# Enhancing Heart-Beat-Based Security for mHealth Applications

Robert M. Seepers, Christos Strydis, Ioannis Sourdis, and Chris I. De Zeeuw

***Abstract*—In heart-beat-based security, a security key is derived from the time difference between consecutive heart beats (the inter-pulse interval, IPI), which may, subsequently, be used to enable secure communication. While heart-beat-based security holds promise in mobile health (mHealth) applications, there currently exists no work that provides a detailed characterization of the delivered security in a real system. In this paper, we evaluate the strength of IPI-based security keys in the context of entity authentication. We investigate several aspects that should be considered in practice, including subjects with reduced heart-rate variability (HRV), different sensor-sampling frequencies, intersensor variability (i.e., how accurate each entity may measure heart beats) as well as average and worst-case-authentication time. Contrary to the current state of the art, our evaluation demonstrates that authentication using multiple, less-entropic keys may actually increase the key strength by reducing the effects of intersensor variability. Moreover, we find that the maximal key strength of a 60-bit key varies between 29.2 bits and only 5.7 bits, depending on the subject's HRV. To improve security, we introduce the inter-multi-pulse interval (ImPI), a novel method of extracting entropy from the heart by considering the time difference between nonconsecutive heart beats. Given the same authentication time, using the ImPI for key generation increases key strength by up to 3.4× (+19.2 bits) for subjects with limited HRV, at the cost of an extended key-generation time of 4.8× (+45 s).**

***Index Terms*—Authentication, Biometrics, Body area networks, Telemedicine.**

## I. Introduction

MOBILE-HEALTH (mHealth) is an emerging technology that allows for continuous, remote health care through the use of mobile devices. Body-area networks (BANs) may provide continuous patient monitoring through the use of cheap, wearable biosensors [1]. Modern implantable medical devices (IMDs) feature wireless capabilities to allow remote configuration without requiring invasive surgery or data-log broadcasting from a home-monitoring station [2]. Due to the wireless nature of mHealth solutions and the sensitivity of the data transmitted, security has shown to be an important aspect of mHealth. Non-secure communication may allow an adversary to steal private patient data or, worse, alter device parameters or even prevent treatment [1], [3].

The inter-pulse interval (IPI) of heart beats has recently been proposed for securing both wireless IMDs and BANs [4]–[6]. In heart-beat-based security (HBBS), each sensor measures a heart-related biosignal, for example, cardiac activity using an electrocardiogram (ECG) or blood flow, and forms a biometric security key based on the time interval between consecutive heart beats. Previous work has shown that this interval may contain a significant degree of entropy, while it may be measured with some consistency and in different locations of a patient's body. These two characteristics allow IPIs to be used for shared-secret generation between two entities simultaneously sampling the same heart beat, thus forming the basis for security aspects such as key agreement [7], BAN-device pairing [6], [8], [9], or IMD (-emergency) authentication [4], [5].

While HBBS shows potential for mHealth applications, it is not yet clear how much security the IPI may provide in practice. The statistical properties of IPIs are not yet fully understood [10] and most related works have not considered subjects with significantly limited heart-rate variability (HRV) [5], [6], [8], [11], [12]. In addition, the effect of intersensor variability ($VAR_{is}$), i.e., the disparity between heart-beat measurements between two entities, has either been neglected [13] or has not been studied in sufficient detail [10]. A more profound understanding of how these properties affect the security of IPI-based keys could lead to new, more efficient key-generation methods.

In this paper, we evaluate the security performance of heart-beat-based security in the context of entity authentication. Specifically, this paper contributes the following.

1) A thorough characterization of the strength of IPI-based keys, investigating several aspects that may occur in practice. Specifically, we consider: *1)* subjects with various degrees of HRV; *2)* different sensor sampling frequencies; *3)* realistic $VAR_{is}$ based on measurements obtained from ECG and blood-pressure recordings; and *4)* average and worst-case authentication time.
2) The first work that considers the use of entropy extraction in HBBS, using a novel method of extraction through the inter-multi-pulse interval (ImPI). The ImPI considers the time difference between nonconsecutive heart beats, resulting in an unprecedented increase in key strength at the cost of an extended key-generation time.

Manuscript received August 31, 2015; accepted October 14, 2015. Date of publication October 29, 2015; date of current version January 31, 2017. This work was supported by the EU-funded projects DeSyRe under Grant 287611 and SHARCS under Grant 644571.

R. M. Seepers, C. Strydis, and C. I. De Zeeuw are with the Department of Neuroscience, Erasmus Medical Center 3015, CE, Rotterdam, The Netherlands (e-mail: r.seepers@erasmusmc.nl; c.strydis@erasmusmc.nl; c.dezeeuw@erasmusmc.nl).

I. Sourdis is with the Department of Computer Science & Engineering, Chalmers University of Technology, 412 58, Gothenburg, Sweden (e-mail: sourdis@chalmers.se).

Digital Object Identifier 10.1109/JBHI.2015.2496151

This paper is structured as follows: First, we briefly discuss why HBBS is a suitable biometric for mHealth applications, along with related works, in Section II. In Section III, we describe the existing and improved method of generating keys in HBBS using the IPI and ImPI, respectively. These key generators are subsequently evaluated in Section IV, after that concluding remarks are given in Section V.

## II. Background and Related Work

In this section, we first compare HBBS to other biometrics qualitatively, after which we discuss works related to its security performance. HBBS is a form of cardiovascular biometrics, which use the characteristics of a person's cardiac cycle for entity authentication. Cardiovascular biometrics are typically based on an ECG, using either a combination of various fiducial features (e.g., "ST-slope" or "ST-interval") or nonfiducial features, for example, the autocorrelation between heartbeat records [14]–[16]. Conventionally, a good biometric is one that is easily measured for the general population (universality, measurability, performance), characterizes an individual well (uniqueness), is invariant over time (permanence) and is accepted by the relevant population (acceptability) [17]. HBBS differs from other cardiovascular biometrics in that it uses only a single fiducial feature, that is, the IPI (also denoted as the "RR-interval") between heart beats. This makes it a suitable candidate for many mHealth applications as [6]

1) heart beats are measurable throughout the body using many types of cardiovascular recordings, including ECG, blood pressure (BP), and photoplethysmography (PPG). As such, it may be measured through a wide spectrum of sensors and locations (more universally than other cardiovascular biometrics), which is common in, for example, a BAN;
2) heart beats ("R-peaks") are arguably the most distinct feature in any cardiovascular recording, permitting low-cost peak detection and key generation; and
3) cardiac function is one of the most commonly measured values in mHealth. As a result, many systems will already have the required sensors and peak detectors in place, allowing HBBS to be included at minimal overhead.

The downside of HBBS is that the IPI is a random (time variant) feature, which compares infavorably to other biometrics in terms of permanence [6]. However, its universality and low-cost detection permit all involved entities to generate a fresh, random key for each communication session, increasing security while bypassing several issues related to permanence, such as template outdating [18].

The key strength of an HBBS system depends on both the randomness of the generated keys and the interkey disparity allowed for a true-key pair, as will be discussed in Section IV. Accordingly, here we first discuss relevant studies on the IPI-entropy (key randomness), after that we review a number of related works on the interkey disparity. The entropy per IPI stems from the HRV, a physiological phenomenon caused by the balancing action between the parasympathetic and sympathetic nervous systems [19], [20]. HRV is known to be reduced when either of these nervous systems dominates the other and is affected by, among others, smoking, age, gender, diabetes, brain damage, cardiovascular disorders (CVDs), mental state, and perhaps most substantially, exercise [19]–[22].

Despite the available knowledge on HRV, only a few works have evaluated the entropy per IPI in the context of security (in bits), considering healthy subjects, hypertensive subjects as well as CVD patients [5], [12], [13], all of which conclude that four highly entropic bits are available per IPI. In addition, a recent, preliminary study has considered the effect of exercise on IPI-entropy, showing that subjects during exercise may lose up to 75% of their entropy compared to subjects at rest [4]. In this study, we build upon the work presented in [4] and [12] to provide a more thorough evaluation on the entropy per IPI, considering both subjects with various degrees of HRV and different sensor sampling frequencies.

