IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 20, 2017, accepted October 16, 2017, date of publication October 31, 2017,
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2766523

Low-Latency Approach for Secure ECG Feature Based Cryptographic Key Generation

SANAZ RAHIMI MOOSAVI[1], (Student Member, IEEE), ETHIOPIA NIGUSSIE[1], (Senior Member, IEEE), MARCO LEVORATO[2], (Member, IEEE), SEPPO VIRTANEN[1], (Senior Member, IEEE), AND JOUNI ISOAHO[1]

[1]Department of Future Technologies, University of Turku, 20500 Turku, Finland
[2]Department of Computer Science, University of California at Irvine, Irvine, CA 92697, USA

Corresponding author: Sanaz Rahimi Moosavi (saramo@utu.fi)

ABSTRACT We propose a low-latency approach for generating secure electrocardiogram (ECG) feature-based cryptographic keys. This is done by taking advantage of the uniqueness and randomness properties of ECG's main features. This approach achieves a low-latency since the key generation relies on four reference-free ECG's main features that can be acquired in short time. We call the approach several ECG features (SEF)-based cryptographic key generation. SEF consists of: 1) detecting the arrival time of ECG's fiducial points using Daubechies wavelet transform to compute ECG's main features accordingly; 2) using a dynamic technique to specify the optimum number of bits that can be extracted from each main ECG feature, comprising of PR, RR, PP, QT, and ST intervals; 3) generating cryptographic keys by exploiting the above-mentioned ECG features; and 4) consolidating and strengthening the SEF approach with cryptographically secure pseudo-random number generators. Fibonacci linear feedback shift register and advanced encryption standard algorithms are implemented as the pseudo-random number generator to enhance the security level of the generated cryptographic keys. Our approach is applied to 239 subjects' ECG signals comprising of normal sinus rhythm, arrhythmia, atrial fibrillation, and myocardial infraction. The security analyses of the proposed approach are carried out in terms of distinctiveness, test of randomness, temporal variance, and using National Institute of Standards and Technology benchmark. The analyses reveal that the normal ECG rhythms have slightly better randomness compared with the abnormal ones. The analyses also show that the strengthened SEF key generation approach provides a higher security level in comparison to existing approaches that rely only on singleton ECG features. For the normal ECG rhythms, the SEF approach has in average the entropy of about 0.98 while cryptographic keys which are generated utilizing the strengthened SEF approach offer the entropy of $\sim$1. The execution time required to generate the cryptographic keys on different processors is also examined. The results reveal that our SEF approach is in average 1.8 times faster than existing key generation approaches which only utilize the inter pulse interval feature of ECG.

INDEX TERMS Cryptographic key generation, electrocardiogram, bio-electrical signal, body area network.

I. INTRODUCTION

Body Area Network (BAN) is one of the main enabling technologies for ubiquitous healthcare systems [1]. It has emerged as a new design to carry out remote patient monitoring efficiently. BAN comprises of medical sensors that obtain, process, manage, transmit, and store patients' health information at all times. Since medical sensor nodes deal with patients' vital health data, securing their communication is an absolute necessity [2]. Without robust security features not only patients' privacy can be breached but also adversaries can potentially manipulate actual health data resulting in inaccurate diagnosis and treatment [3].

Medical sensors rely on cryptography to secure their communications [4]. Proper application of cryptography requires the use of secure keys and key generation methods. Key generation approaches that are proposed for generic wireless sensors are not directly applicable to tiny sensors used in BANs as they are highly resource-constrained and demand a higher security level [5]. Key generation in sensor networks generally requires some form of pre-deployment. Nevertheless, given the constrained nature of medical sensors used in BSNs, conventional key generation approaches may potentially involve reasonable computations as well as latency during network or any subsequent adjustments, due to their need for pre-deployment. Biometrics are generally regarded as the only solution that is lightweight, requires low resources, and indeed can identify authorized subjects in BANs [4], [6]–[8]. By developing robust key generation approaches

