conf. Embedded Netw. Sensor Syst.*, Nov. 2017, p. 59.

[8] K. Pandia, S. Ravindran, R. Cole, G. Kovacs, and L. Giovangrandi, "Motion artifact cancellation to obtain heart sounds from a single chest-worn accelerometer," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2010, pp. 590–593.

[9] W. Liu and Y. Ren, "A modified approach of peak extraction from BCG for heart rate estimation," *IOP Conf. Earth Environ. Sci.*, vol. 252, no. 4, Jul. 2019, Art. no. 042086.

[10] P. Bjerregaard and I. Gussak, "Naming of the waves in the ECG with a brief account of their genesis," *Circulation*, vol. 100, no. 25, p. e148, Dec. 1999.

[11] N. Reljin, J. Lazaro, M. B. Hossain, Y. S. Noh, C. H. Cho, and K. H. Chon, "Using the redundant convolutional encoder–decoder to denoise QRS complexes in ECG signals recorded with an armband wearable device," *Sensors*, vol. 20, no. 16, p. 4611, Aug. 2020.

[12] V. Gupta and M. Mittal, "A novel method of cardiac arrhythmia detection in electrocardiogram signal," *Int. J. Med. Eng. Informat.*, vol. 12, no. 5, p. 489, 2020.

[13] R. Gonzalez-Landaeta, O. Casas, and R. Pallas-Areny, "Heart rate detection from an electronic weighing scale," in *Proc. 29th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2007, pp. 6282–6285.

[14] Y. Zhu, H. Zhang, M. Jayachandran, A. K. Ng, J. Biswas, and Z. Chen, "BCG with fiber optic sensor in headrest position: A feasibility study and a new processing algorithm," in *Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2013, pp. 5203–5206.

[15] D. D. He, E. S. Winokur, and C. G. Sodini, "An ear-worn continuous ballistocardiogram (BCG) sensor for cardiovascular monitoring," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2012, pp. 5030–5033.

[16] J. Alametsä, A. Värri, J. Viik, J. Hyttinen, and A. Palomäki, "Ballistocardiogaphic studies with acceleration and electromechanical film sensors," *Med. Eng. Phys.*, vol. 31, no. 9, pp. 1154–1165, Nov. 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1350453309001581

[17] R. C.-W. Phan and P. Mingard, "Analyzing the secure simple pairing in Bluetooth v4.0," *Wireless Pers. Commun.*, vol. 64, no. 4, pp. 719–737, Jun. 2012.

[18] R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Comput.*, vol. 8, no. 6, pp. 792–806, Jun. 2009.

[19] D. Bichler, G. Stromberg, M. Huemer, and M. Löw, "Key generation based on acceleration data of shaking processes," in *Proc. Int. Conf. Ubiquitous Comput.* Innsbruck, Austria: Springer, 2007, pp. 304–317.

[20] B. Groza and R. Mayrhofer, "SAPHE: Simple accelerometer based wireless pairing with heuristic trees," in *Proc. 10th Int. Conf. Adv. Mobile Comput. Multimedia (MoMM)*, 2012, pp. 161–168.

[21] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma, and J. Ma, "Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist worn devices," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5618–5630, Jun. 2019.

[22] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 358–370, Feb. 2013.

[23] J. Wu and J. Shang, "AudioKey: A usable device pairing system using audio signals on smartwatches," *Int. J. Secur. Netw.*, vol. 15, no. 1, p. 46, Jan. 2020.

[24] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, "MagPairing: Pairing smartphones in close proximity using magnetometers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1306–1320, Jun. 2016.

[25] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst., Appl., Services*, 2011, pp. 211–224.

[26] A. Srivastava, J. Gummeson, M. Baker, and K.-H. Kim, "Step-by-step detection of personally collocated mobile devices," in *Proc. 16th Int. Workshop Mobile Comput. Syst. Appl.*, Feb. 2015, pp. 93–98.

[27] E. A. Heinz, K. S. Kunze, S. Sulistyo, H. Junker, P. Lukowicz, and G. Tröster, "Experimental evaluation of variations in primary features used for accelerometric context recognition," in *Proc. Eur. Symp. Ambient Intell.* Veldhoven, The Netherlands: Springer, 2003, pp. 252–263.

[28] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proc. Int. Conf. Adv. Mobile Comput. Multimedia (MoMM)*, 2013, p. 293.

[29] J. Lester, B. Hannaford, and G. Borriello, "Are you with me?—Using accelerometers to determine if two devices are carried by the same person," in *Pervasive Computing*. Vienna, Austria: Springer, 2004, pp. 33–50.