In an attempt to increase the entropy obtained from IPIs, Bao *et al.* [8] have proposed using the multi-inter-pulse interval (*m*IPI) for key generation, where $m\text{IPI}_{(i,j)}$ is the accumulation of all IPIs previously considered for key generation, i.e., $m\text{IPI}_{(i,j)} = \sum_{i=1}^{j-1} \text{IPI}_{(i,i+1)}; j > i$. While our own experiments confirm the *apparent* increase in entropy per $m$IPI, we note that it does *not* enhance security. The *m*IPI attempts to increase randomness using a simple addition and, as famously stated by John von Neumann, "any one who considers arithmetical methods to produce random digits is, of course, in a state of sin" [23]. In this paper, we present the ImPI that, contrary to the *m*IPI, does *not* reuse its entropic source and *does* allow for an increase in key strength, albeit at the cost of extended key-generation time. To the best of our knowledge, our work is the first to successfully apply entropy extraction in HBBS.

The interkey disparity allowed for a true-key pair (Hamming-distance threshold, $T_{\text{HD}}$) is determined by the (expected) $\text{VAR}_{\text{is}}$ in an mHealth system. While all studies agree that $\text{VAR}_{\text{is}}$ results in a reduction of security performance, the characteristics of such variability are not fully understood, partially due to the different methodologies followed [10]. Poon *et al.* [6] and Bao *et al.* [8] have modeled the $\text{VAR}_{\text{is}}$ as the difference between an ECG and PPG, showing a significant disparity between generated keys (a 2.06% false-rejection rate has been described for a 128-bit key using $T_{\text{HD}} = 48$). Another study has shown a similar disparity (describing a best-case $T_{\text{HD}} = 16$ bits for a 60-bit key) by considering $\text{VAR}_{\text{is}}$ as the difference between ECG and blood-pressure recordings [12]. Other works have either overlooked the $\text{VAR}_{\text{is}}$ [13] or have modeled it as two different leads of the same ECG [5], [11], both of which cannot be considered realistic for typical mHealth applications. In this study, we use an $\text{VAR}_{\text{is}}$ model described in [12], which considers multiple biosignals (ECG and blood pressure) measured at different locations of the same body. We consider such a model representative for typical mHealth applications, as it is likely that two different entities, for example, in a BAN, will have access to different biosignals and will be recorded from different locations. We demonstrate how the $\text{VAR}_{\text{is}}$ affects the security strength considering various parameters, including the bits selected per IPI, the (average) heart rate of a subject, multikey authentication, sensor-sampling frequency and the average and worst-case authentication time.

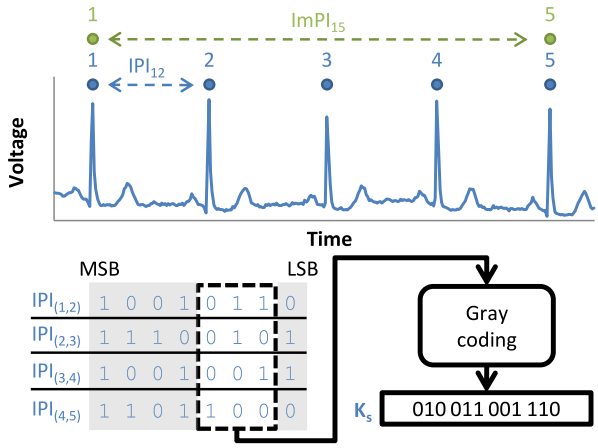


Fig. 1. Key generation using the I(m)PI.

## III. Inter-(multi)-Pulse Interval

In this section, we describe the most commonly used method for facilitating entity authentication in HBBS based on the IPI, after which we present our improved method using the ImPI.

Entity authentication in HBBS comprises two steps: security-key generation by two entities and entity-authentication, if these keys are similar enough. Fig. 1 illustrates the method of security-key generation using the IPI [4]–[6], [12], [13]. First, each entity detects a number of heart beats from their cardiac biosignals and calculates the time interval (IPI, in this study considered as an 8-bit value) between consecutive heart beats, i.e., $\text{IPI}_{(i,i+1)} = \text{beat}_{i+1} - \text{beat}_i$. From each IPI, a predefined set of bits $m$ is selected (the key-bit selection, containing $n_m$ bits per IPI) to form a key segment: The most-significant IPI bits are commonly discarded due to their inherent low entropy, while the least-significant IPI bits may be discarded due to a high $\text{VAR}_{\text{is}}$.[11] Gray coding is applied to the key segment in order to strengthen it against $\text{VAR}_{\text{is}}$ (reducing the number of bits affected by a disparity between IPIs), after which $n$ key segments are concatenated to form security key $k$. Entity authentication is successful if the generated keys are similar enough (not identical, as some disparity may be expected for a given true-key pair due to $\text{VAR}_{\text{is}}$). This similarity is commonly assessed by comparing the Hamming distance between the keys to a predefined threshold ($hd(k_1 \oplus k_2) < T_{\text{HD}}$, where $hd(x)$ represents the number of nonzero values in x and $T_{\text{HD}}$ denotes the Hamming-distance threshold).

It will be shown in our evaluation in Section IV-B that the strength of IPI-based keys is in part limited by the low entropy of the most-significant IPI-bits due to correlations between consecutive heart beats. We strive to increase the key strength by replacing the IPI with the ImPI in the key-generation process, where we define the ImPI as the time difference considering $j$ consecutive heart beats, i.e., $\text{ImPI}_{(j\cdot(i-1)+1,j\cdot i+1)} = \text{beat}_{j\cdot i+1} - \text{beat}_{j\cdot(i-1)+1}$. The ImPI is illustrated for $j = 4$ ($\text{ImPI}_{(1,5)}$) in Fig. 1. Note that the ImPI is equivalent to the IPI for $j = 1$. By increasing $j$, we limit the effect of inter-IPI correlations as individual, consecutive heart beats are ignored for key generation, resulting in an increase in entropy per ImPI. The true-key-pair disparity, however, depends on the accuracy at which each entity may detect each heart beat in IPI/ImPI generation. As both the IPI and ImPI are calculated based on two heart beats, this disparity remains unaffected. Accordingly, it may be expected (and shown in subsequent sections) that using the ImPI allows for an increase in key strength, albeit at an increased key-generation time (as more heart beats are required to obtain an ImPI).

[1]Assuming precise and nondrifting sensors, $\text{VAR}_{\text{is}}$ is the variance between two different sensor measurements of cardiac biosignals, caused by the variable pulse-transition time of ventricular contraction (heart beats) to the rest of the body due to, for example, motion and pressure differences.

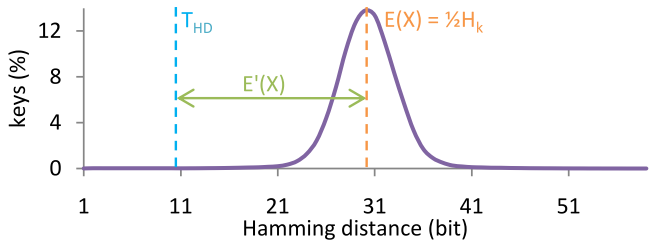


Fig. 2. Key strength $\text{KS}_{\text{eff}}$ as a function of $H_k$ and $T_{\text{HD}}$.

## IV. Evaluation

In this section, we evaluate the performance of the IPI and ImPI-based key generators, considering the key entropy, true-key-pair disparity, and authentication time. First, we introduce our experimental setup in Section IV-A, after that our evaluation follows in Section IV-B.