using biometric systems, the security of medical sensors can be offered in a plug-n-play manner where neither a network establishment nor a key pre-distribution mechanism is required. Cryptographic keys can be generated within the network on the fly through the usage of information collected by medical sensors. Furthermore, key revocation and renewal will be done automatically when and as needed. The choice of a biometric to be used for generating cryptographic keys relies on the capability of medical sensors on extracting an individual's relevant biometric information. The selected feature(s) should also meet the following design goals [4]: (i) *Distinctive*, meaning that it should be different for different subjects at any given time. (ii) *Time-variant*, meaning that it should be different for the same person at different time intervals. (iii) *Random*, meaning that it should be cryptographically random to provide security. A low degree of randomness enables an attacker to acquire a patient's cryptographic key and manipulate their medical data. (iv) *Universal*, meaning that the feature should be measurable from each subject.

Iris, fingerprints, and voice are some physiological features of the body which have the potential to identify individuals with a high degree of assurance. However, these biometric traits are not secure enough to be used for key generation techniques. The reason is that people often leave their fingerprints everywhere, audio recorders can be utilized to deceive speech recognition systems, and iris images can be captured by hidden cameras [1]. Over the last decades, several efforts have been made for the development of the next generation of biometrics known as internal biometrics (also called physiological biometrics or bio-signals) [9]. The main physiological biometrics include electrocardiogram (ECG), electroencephalogram (EEG) [10], and photoplethysmogram (PPG) [11]. From mentioned bio-signals, ECG is the only fiducial-based physiological signal of humans. Fiducials are points of interest (P, Q, R, S, and T waves) that can be extracted from each ECG signal. It has been found that the ECG meets the aforementioned design goals of a biometric trait to be used for cryptographic key generation techniques [4], [7].

Current ECG-based cryptographic keys are mostly generated using Inter Pulse Interval (IPI) feature of an ECG signal [5], [7], [12]–[16]. IPI is measured from two consecutive R peak points where the R peaks are the tallest and most conspicuous peaks in an ECG signal. In [17], we demonstrated that existing IPI-based key generation approaches suffer from a low level of security in terms of distinctiveness, test of randomness, and temporal variance. In this regard, in [17], we presented two different ECG-based cryptographic key generation approaches that offer higher security levels compared to conventional approaches. More precisely, we proposed to integrate Cryptographically Secure Pseudo-Random Number Generators (CSPRNG) along with IPI sequences to generate robust ECG-based cryptographic keys. First, we proposed a strengthened IPI-based key generation approach using a sequence of IPIs and the Fibonacci Linear Feedback Shift Register Pseudo Random Number Generator (LFSR-PRNG), called IPI-PRNG [18]. Second, we proposed an alternative key generation approach that utilized the Advanced Encryption Standard (AES) algorithm [19] and IPI sequences as the seed generator for the AES, called IPI-AES. In IPI-PRNG and IPI-AES approaches, our main focus was to enhance the security of the generated cryptographic keys while realizing a clear trade-off between the security level and key generation execution time.

In this article, we propose a new approach, called Several ECG Feature (SEF) based cryptographic key generation. The SEF approach alleviates the key generation execution overhead of the existing as well as our previous approaches, while preserving the achieved high security levels. The proposed approach is applied to both normal and abnormal ECG signals. The main contributions of this article, which is a major extension of our recent work published in [17], are threefold:

- The SEF approach uses 4 main reference-free[1] features of the ECG signal (being extracted from every ECG heartbeat cycle) along with consecutive IPI sequences to generate ECG-based cryptographic keys.
- To reinforce and enhance the security level of our approach, we consolidate the SEF key generation approach with two different cryptographically secured pseudo random number generators: (i) SEF-PRNG: we strengthened the security level of the SEF approach by exploiting the Fibonacci-LFSR pseudo random number generator (ii) SEF-AES: our SEF approach is also strengthened by utilizing the AES algorithm in counter mode. This technique exploits our SEF key generation approach as the seed generator for the AES algorithm.
- We evaluate the efficiency of our SEF, SEF-PRNG, and SEF-AES approaches by simulations in terms of distinctiveness, test of randomness, temporal variance, and execution time on real ECG data from 239 subjects with different heart health conditions.