[30] C. Cornelius and D. Kotz, "Recognizing whether sensors are on the same body," in *Pervasive*. Berlin, German: Springer-Verlag, 2011, pp. 332–349.

[31] R. D. Findling, M. Muaaz, D. Hintze, and R. Mayrhofer, "ShakeUnlock: Securely transfer authentication states between mobile devices," *IEEE Trans. Mobile Comput.*, vol. 16, no. 4, pp. 1163–1175, Apr. 2017.

[32] Q. Lin, W. Xu, J. Liu, A. Khamis, W. Hu, M. Hassan, and A. Seneviratne, "H2B: heartbeat-based secret key generation using piezo vibration sensors," in *Proc. 18th Int. Conf. Inf. Process. Sensor Netw.*, Apr. 2019, pp. 265–276.

[33] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 1099–1112.

[34] M. Di Rienzo, E. Vaini, P. Castiglioni, G. Merati, P. Meriggi, G. Parati, A. Faini, and F. Rizzo, "Wearable seismocardiography: Towards a beat-by-beat assessment of cardiac mechanics in ambulant subjects," *Autonomic Neurosci.*, vol. 178, nos. 1–2, pp. 50–59, Nov. 2013.

[35] K. Sørensen, S. E. Schmidt, A. S. Jensen, P. Søgaard, and J. J. Struijk, "Definition of fiducial points in the normal seismocardiogram," *Sci. Rep.*, vol. 8, no. 1, Dec. 2018.

[36] M. Dyrholm, R. Goldman, P. Sajda, and T. R. Brown, "Removal of BCG artifacts using a non-kirchhoffian overcomplete representation," *IEEE Trans. Biomed. Eng.*, vol. 56, no. 2, pp. 200–204, Feb. 2009.

[37] J. Gomez-Clapers, R. Casanella, and R. Pallas-Areny, "A novel algorithm for fast BCG cycle extraction in ambulatory scenarios," in *Proc. Comput. Cardiol. Conf. (CinC)*, Sep. 2016, pp. 357–360.

[38] N. Nguyen, S. Sigg, A. Huynh, and Y. Ji, "Pattern-based alignment of audio data for ad hoc secure device pairing," in *Proc. 16th Int. Symp. Wearable Comput.*, Jun. 2012, pp. 88–91.

[39] D. J. Berndt and J. Clifford, "Using dynamic time warping to find patterns in time series," in *Proc. 3rd Int. Conf. Knowl. Discovery Data Mining*, 1994, pp. 359–370.

[40] P. de Chazal, M. O'Dwyer, and R. B. Reilly, "Automatic classification of heartbeats using ECG morphology and heartbeat interval features," *IEEE Trans. Biomed. Eng.*, vol. 51, no. 7, pp. 1196–1206, Jul. 2004.

[41] Y. Sun, K. L. Chan, and S. M. Krishnan, "Characteristic wave detection in ECG signal using morphological transform," *BMC Cardiovascular Disorders*, vol. 5, p. 28, Sep. 2005.

[42] G. D. Clifford, F. Azuaje, and P. McSharry, *Advanced Methods and Tools for ECG Data Analysis*. Norwood, MA, USA: Artech House, 2006.