### A. Experimental Setup

To evaluate the performance of IPI- and ImPI-based key generators, we first introduce the effective key strength $\text{KS}_{\text{eff}}$ as a figure of merit. Using $\text{KS}_{\text{eff}}$, we may quantify the security performance as a function of the key entropy $H_k$ and the required Hamming-distance threshold $T_{\text{HD}}$ for a given true-key pair. Afterwards, we present the datasets considered in our evaluation.

*1) Key Strength:* The strength of a key is determined by the effort required by an attacker to guess it. To quantify the key strength in bits, we define the effective key strength $\text{KS}_{\text{eff}}$ as the number of *entropic bits* that should be known to an attacker in order to successfully authenticate to the IMD with probability $P_{\text{auth}} = 0.5$ [12]. That is, an attacker would have to mount on average $2^{\text{KS}_{\text{eff}}}$ attacks. To exemplify, in Fig. 2, we plot a distribution of Hamming distances between an authentication key and various randomly selected attacker keys. This distribution $\boldsymbol{X}$ ($x$ being the number of mismatched bits in an $n$-bit key) is expectedly binomial with an average number of mismatches $E(X) = p_0 \cdot H_k = p_1 \cdot H_k = \frac{H_k}{2}$, where $p_0$ and $p_1$ denote the probability of a bit being zero or one (for entropic bits, $p_0 = p_1 = \frac{1}{2}$) and $H_k$ denotes the number of entropic bits in the key (ideally, $H_k = \text{n}$). Since, on average, half the number of entropic bits are mismatched by simply guessing, for successful authentication, an attacker would need to try up to

$$\text{KS} = 2 \cdot E(X) - 1 = H_k - 1 \text{ bits}$$

the "$-1$" term accounting for $P_{\text{auth}} = 0.5$.

As it is unlikely that keys will be a perfect match due to $\text{VAR}_{\text{is}}$, we allow entities to authenticate if their keys differ no more than $T_{\text{HD}}$ bits, where $T_{\text{HD}}$ denotes the Hamming-distance threshold. As a result, the average number of mismatched bits will be effectively reduced by the amount of "don't care" $T_{\text{HD}}$ bits; essentially changing $E(X)$ to $E'(X) = \frac{H_k}{2} - T_{\text{HD}}$ (see Fig. 2). In this more general case, $\text{KS}_{\text{eff}}$ is calculated as follows:

$$\begin{aligned} \text{KS}_{\text{eff}} &= 2 \cdot E'(X) - 1 \\ &= H_k - 2 \cdot T_{\text{HD}} - 1 \quad \text{bits.} \end{aligned} \tag{1}$$

Note that $\text{KS}_{\text{eff}}$ may now assume negative values, signifying that an attacker would require less than one attack on average to guess the key ($2^{\text{KS}_{\text{eff}}} < 1$). Obviously, a negative $\text{KS}_{\text{eff}}$ will never exist in practice as an attacker would always require at least one attack, i.e., $\text{KS}_{\text{eff}}$ would be greater or equal to zero. Nevertheless, considering $\text{KS}_{\text{eff}}$ as a potentially negative value will allow us to investigate exactly how far the generated keys are from providing any form of security ($\text{KS}_{\text{eff}} > 0$). To determine $\text{KS}_{\text{eff}}$ we, thus, have to evaluate the key entropy $H_k$ and required Hamming-distance threshold $T_{\text{HD}}$; the acquisition of which is described next.

*a) Entropy:* The upper limit $H_k$ of the effective key strength is determined by the randomness of the key-bit selection $m$ (the bit positions selected per IPI) for key generation. We assess this randomness for different $m$ by using arithmetic mean, autocorrelation, and compression tests over the generated keys (extending the tests used in [12])

1) The arithmetic-mean test evaluates the average probability of a particular key bit being one or zero, i.e., ($P(x_i = 0)$, $P(x_i = 1)$), and thus, represents the randomness when a bit is sampled from a key. This test reveals a bias in the key bits if $P(x_i = 0) \neq P(x_i = 1)$.
2) The autocorrelation test determines the probability of a key-bit being identical to its $l$th neighboring bit, i.e., $P(x_i = x_{i-l})$, where we choose $l = 1, 2, 3, ..., 20$ to determine if there are any intrakey correlations. A high value for $P(x_i = x_{i-l})$ indicates repetitive patterns in consecutive IPIs, yielding a reduction in entropy (and security) as the bits in $\text{IPI}_{(i,i+1)}$ have predictive value over those in $\text{IPI}_{(i+l,i+1+l)}$.
3) The compression test splits the generated keys into $c$-sized symbols $S$ and evaluates the frequency of each symbol occurring, i.e., $P(s) = \frac{\sum S=s}{\sum S}$, where $s = 1, 2, 3, \ldots, 2^c$, $S$ is the value of $c$ consecutive bits and we choose $c = 1, 2, 3, \ldots, 8$. A high value for $P(s)$ indicates that certain symbols (bit patterns) $s$ occur more frequently throughout the distribution, indicating correlations between consecutive IPIs and reducing entropy for reasons stated previously.

Based on the probabilities calculated using our tests, we may compute the Shannon entropy for the arithmetic mean ($H_{\text{am}}$), autocorrelation ($H_{\text{ac}}$), and compression ($H_c$) tests as [24]

$$H = \sum_i p_i \log_2 p_i \tag{2}$$

where $p_i$ is the probability of a particular event, for example, the probability of a given symbol $s$ in the compression test. As a conservative estimation, we define the minimum entropy $H_{\min} = \min(H_{\text{am}}, H_{\text{ac}}, H_c)$.

$H_k$ is expressed in terms of equivalent entropic bits, that is, the probability of guessing key $k$ is equivalent to guessing a key with $H_k$ truly entropic bits (where a truly entropic bit satisfies $H = 1, p_1 = p_0 = \frac{1}{2}$). To compute $H_k$, we first calculate $H^i_{\min}$ for all $i$ IPI-bit positions and subsequently obtain $p^i_0$ and $p^i_1$ from (2). For each IPI-bit position, a symbol $S$ may be formed by concatenating $n_{\text{eq}}$ bits. Based on $p^i_0$ and $p^i_1$, the highest probability of guessing $S$ is $p_S = p^{n_{\text{eq}}}_{\max}$,[2] where $p_{\max} = \max(p^i_0, p^i_1)$. By setting $p_S = \frac{1}{2}$, i.e., $S$ is equivalently random as a truly entropic bit (as $p_S = p_{\overline{S}} = \frac{1}{2}$), we may compute the number of bits required to form $S$ as $n_{\text{eq}} = \log_{p_{\max}}(\frac{1}{2})$. Accordingly, each IPI bit shall have equivalent entropy $H^i_{\text{eq}} = \frac{1}{n_{\text{eq}}}$. After calculating $H^i_{\text{eq}}$ for each IPI-bit position, the entropy of the key-bit selection $m$ may be obtained[3] from $H^m_{\text{eq}} = \sum_i H^i_{\text{eq}}$, for all $i \epsilon m$. Finally, as $n$ key-segments are combined to form key $k$, we obtain $H_k = H^m_{\text{eq}} \cdot n$.

*b) Hamming-Distance Threshold:* $T_{\text{HD}}$ is a function of the desired probability of key-matching and $\text{VAR}_{\text{is}}$. Lowering $T_{\text{HD}}$ allows for an increase in $\text{KS}_{\text{eff}}$ (as an attacker's key is required to be more similar to the actual key), yet also reduces the chance of successful matching for a true-key pair. To determine $T_{\text{HD}}$, we compare the keys generated by two entities and see at what threshold $T_{\text{HD}}$ the keys would lead to authentication *reliably*, where we define reliable authentication of a new key as successful authentication within a predefined, upper time limit with probability $P_{\text{auth}} = 1 - 10^{-6}$ [12]. Without loss of generality, in this study, we set the key length to 60 bits and the time limit to 60 s. We expect that such an authentication criterion will be feasible for some of the most safety-critical applications of IPI-based security, such as providing emergency-authentication credentials [4], [5]. We evaluate a 60-bit key as it is allows us to easily assess the key strength under our authentication constraints, as has been done in prior work [5], [12].