The remainder of the paper is organized as follows: in Section II, the related work and motivation are discussed. In Section III, bio-electrical signals and ECG characteristics are discussed. Section IV presents the proposed cryptographic key generation approaches utilizing the ECG bio-electrical signal. Simulation results including distinctiveness, test of randomness, temporal variance, and key generation execution time are provided and discussed in Section V. Finally, Section VI concludes the paper.

II. RELATED WORK AND MOTIVATION

In [20]–[24], fuzzy vault-based bio-cryptographic key generation protocols are proposed for BANs. In each of these protocols, frequency domain characteristics of PPG and ECG signals are used as the physiological parameters. Bao *et al.* [25] presented an entity authentication protocol and a fuzzy commitment-based key distribution protocol, in which the IPI values generated from the PPG signals are

[1] In this context, the reference-free property indicates a dynamic technique in which no ECG fiducial point is fixed as reference.

employed as the physiological parameters. In their work, adaptive segmentation is used to divide the value range of the IPI into segments. The main drawback of the above-mentioned approaches is that they are not applicable enough to be used for generating cryptographic keys for medical sensors. This is due to the required heavy-weight computations. Poon *et al.* [4] and Zhang *et al.* [7] further evaluated the performance of Bao *et al.*'s [25] approach using both PPG and ECG signals with respect to their error rates. In another study by Bao *et al.* [12], another solution is proposed for which physiological parameter generation is utilized in a bio-cryptographic security protocol. The authors claimed that the physiological parameters which are generated utilizing the individual and multi-level IPI sequences have comparable distinctiveness and randomness. Nevertheless, the latency of these approaches is very high as 256 IPIs are required in order to generate a 64 bit cryptographic key.

Altop *et al.* [5] and Xu *et al.* [14] proposed key generation approaches in which the IPI values generated from ECG signals are utilized. In both of these works, the authors employ Gray encoding to map each IPI value to a 4-bit binary number using a uniform quantization method. According to the authors, the generated physiological parameters pass the randomness measurement tests presented by the NIST test benchmark [26]. They also stated that the generated physiological parameters pass both temporal variance and distinctiveness tests. However, in [5] and [14] no related numerical information for experimental performance evaluation in terms of key generation execution time is provided. In addition, compared to our approach, these works have failed to provide as high a security level as our approach in terms of distinctiveness, test of randomness, and temporal variance. Zhang *et al.* [7], Poon *et al.* [4], and Bao *et al.* [12] evaluated the performance of the physiological parameter generation, utilizing both PPG and ECG signals. The authors developed physiological parameter generation techniques which can be utilized in bio-cryptographic key generation approaches. In their work, these authors claimed that physiological parameters generated utilizing IPI sequences offer promising features to be exploited for cryptographic key generation approaches.

Zheng *et al.* [27] proposed a time-domain physiological parameter generation method. They used the time distances between the R peaks as the **reference points** and other peak values of an ECG signal from one heartbeat cycle. The authors claimed that their solution is faster than the conventional IPI-based methods and it ensures the property of randomness. However, their proposed approach lacks reliability as it is only applicable to ECG records collected form subjects with normal ECG rhythm or subjects with no sever cardiovascular diseases. In healthcare systems, subjects often suffer from Cardiovascular Diseases (CVDs) such as Cardiac Arrhythmia, Poor R-wave Progression, Myocardial infraction and Anterior Wall MI in which the R peaks are not easily detectable, or might be even missing within one heartbeat cycle. Choosing the R peak as the reference for calculation all the other features is not always reliable to be used for the binary sequence generations. In addition, as the main focus of the approach present in [27] is on rapid key generation, distinctiveness and temporal variance properties were not analyzed and reported in their approach. In this context, we claim that a robust ECG-based cryptographic key generation approach needs to cover both healthy and unhealthy human subjects. This necessities ECG features selection which is independent of any reference point. In a scenario where one or more fiducial points cannot be detected (due to some abnormalities), the system tries to compute and use as many features as it can collect from the current heartbeat cycle. This will be continued until the next heartbeat cycle(s) that ECG signal becomes normal. When ECG features selection is independent of any reference point, the efficiency and reliability of the ECG-based cryptographic key generation will not be affected.