[43] M. Etemadi, O. Inan, L. Giovangrandi, and G. Kovacs, "Rapid assessment of cardiac contractility on a home bathroom scale," *IEEE Trans. Inf. Technol. Biomed.*, vol. 15, no. 6, pp. 864–869, Nov. 2011.
[44] J. Paalasmaa, H. Toivonen, and M. Partinen, "Adaptive heartbeat modeling for beat-to-beat heart rate measurement in ballistocardiograms," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 6, pp. 1945–1952, Nov. 2015.
[45] F. R. Hampel, "The influence curve and its role in robust estimation," *J. Amer. Statist. Assoc.*, vol. 69, no. 346, pp. 383–393, 1974.
[46] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Trans. Biomed. Eng.*, vols. BME–32, no. 3, pp. 230–236, Mar. 1985.
[47] S. Vaudenay, "Secure communications over insecure channels based on short authenticated strings," in *Proc. Annu. Int. Cryptol. Conf.* CA, USA: Springer, 2005, pp. 309–326.
[48] J. Suomalainen, J. Valkonen, and N. Asokan, "Security associations in personal networks: A comparative analysis," in *Proc. Eur. Workshop Secur. Ad-Hoc Sensor Netw.* Cambridge, U.K.: Springer, 2007, pp. 43–57.
[49] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, *Internet Key Exchange Protocol Version 2 (IKEV2)*, document RFC 5996, Sep. 2010.
[50] P. Zimmermann, A. Johnston, and J. Callas, "ZRTP: Media path key agreement for unicast secure RTP," RFC 6189, 2011, pp. 1–115.
[51] M. Toorani, "Security analysis of J-PAKE," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2014, pp. 1–6.
[52] Y. Sun, C. Wong, G.-Z. Yang, and B. Lo, "Secure key generation using gait features for body sensor networks," in *Proc. IEEE 14th Int. Conf. Wearable Implant. Body Sensor Netw. (BSN)*, May 2017, pp. 206–210.
[53] N. Beck, S. Zuo, and S. Sigg, "BCG and ECG-based secure communication for medical devices in body area networks," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops other Affiliated Events (PerCom Workshops)*, Mar. 2021, pp. 207–212.
[54] R. M. Bolle, J. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. NY, USA: Springer, 2013.
[55] R. Mayrhofer, V. Mohan, and S. Sigg, "Adversary models for mobile device authentication," 2020, *arXiv:2009.10150*.
[56] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané, "Broken hearted: How to attack ECG biometrics," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–15.
[57] D. Schürmann, A. Brüsch, N. Nguyen, S. Sigg, and L. Wolf, "Moves like jagger: Exploiting variations in instantaneous gait for spontaneous device pairing," *Pervas. Mobile Comput.*, vol. 47, pp. 1–12, Jul. 2018.
[58] K. Jindal, S. Dalal, and K. K. Sharma, "Analyzing spoofing attacks in wireless networks," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Technol.*, Feb. 2014, pp. 398–402.
[59] J.-P. Couderc, S. Kyal, L. K. Mestha, B. Xu, D. R. Peterson, X. Xia, and B. Hall, "Detection of atrial fibrillation using contactless facial video monitoring," *Heart Rhythm*, vol. 12, no. 1, pp. 195–201, 2015.
[60] W. Verkruysse, L. O. Svaasand, and J. S. Nelson, "Remote plethysmographic imaging using ambient light," *Opt. Exp.*, vol. 16, no. 26, p. 21434, 2008.
[61] G. Balakrishnan, F. Durand, and J. Guttag, "Detecting pulse from head motions in video," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2013, pp. 3430–3437.
[62] D. Shao, F. Tsow, C. Liu, Y. Yang, and N. Tao, "Simultaneous monitoring of ballistocardiogram and photoplethysmogram using a camera," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 5, pp. 1003–1010, May 2017.

SI ZUO received the M.Sc. degree from the Department of Communications and Networking, Aalto University, where she is currently pursuing the Ph.D. degree with the Department of Communications and Networking. Her research interests include the analysis of healthcare and bioinformatic data with machine learning methods to improve usable security.

STEPHAN SIGG received the Ph.D. (Dr. rer. nat.) degree from the University of Kassel, Germany, in 2008. He is currently an Associate Professor at the Department of Communications and Networking, Aalto University. He was with the Chair of Communication Technology (ComTec), University of Kassel, from 2005 to 2007. His research interests include the design, analysis, and optimization of (randomized) algorithms in mobile and pervasive computing domains, in particular focusing on (wireless) networking and security.

LE NGU NGUYEN received the Doctor of Science (Technology) degree from the Department of Communications and Networking (ComNet), Aalto University, Finland. He is currently a Postdoctoral Researcher at the Center for Machine Vision and Signal Analysis (CMVS), University of Oulu, Finland. His research interests include usable security (e.g., audio-based device pairing and image-based user authentication) and machine learning applications in pervasive computing (e.g., sport activity analysis and radar-based sensing).

NILS BECK is currently pursuing the master's degree in computational linguistics with the University of Stuttgart, Germany. He joined the Ambient Intelligence Group, Aalto University, for a research internship.

NICO JÄHNE-RADEN received the master's degree in biomedical informatics from Technische Universität Braunschweig. He is currently a Research Associate at the Peter L. Reichertz Institute for Medical Informatics, TU Braunschweig and Hannover Medical School, Germany. His research interests include medical signal processing and analyzing (e.g., ballistocardiography).

MARIE CATHRINE WOLF is currently a Research Associate at the Peter L. Reichertz Institute for Medical Informatics, TU Braunschweig and Hannover Medical School, Germany. Her research interests include the processing and analysis of medical signals.