We model $\text{VAR}_{\text{is}}$ as the time difference between the heart beats measured by ECG and BP recordings obtained from the *Fantasia dataset* [25], that is, $\text{VAR}_{\text{is}} = \text{beats}_{\text{BP}} - \text{beats}_{\text{ECG}}$. We consider this model realistic for typical mHealth applications, such as a BAN, as it incorporates the effects of both different biosignals and measurement locations. As our used datasets provide ECG recordings only (first entity), we add $\text{VAR}_{\text{is}}$ to these recordings to emulate BP recordings (second entity) [12]. The validity of this approach is supported by the following simularities between our model and established works that measure the second recording directly.

1) The time difference between the recording are normally distributed, as also described in [5] and [26].
2) The bit-error rates (presented in Table I) are similar to those reported in [26]. Note that the bit-error rate is sub-

[2]Given that $p_0 = 1 - p_1$, a maximum operator is used so as to get the highest probability between $p_0$ and $p_1$. This is the only way that, when concatenating multiple bits $n$, we can get a combined probability $p^n_{0|1} = 0.5$.

[3]In this and a previous study, we have not found any *intra*-IPI dependences (between IPI bits), permitting $H^m_{\text{eq}}$ to be calculated as a linear addition of the $H^i_{\text{eq}}$ of the selected IPI bits [12].

TABLE I
AVERAGE BIT-ERROR RATE (BER) DATASET DUE TO $VAR_{IS}$ WHEN APPLIED TO THE *MIT-Regular* DATASET

| Bit # | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| BER | 0.46 | 0.29 | 0.15 | 0.08 | 0.04 | 0.02 | 0.01 | 0.00 |

TABLE II
DATASET SPECIFICATIONS

| Dataset | #Subjects | #IPIs | Avg. Heart Rate (BPM) | Sensor Freq. (Hz) |
|---|---|---|---|---|
| *MIT-Regular* | 11 | 21696 | 69.3 | 360 |
| *MIT-Ectopic* | 12 | 16008 | 81.7 | 360 |
| *MIT-Episode* | 20 | 38424 | 86.4 | 360 |
| *RE-Rest* | 58 | 10668 | 75.8 | 200 |
| *RE-Exercise* | 53 | 11864 | 101.4 | 200 |

stantial (0.46) for the least-significant IPI-bits and shows an exponential decrease for more significant IPI-bits.

3) The relation between $T_{\mathrm{HD}}$ and the resulting authentication rate [12] is analogous to that reported in [6], [8], and [26].

*2) Datasets:* Table II shows the number of IPIs, average heart rate [in beats per minute (BPM)] and sensor-sampling frequencies of the datasets used in our experiments. As we consider CVD patients as likely users of (cardiac) IMDs, we have used the *MIT-BIH arrhythmia* (*MIT-**) dataset, a commonly used dataset containing recordings of subjects with a wide variety of CVDs [27], [28]. In order to investigate the impact of cardiac arrhythmias on the entropy of IPIs, we have split this dataset into the following subsets: *MIT-Regular:* Subjects that show less than 0.5% of abnormalities from a normal sinus rhythm; *MIT-Ectopic:* Subjects with 0.5–10% of their heart beats being ectopic (premature ventricular or atrial contraction); and *MIT-Episode:* Subjects that exhibit episodes of ventricular bigeminy, trigeminy, tachycardia or with more than 10% of their beats being ectopic. In addition, we have used the *Rest-And-Exercise* (*RE-**) dataset from the BioSec ECG-database [18]. This dataset contains two sets of recordings, one from subjects at rest (*RE-Rest*) and one from the same subjects immediately after exercise (*RE-Exercise*). Using the *RE-Exercise* dataset will allow us to investigate the strength of keys generated for subjects during exercise, which is known to drastically reduce HRV (and thus, entropy per IPI) as described in Section II. Besides, as the recordings in the *RE-** dataset are sampled at 200 Hz, roughly half of the *MIT-** dataset (360 Hz), we may characterize the key strength as a function of sampling frequency by comparing the *RE-Rest* and *MIT-Regular* datasets.

## B. Experimental Results

As described in the previous section, the effective key strength $\mathrm{KS}_{\mathrm{eff}}$ is used to quantify the performance of IPI- and ImPI-based key generators. To obtain $\mathrm{KS}_{\mathrm{eff}}$, we first provide a detailed description of the key entropy $H_k$, followed by an evaluation of the required Hamming-distance threshold $T_{\mathrm{HD}}$ for a given true-key pair. $\mathrm{KS}_{\mathrm{eff}}$ is, then, derived by considering (1).

TABLE III
ENTROPY-TEST RESULTS FOR THE *MIT-Regular* DATASET

| Bit | $H^i_{\mathrm{am}}$ | $H^i_{\mathrm{ac}}$ | $H^i_c$ | $H^i_{\mathrm{min}}$ | $H^i_{\mathrm{eq}}$ |
|---|---|---|---|---|---|
| 0 | 1.00 | 1.00 | 1.00 | 1.00 | 0.91 |
| 1 | 1.00 | 1.00 | 1.00 | 1.00 | 0.91 |
| 2 | 1.00 | 1.00 | 1.00 | 1.00 | 0.92 |
| 3 | 1.00 | 1.00 | 1.00 | 1.00 | 0.91 |
| 4 | 1.00 | 0.98 | 0.97 | 0.97 | 0.74 |
| 5 | 0.99 | 0.89 | 0.86 | 0.86 | 0.48 |
| 6 | 0.99 | 0.74 | 0.70 | 0.70 | 0.30 |
| 7 | 0.83 | 0.46 | 0.42 | 0.42 | 0.13 |

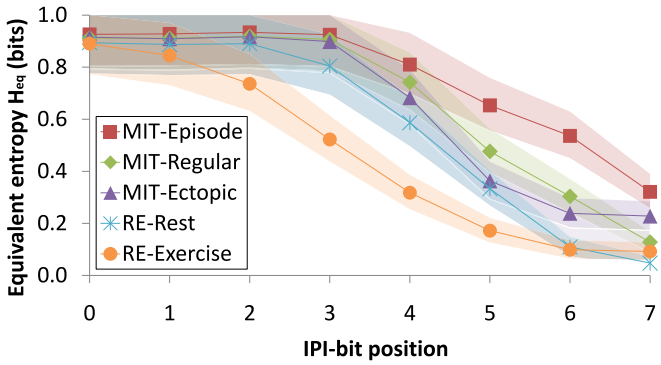


Fig. 3. Entropy per IPI bit $H^i_{\mathrm{eq}}$ for the considered datasets.

*1) Entropy:* In this section, we evaluate the entropy per ImPI, considering the frequency and HRV characteristics of the used datasets. This evaluation is first carried out for the baseline key generator, which is based on the IPI, after which we show how the ImPL improves the key entropy.

*a) IPI:* Let us first consider the situation where only one bit is selected per IPI for the baseline key generator. Table III presents the entropy results for the *MIT-Regular* dataset, showing the test results for all $i$ IPI-bits ($H^i_{\mathrm{am}}$, $H^i_{\mathrm{ac}}$, and $H^i_c$) and the resulting min-entropy $H^i_{\mathrm{min}}$. Other datasets have similar results and are discussed later in this section. In line with related work, we see that the four least-significant bits of each IPI contain a high degree of entropy, scoring the maximum 1.00 for all tests. From IPI-bit position 4 onwards, we find that the entropy results are gradually decreasing: While $H^i_{\mathrm{am}}$ appears mostly unaffected, we see a substantial decrease in $H^i_{\mathrm{ac}}$ and $H^i_c$. That is, these most-significant IPI-bits do not show a particular bias, they show significant correlations between consecutive IPIs (the minimum value for $H^i_{\mathrm{ac}}$ and $H^i_c$ were obtained using test parameters $l = 1$ and $c = 8$, respectively), effectively reducing entropy. Table III also presents the equivalent entropy per IPI-bit $H^i_{\mathrm{eq}}$. Note that even though $H^i_{\mathrm{min}}$ is considerably high for several bit positions (1.00), $H^i_{\mathrm{eq}}$ is substantially lower with a maximum value of 0.92: Due to the logarithmic scale onto which $H^i_{\mathrm{min}}$ is defined, even a small difference between the maximum-attainable entropy ($H^i_{\mathrm{min}} = 1$) and the measured $H^i_{\mathrm{min}}$ results in a significant reduction in $H^i_{\mathrm{eq}}$. For the most-significant IPI bits, the impact on $H^i_{\mathrm{eq}}$ is more dramatic.