In [17], our main focus was on the development and analysis of secure and efficient ECG-based cryptographic key generation techniques. We proposed two different ECG-based cryptographic key generation approaches for which the IPI feature of ECG underlays both of the approaches. The aim was to enhance the security of BANs through a robust key generation approach where keys are generated on the fly without requiring key pre-distribution solutions. It was realized that there is a clear trade-off between the security level and the key generation execution time of the proposed ECG-based cryptographic key generation approaches. This article essentially extends our previous work by reducing the key generation execution times yet providing high security levels. Our proposal is motivated by the fact that to alleviate the key generation execution times, while preserving high security levels, other main features of an ECG signal in addition to RR (also known as IPI) can be exploited. In this regard, our proposed approach exploits the main fiducial points of an ECG signal to detect and compute the the main ECG features. The utilized main features include PR, RR, PP, QT, and ST intervals. This is based on the fact these features are highly reliable and ensure the randomness property. For this purpose, we have comprehensively studied the aforementioned main features of most known ECG signals ranging from normal to abnormal ones belonging to patients with various cardiovascular diseases. We have also investigated the property of randomness of the aforementioned features to ensure that they can be used along with IPI for generating cryptographic keys. We hypothesize that, by exploiting additional features, cryptographic keys can be generated faster and in more efficient and reliable manner than those approaches which rely only on singleton IPI sequences and require R peaks as the reference points. Our approach considers both normal and abnormal electrocardiogram signal waveforms.

III. BIO-ELECTRICAL SIGNALS AND ELECTROCARDIOGRAM (ECG) CHARACTERISTICS

A Bio-electrical signal is any signal that can be continuously monitored and measured from any living being's body.

Bio-electrical signals refer to the change in electric current generated by the sum of an electrical potential difference across an organ, a specialized tissue or a cell system. Such signals are low frequency and low amplitude electrical signals that can be measured from biological beings, for instance, humans.

ECG is a rhythmically repeating and quasi-periodical signal which is synchronized by the function of the heart, and the heart performs the generation of bio-electrical events. It is the electrical manifestation of the contractile activity of the heart that is recorded at the chest level by measuring signal levels from several electrical leads attached to the patient's skin. ECG has been mainly employed in various medical applications. For instance, it has been utilized to diagnose cardiac diseases, which are one of the leading causes of death in the world [28]. Over the last few decades, there have been many efforts to develop automatic and computer-based diagnostics of heart failures [6], [21], [29]–[31]. Recently, ECG has been broadly utilized for biometric identification [32]–[35].

ECG signals consist of a series of positive and negative waves. Signals captured from each lead provide different information. In a single heartbeat cycle, there are particular waves called P, QRS and T that can be recognized using different leads for measurement. The first peak, the P wave, is a small upward wave, which specifies atrial depolarization. Approximately 160 ms after the onset of the P wave, the QRS wave is produced by ventricle depolarization. The ventricular T wave in the ECG indicates the stage of re-polarization of the ventricles. A significant modification concerning the ECG anatomy occurs from birth to adolescence, that is, during the first 16 years of life [36]. According to the study presented in [36], the amplitude of the P wave does not change considerably while the amplitudes of the S and R waves reduce from childhood to adolescence. A progressive modification of the T wave from childhood to adolescence has also been stated by Dickinson [37]. 48 In addition, the QT interval will shorten much more than the rest of the intervals when the heart rate increases. This change can be corrected by normalizing the QT interval according to the heart rate. The dependence of the QT interval to heart rate can be adjusted utilizing Bazett's QT interval correction for which the corrected QT interval is found to be somewhat constant over the years [38]. It should be mentioned that for simplicity, we have not considered QT interval correction/normalization in this article. Aging does not affect any gender-based variances in cardiac electrophysiological properties in adolescents. However, stress, anxiety, and physical exercise can change the Heart Rate Variability (HRV) and morphology [36].