To understand the effects of HRV and sensor-sampling frequency on the entropy per IPI, we depict $H^i_{\mathrm{eq}}$ for the various datasets in Fig. 3, including confidence intervals (with a confidence coefficient of 0.01). Note that $H^i_{\mathrm{eq}}$ is monotonously

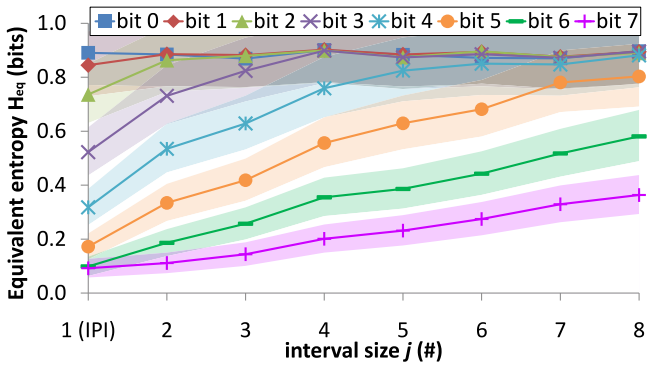


Fig. 4. Entropy per ImPI bit $H^i_{\mathrm{eq}}$ as a function of interval size $j$, here depicted for the *RE-Exercise* dataset.

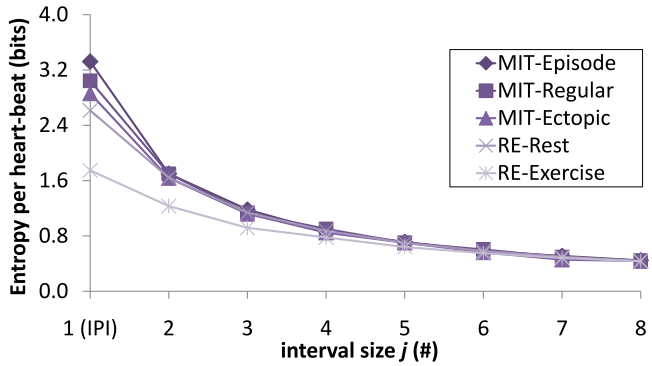


Fig. 5. Entropy per heart beat $H^m_{\mathrm{eq}}/j$ using ImPI-bit positions 2–5.

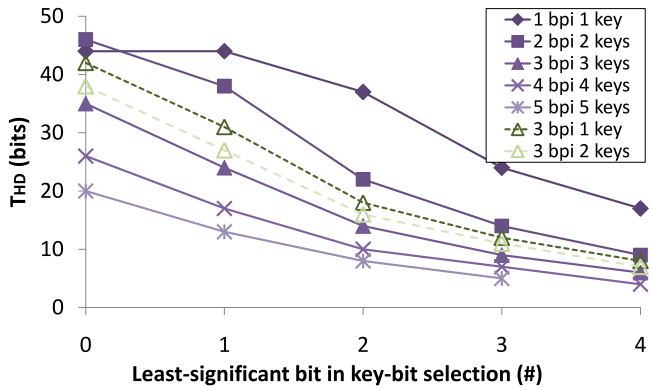


Fig. 6. $T_{\mathrm{HD}}$ for the *MIT-Regular* dataset as a function of the bits selected per IPI and multikey authentication. $n_m$ consecutive bits are selected per IPI (bpi), starting from the IPI-bit position on the *x*-axis.

decreasing for all datasets as a function of $i$, i.e., the inclusion of more significant IPI-bits in the key-bit selection $m$ will inevitably result in a reduction of $H^m_{\mathrm{eq}}$. From Fig. 3, we make three interesting observations: *1)* all of the *MIT-** datasets maintain a relatively high $H^i_{\mathrm{eq}}$ ($\geq 0.90$) for their four least-significant IPI-bits. While it appears that ectopic beats result in a slightly lower $H^i_{\mathrm{eq}}$ compared to a regular heart rate (comparing *MIT-Ectopic* to *MIT-Regular*), we find that the entropy of patients during episodes of arrhythmia is significantly higher (*MIT-Episode*); *2)* comparing the *MIT-Regular* to the *RE-Rest* datasets shows the effect of a lower sensor-sampling rate. The *RE-Rest* follows the same trend as the *MIT-Regular* dataset, albeit shifted to the left by one bit position, i.e., lowering the sampling frequency reduces the entropy which may be obtained; and *3)* the *RE-Exercise* dataset shows a rapid decrease in entropy from IPI-bit position 1 onwards compared to other datasets, i.e., subjects with limited HRV show a significant reduction in entropy per IPI.

*b) ImPI:* Let us now consider $H^i_{\mathrm{eq}}$ for ImPIs as a function of interval size $j$, as depicted in Fig. 4 for the *RE-Exercise* dataset. Recall from Section III that the ImPI is equivalent to the IPI for $j = 1$. Other datasets follow similar trends and will be discussed later in this section. First, looking at $i = 0$ (the least-significant ImPI-bit), we observe that $H^0_{\mathrm{eq}}$ remains at its maximum value of 0.89 bit. As this bit position already contains a strong degree of entropy, increasing the interval size $j$ per ImPI does not increase $H^0_{\mathrm{eq}}$. For subsequent bit positions, however, we find that increasing $j$ *does* increase their entropy. Bit position 2, for example, has an entropy $H^2_{\mathrm{eq}}$ of 0.74 for $j = 1$; 0.86 for $j = 2$; and reaches the "ceiling" of 0.89 bit for $j = 3$. For more significant ImPI-bits, the increase in $H^i_{\mathrm{eq}}$ is more limited. Regardless of bit position, though, all trends in Fig. 4 appear to be monotonously increasing, i.e., increasing $j$ results in an increase in entropy per ImPI.

The downside of increasing $j$ is that $j$ times more heart beats are required to obtain one ImPI, i.e., less ImPIs may be generated in a given amount of time compared to IPIs. To provide a direct comparison in terms of extraction rate, that is, the entropy extracted per heart beat, we normalize the obtained entropy per ImPI by the heart-beat intervals considered ($H_{\mathrm{eq}}/j$). A representative example is provided in Fig. 5 for the various datasets, where the key-bit selection $m$ is bits 2-5 of each ImPI. For $j = 1$ (IPIs), we find a difference in $H^m_{\mathrm{eq}}/j$ between the various datasets due to the differences in the entropy $H^m_{\mathrm{eq}}$ per IPI, as previously shown in Fig. 3. By subsequently increasing $j$, we find that $H^m_{\mathrm{eq}}/j$ is reduced for all datasets, in particular for the *MIT-** datasets that have a high $H^m_{\mathrm{eq}}/j$ for $j = 1$. Datasets with high initial entropy ($j = 1$) cannot benefit from $j >1$, resulting in progressively lower entropy for increasing $j$'s. Datasets with limited entropy per IPI (*RE-Exercise*, *RE-Rest*), on the other hand, allow for an increase in $H^m_{\mathrm{eq}}$ when $j$ is increased, resulting in a less dramatic reduction in $H^m_{\mathrm{eq}}/j$. Due to this saturation of entropy, we find that $H^m_{\mathrm{eq}}$ (and thus, the entropy per ImPI) becomes asymptotically the same as $j$ is increased for all datasets.

*2) Hamming-Distance Threshold:* We next evaluate the required Hamming-distance threshold $T_{\mathrm{HD}}$ for a given true-key pair. First, we consider $T_{\mathrm{HD}}$ for an IPI-based key-generator as a function of the key-bit selection $m$, multikey authentication and heart rate. Afterwards, we describe the effects on $T_{\mathrm{HD}}$ when using the ImPI.

*a) IPI:* Fig. 6 depicts $T_{\mathrm{HD}}$ as a function of the key-bit selection $m$ [recall that $m$ is formed by selecting $n_m$ bits per IPI (bpi)] and $a$-multikey authentication (described later) for the *MIT-Regular* dataset. When $m$ includes the least-significant IPI bit (starting from bit 0), we find a high value for $T_{\mathrm{HD}}$. This value generally drops when selecting more significant bits for $m$: As these more significant IPI-bits are less sensitive to $\mathrm{VAR}_{\mathrm{is}}$, they contribute relatively little to the disparity between two keys.

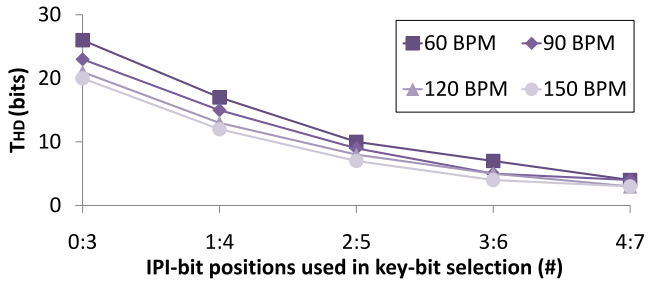


Fig. 7. $T_{\mathrm{HD}}$ as a function of heart rate. Four consecutive bits are selected per IPI.

TABLE IV
AVERAGE 60-BIT-KEY-GENERATION TIME IN SECONDS

| Dataset | Heart Rate (BPM) | Bits Per IPI (#) 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| *MIT-Regular* | 68.3 | 52.7 | 26.3 | 17.6 | 13.2 | 10.5 | 8.8 |
| *MIT-Ectopic* | 81.7 | 44.1 | 22.0 | 14.7 | 11.0 | 8.8 | 7.3 |
| *MIT-Episode* | 86.4 | 41.7 | 20.8 | 13.9 | 10.4 | 8.3 | 6.9 |
| *RE-Rest* | 75.7 | 47.5 | 23.8 | 15.8 | 11.9 | 9.5 | 7.9 |
| *RE-Exercise* | 101.4 | 35.5 | 17.8 | 11.8 | 8.9 | 7.1 | 5.9 |

Using $n_m$ bpi's implies that the number of IPIs needed to form a 60-bit key is reduced (to $\frac{60}{n_m}$), allowing for multiple authentication attempts to be made within our 60-s authentication-time constraint. We refer to this as multikey authentication. As we require an entity to authenticate reliably with probability $P_{\text{auth}} = 1 - 10^{-6}$ within 60 s, having $a$ attempts results in $P_{\text{auth-key}} = 1 - \sqrt[a]{10^{-6}}$ for each individual key. In turn, this lowers $T_{\mathrm{HD}}$: To illustrate, Fig. 6 also depicts $T_{\mathrm{HD}}$ when selecting 3 bpi, where $T_{\mathrm{HD}}$ is based on $a = 1$, 2, or 3 authentication attempts (keys). Note that $T_{\mathrm{HD}}$ is decreased with increasing values of $a$.

So far we have discussed $T_{\mathrm{HD}}$ for the *MIT-Regular* dataset, of which the average heart rate is 68.3 BPM. As a higher heart rate implies faster key generation, it may be possible to further decrease $T_{\mathrm{HD}}$ as a function of the heart rate by increasing the number of authentication attempts. In practice, an entity could calculate the total time $t$ required to obtain enough IPIs for key generation, derive the possible number of authentication attempts within our authentication-time constraint as $a = \frac{60}{t}$ and base $T_{\mathrm{HD}}$ on $a$-multikey authentication. To exemplify, Fig. 7 depicts $T_{\mathrm{HD}}$ for various heart rates, where keys are generated using four bits per IPI. Note that a higher heart rate results in a reduction in $T_{\mathrm{HD}}$. This reduction in $T_{\mathrm{HD}}$ is most noticeable when least-significant IPI-bit positions are included in the key-bit selection.

Multikey authentication does not only benefit $T_{\mathrm{HD}}$: As each key authenticates with a probability of $1 - \sqrt[a]{10^{-6}}$, we may improve the average authentication time significantly. For example, using $n_m = 2$, 3, or 4 bpi results in an authentication probability of 99.997%, 99.978%, or 99.944% per key, while requiring $\frac{1}{n_m}$ of the key-generation time when $n_m = 1$ bpi. Table IV presents the average time required to generate a key for our used datasets, based on the number of bits selected. Obviously, both a higher heart rate and the use of more bits per IPI lead to faster key generation and authentication time.

*b) ImPI:* Let us now discuss $T_{\mathrm{HD}}$ for an ImPI-based key-generator. As with the IPI, each ImPI is calculated as the difference between two heart beats, where the detection of each heart beat is subject to $\mathrm{VAR}_{\mathrm{is}}$. Our experiments have confirmed that the disparity between two keys is independent from the number of considered heart beats per ImPI $j$, i.e., $T_{\mathrm{HD}}$ is not directly affected by the used heart beats. However, $T_{\mathrm{HD}}$ is indirectly affected, as increasing $j$ increases the average key-generation time by a factor $j$. This reduces the number of keys that may be generated in the 60-s authentication window, leading to an increase in $T_{\mathrm{HD}}$ given the discussion on multikey authentication previously. Moreover, certain key-bit selections may no longer be feasible: For example, when $j = 5$ and $n_m = 3$bpi, subjects from the *MIT-Regular* would require an average key-generation time of $5 \cdot 17.6 = 88$ s (see Table IV), exceeding our authentication time constraint.

*3) Key Strength:* Based on the $H_k$ and $T_{\mathrm{HD}}$, we may now calculate the effective key strength $\mathrm{KS}_{\mathrm{eff}}$. Here, we calculate $H_k$ based on the accumulation of the entropy of individual ImPI-bits included in the key-bit selection (as discussed in Section IV-B1) and base $T_{\mathrm{HD}}$ on both the bits selected per ImPI, the average heart rate per dataset and multikey authentication. For all cases, $\mathrm{KS}_{\mathrm{eff}}$ is evaluated for a 60-bit key and reliable authentication with probability $P_{\text{auth}} = 1 - 10^{-6}$ within 60 s,[4] as described in Section IV-A1. First, we discuss $\mathrm{KS}_{\mathrm{eff}}$ for IPI-based keys, after that we conclude with the results for ImPI-based keys.

*a) IPI:* Fig. 8(a) depicts the key strength for the *MIT-Regular* dataset, varying the IPI bits in the key-bit selection.[5] Other datasets yield similar results and are discussed at the end of this section. First, let us consider $\mathrm{KS}_{\mathrm{eff}}$ when a single key is generated using 1 bpi (in 52.7 s, see Table IV). For bit position 0, we find a negative $\mathrm{KS}_{\mathrm{eff}}$ of $-34.2$ bits: While bit 0 contains the most entropy ($H_k = 53.6$ bits), it is also the most strongly affected by $\mathrm{VAR}_{\mathrm{is}}$ ($T_{\mathrm{HD}} = 44$ bits), resulting in a negative $\mathrm{KS}_{\mathrm{eff}}$. As the entropy for the four least-significant IPI bits is roughly the same for the *MIT-Regular* dataset (see Table III), while $\mathrm{VAR}_{\mathrm{is}}$ decreases, we find an increase in $\mathrm{KS}_{\mathrm{eff}}$ up to bit position 4, at which point $\mathrm{KS}_{\mathrm{eff}} = 9.5$ bits. From bit 4 onwards, $\mathrm{KS}_{\mathrm{eff}}$ once again drops: While $T_{\mathrm{HD}}$ does decrease for more significant IPI bits, the even steeper decrease in entropy results in negative $\mathrm{KS}_{\mathrm{eff}}$ scores.

By using multiple bpi's, it becomes possible to generate multiple keys in the same time of generating a single key using 1 bpi—and thus, perform multiple authentication attempts. This results in an increase in $\mathrm{KS}_{\mathrm{eff}}$ as may be observed from Fig. 8(a), which may be attributed to the effect of multikey authentication on $T_{\mathrm{HD}}$. From all key-bit selections, the maximum $\mathrm{KS}_{\mathrm{eff}}$ (22.7 bits) is obtained by generating a key using IPI bits 2–4: In this case, $T_{\mathrm{HD}}$ is based on three authentication attempts, where a

[4]As discussed in Section IV-B2, certain key-bit selections result in a key-generation time significantly smaller than 60 s. In these cases, multiple authentication attempts may be made within our authentication constraint of 60 s, which effectively decreases $T_{\mathrm{HD}}$, and thus, increases $KS_{\mathrm{eff}}$.

[5]Recall from Section IV-A that a negative key strength ($\mathrm{KS}_{\mathrm{eff}} < 0$) indicates that an attacker is more likely to authenticate on their first attempt than not, i.e., the generated keys provide practically no security.

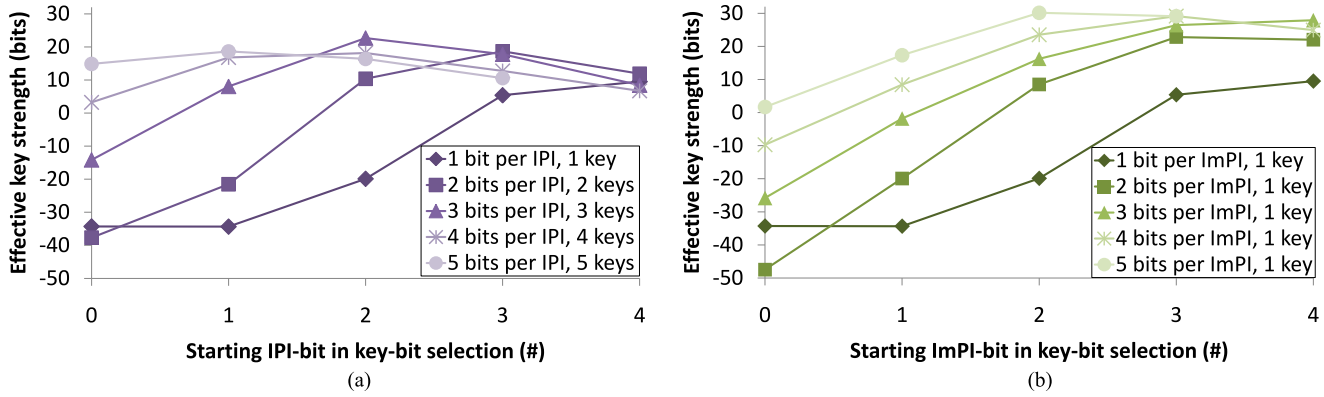


Fig. 8. Effective key strength $\mathrm{KS}_{\mathrm{eff}}$ for the *MIT-Regular* dataset using ImPI-based key generation. $n_m$ consecutive bits are selected per ImPI, starting from the ImPI-bit position on the *x*-axis. (a) IPI-based key generation, where $\mathrm{KS}_{\mathrm{eff}}$ is based on $n_m$ authentication attempts; (b) ImPI-based key generation where $\mathrm{KS}_{\mathrm{eff}}$ is based on a single authentication attempt by setting $j = n_m$, i.e., only one key is generated.

TABLE V
BEST KEY STRENGTH PER DATASET USING THE IPI

| Dataset | Bits Selected | Best $\mathrm{KS}_{\mathrm{eff}}$ (bit) | Single Key-Generation Time (s) |
|---|---|---|---|
| *MIT-Regular* | 2–4 | 22.7 | 17.6 |
| *MIT-Ectopic* | 2–4 | 19.1 | 14.7 |
| *MIT-Episode* | 2–6 | 29.2 | 8.3 |
| *RE-Rest* | 1–5 | 16.4 | 11.9 |
| *RE-Exercise* | 1–3 | 5.7 | 11.8 |

TABLE VI
BEST KEY STRENGTH PER DATASET USING THE IMPI, COMPARED TO THE STRONGEST IPI-BASED KEYS

| Dataset | Interval Size ($j$) | Bits Selected | Best $\mathrm{KS}_{\mathrm{eff}}$ (bit) | Single Key-Generation Time (s) |
|---|---|---|---|---|
| *MIT-Regular* | 6 | 2-7 | 30.2 (+33%) | 52.7 (3.0×) |
| *MIT-Ectopic* | 6 | 2-6 | 26.6 (+39%) | 52.9 (3.6×) |
| *MIT-Episode* | 4 | 3-6 | 29.8 (+2%) | 55.5 (6.7×) |
| *RE-Rest* | 5 | 2-6 | 31.3 (+92%) | 47.5 (4.0×) |
| *RE-Exercise* | 8 | 2-6 | 24.9 (+3.4×) | 56.8 (4.8×) |

single key is generated in 17.6 s (see Table IV). That is, reliable authentication using three keys is provided in $3 \cdot 17.6 = 52.7$ s.

Following the same methodology for all datasets, Table V summarizes the best key-bit selections and resulting key strengths for each dataset. For the *MIT-** datasets, we find a $\mathrm{KS}_{\mathrm{eff}} \geq 19.1$ bits. The *MIT-Episode* dataset yields a more substantial $\mathrm{KS}_{\mathrm{eff}} = 29.2$ bits compared to its counterparts, attributed to the high $H_{\mathrm{eq}}^{i}$ that may be found in its most-significant bits. Note that all *MIT-** datasets exclude IPI-bits 0 and 1 from their key-bit selection. Conversely, it may be stated that these sensors are oversampling (by a factor 4) and that a sensor with a 1/4th the sampling rate (90 Hz) would be more than sufficient. For the *RE-Exercise* dataset, we find a maximum $\mathrm{KS}_{\mathrm{eff}} = 5.7$ bits obtained using IPI bits 1–3, significantly smaller than for the *RE-Rest* dataset ($\mathrm{KS}_{\mathrm{eff}} = 16.4$ bits). The reduced entropy per IPI of these former subjects prohibits the generation of strong security keys. Finally, the average key-generation time for each individual key is equal to or less than 17.4 s for all datasets, allowing over 99.9% of the authentication attempts to complete within this time as discussed in the previous section.

*b) ImPI:* In the previous sections, it was shown that by increasing the interval size $j$, the entropy per ImPI is increased (i.e., increasing $H_k$) while less keys may be generated in the same time, increasing $T_{\mathrm{HD}}$. To understand the key strength as a function of $j$, let us first set the number of selected bits per ImPI $n_m = j$. In doing so, only one ImPI key is generated and we exclude the effect of multikey authentication on $T_{\mathrm{HD}}$. Fig. 8(b) depicts a representative example of this evaluation for the *MIT-Regular* dataset. Similar to IPI-based keys [see Fig. 8(a)], we find that the ImPI-key strength is limited when the key-bit selection includes the least-significant ImPI bits and is increased when including more significant bits.

We may now determine the most efficient solution—using multiple IPI keys or a single ImPI key—by comparing the results for IPI and ImPI-based keys in Fig. 8(a) and (b). When the key-bit selection includes ImPI bit positions 0 or 1, we find that the $\mathrm{KS}_{\mathrm{eff}}$ of an ImPI-based key is lower than that of an IPI-based key. As discussed in Section IV-B1a, the entropy of these bit positions is high even if $j = 1$ and is barely increased as a function of $j$, i.e., $H_k$ does not change significantly. $T_{\mathrm{HD}}$, on the other hand, is increased substantially by lowering the number of generated ImPI-keys, resulting in an overall reduction in $\mathrm{KS}_{\mathrm{eff}}$. When the key-bit selection is shifted to more significant bits, we find that an ImPI-based key yields a *stronger* $\mathrm{KS}_{\mathrm{eff}}$: While $T_{\mathrm{HD}}$ is increased by reducing the number of generated keys, the substantial increases in entropy due to the used bit positions yields a higher $\mathrm{KS}_{\mathrm{eff}}$. The strongest ImPI key ($\mathrm{KS}_{\mathrm{eff}} = 30.2$ bits) is obtained using ImPI bits 2–7 and provides reliable authentication within 52.7 s. Under the same authentication constraints, the strongest IPI key (discussed before) has a more limited key strength of $\mathrm{KS}_{\mathrm{eff}} = 22.7$ bits. ImPI-based keys may, thus, achieve a higher key strength than IPI-based keys.

Finally, by varying both $j$ and the selection of bits ($j$ does not necessarily equal $n_m$), we derive the best possible $\mathrm{KS}_{\mathrm{eff}}$ for each dataset, as presented in Table VI. In line with our previous conclusions, we find that the datasets that already contain a high degree of entropy do not benefit much from using the ImPI, most notably the *MIT-Episode* dataset. For datasets with lower entropy, however, we find substantial increases in the key strength, up to $\mathrm{KS}_{\mathrm{eff}} = 24.9$ bits (+3.4× compared to the optimal

IPI-bit selection) for the *RE-Exercise* dataset. That is, when the entropy per IPI is limited, the ImPI provides stronger security than IPI-based keys. It is interesting to observe that when using the ImPI, all datasets shift their key-bit selection to the more significant bits per ImPI, taking advantage of the increase in $H_{\mathrm{eq}}$ and minimal increase in $T_{\mathrm{HD}}$. Finally, note that while these keys are generated within our authentication-time constraint of 60 s, we do find a substantial increase in key generation time between 3 and 6.7×.

## V. Conclusion

This paper has presented a thorough evaluation of the security performance of a heart-beat-based-security system that uses IPI as a source of entropy, considering the effects of (limited) HRV, sensor-sampling frequencies, $\mathrm{VAR}_{\mathrm{is}}$, and multikey authentication. In addition, we have introduced a novel key-generator based on the ImPI, which considers the time interval between two nonconsecutive heart beats. It was shown that while successful authentication may occur within 17.4 s for an IPI-based key-generator, the effective key strength may be as low as 5.7 bits for subjects with limited HRV. This key strength was successfully increased by up to 3.4× (+19.2 bits) through using the ImPI-based key generation, at the cost of an increase in key-generation time of 4.8× (from 11.8 to 59.8 s). That is, using the ImPI in key generation results in stronger keys than using the IPI, given the same authentication time. In order to maximize the security of heart-beat-based systems, future security protocols should consider the possibility of dynamically adjusting the key-generation settings, as revealed by this study.

## Acknowledgment

The authors would like to thank Dr. F. Agrafioti for her feedback, without which this work would not have been completed.

## References

[1] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[2] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel, "Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2010, pp. 917–926.

[3] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: New directions for implantable medical device security," presented at the HotSec, Berkeley, CA, USA, 2008.

[4] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. De Zeeuw, "Adaptive entity-identifier generation for IMD emergency access," in *Proc. ACM Cryptography Security Comput. Syst.*, 2014, pp. 41–44.

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

[6] C. C. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73–81, Apr. 2006.

[7] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, Jan. 2010.

[8] S.-D. Bao, C. C. Poon, Y.-T. Zhang, and L.-F. Shen, "Using the timing information of heartbeats as an entity identifier to secure body sensor network," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 6, pp. 772–779, Nov. 2008.

[9] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE Conf. Comput. Commun.*, 2011, pp. 1862–1870.

[10] M. Rushanan, A. D. Rubin, D. F. Kune, C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Security Privacy*, pp. 529–539, 2014.

[11] S.-Y. Chang, Y.-C. Hu, H. Anderson, T. Fu, and E. Y. Huang, "Body area network security: Robust key establishment using human body channel," in *Proc. USENIX Conf. Health Security Privacy*, 2012, pp. 1–10.

[12] R. M. Seepers, C. Strydis, P. Peris-Lopez, I. Sourdis, and C. De Zeeuw, "Peak misdetection in heart-beat-based security characterization and tolerance," in *Proc. IEEE Eng. Med. Biol. Soc. Conf.*, 2014, pp. 5401–5405.

[13] G.-H. Zhang, C. C. Poon, and Y.-T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 1, pp. 176–182, Jan. 2012.

[14] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG analysis: A new approach in human identification," *IEEE Trans. Instrum. Meas.*, vol. 50, no. 3, pp. 808–812, Jun. 2001.

[15] K. N. Plataniotis, D. Hatzinakos, and J. K. Lee, "ECG biometric recognition without fiducial detection," in *Proc. Biometrics Symp.: Special Session Res. Biometric Consortium Conf.*, 2006, pp. 1–6.

[16] T.-W. Shen, W. Tompkins, and Y. Hu, "One-lead ECG for identity verification," in *Proc. IEEE EMBS/BMES Annu. Conf. Fall Meeting*, 2002, vol. 1, pp. 62–63.

[17] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society*. New York, NY, USA: Springer, 1999.

[18] F. Agrafioti, F. M. Bui, and D. Hatzinakos, "Medical biometrics in mobile health monitoring," *Security Commun. Netw.*, vol. 4, no. 5, pp. 525–539, 2011.

[19] U. R. Acharya, K. P. Joseph, N. Kannathal, C. M. Lim, and J. S. Suri, "Heart rate variability: A review," *Medi. Biol. Eng. Comput.*, vol. 44, no. 12, pp. 1031–1051, 2006.

[20] B. M. Appelhans and L. J. Luecken, "Heart rate variability as an index of regulated emotional responding," *Rev. Gen. Psychol.*, vol. 10, no. 3, pp. 229–240, 2006.

[21] I. Antelmi, R. S. De Paula, A. R. Shinzato, C. A. Peres, A. J. Mansur, and C. J. Grupi, "Influence of age, gender, body mass index, and functional capacity on heart rate variability in a cohort of subjects without heart disease," *Amer. J. Cardiol.*, vol. 93, no. 3, pp. 381–385, 2004.

[22] M. P. Tulppo, T. Makikallio, T. Takala, T. Seppanen, and H. V. Huikuri, "Quantitative beat-to-beat analysis of heart rate dynamics during exercise," *Amer. J. Physiol.—Heart Circulatory Physiol.*, vol. 271, no. 1, pp. H244–H252, 1996.

[23] J. von Neumann, *Various Techniques Used in Connection With Random Digits*, National Bureau of Standards Applied Math Series, pp. 36–38, 1951.

[24] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[25] N. Iyengar, C. K. Peng, R. Morin, A. L. Goldberger, and L. A. Lipsitz, "Age-related alterations in the fractal scaling of cardiac interbeat interval dynamics," *Amer. J. Physiol.*, vol. 271, no. 4, pp. R1078–R1084, 1996.

[26] T. Hong, S.-D. Bao, Y.-T. Zhang, Ye Li, and P. Yang, "An improved scheme of IPI-based entity identifier generation for securing body sensor networks," in *Proc. IEEE Eng. Med. Biol. Soc. Conf.*, 2011, pp. 1519–1522.

[27] A. L. Goldberger, L. A. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C.-K. Peng, and H. E. Stanley, "Physiobank, physiotoolkit, and physionet components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

[28] G. B. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," *IEEE Eng. Med. Biol. Mag.*, vol. 20, no. 3, pp. 45–50, May/Jun. 2001.

Authors' photographs and biographies not available at the time of publication.