IV. GENERATING CRYPTOGRAPHIC KEYS UTILIZING ECG BIO-ELECTRICAL SIGNAL

Medical sensors rely on cryptographic keys to secure end-to-end communications or encrypt/decrypt messages that need to be conveyed between the sensors and health caregivers [17], [39]. Solutions based on cryptographic keys generated from individuals' ECG signals are best suited for tiny medical sensors as these solutions are lightweight and require low resources [8]. By developing robust and efficient cryptographic key generation approaches, the security of medical sensors can be offered in a plug-and-play manner where neither a network establishment nor a key pre-distribution mechanism is required. Cryptographic keys can be generated within the network on the fly via the usage of ECG data collected by medical sensors when and as needed. The generated keys can be employed, for example, in end-to-end communications to securely encrypt/decrypt patients' medical data being transferred between sensors and health caregivers [17], [39]. The keys can also be used for authentication and authorization of peers, confidentiality, and integrity of the conveyed messages in BSNs [40]–[42]. A robust cryptographic key generated within a BAN can also prevent probable attack scenarios including passive information gathering and message corruption, replay attacks and Denial of Service attacks (DoS), just to name a few.

As Fig. 1 presents, the first step to generate ECG-based cryptographic keys is raw ECG data acquisition from subjects. The collected ECG data include information about the heart rate, morphology, and rhythm being recorded by placing a set of electrodes on body surfaces such as neck, chest, legs, and arms. Once collected, raw ECG data needs to be prepared for further analysis. Analysis of the ECG signal can be split into two principal steps by functionality: ECG signal *pre-processing* and *feature extraction*.

A. ECG SIGNAL PRE-PROCESSING

The collected data from ECG signals normally contains noise. The noise has to be removed since the presence of noise makes the analysis and the classification of the data less accurate. Pre-processing suppresses or removes noise from an ECG signal by employing an appropriate filtering scheme. Hence, pre-processing is an essential task prior to extracting the features of an ECG signal.

B. ECG SIGNAL FEATURE EXTRACTION

ECG feature extraction is a procedure where the main features of a sample are extracted. The main objective of the ECG feature extraction process is to select and maintain relevant data of an original signal. Current ECG feature extraction methods are classified into two major classes, fiducial methods and non-fiducial methods. In fiducial methods, points of interest including P, Q, R, S, and T within a single heartbeat waveform (i.e., local minima or maxima or amplitude difference between consecutive fiducial points) are used. Algorithms based on non-fiducial points do not utilize peculiar points to generate the feature set. Non-fiducial methods extract discriminative data from an ECG signal without having to concentrate on fiducial points. They are prone to a high dimension feature space, which in turn propagates the computational overhead and requires more information for trainings that are practically unbounded [43]. High dimensional information may include irrelevant and superfluous data that can degrade the performance of the classifier. In this

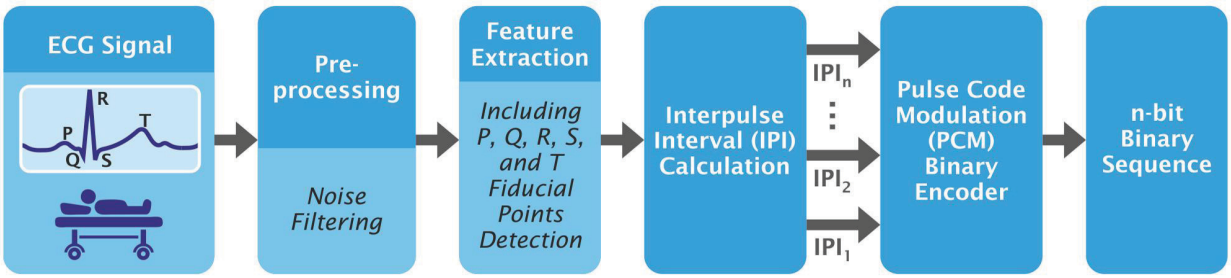

FIGURE 1. Block diagram of ECG signal analysis and *n*-bit binary sequence generation using consecutive IPI sequences.

article, a fiducial-based algorithm is employed to perform the ECG feature extraction task. In particular, Discrete Wavelet Transform (DWT) is utilized to extract the required features of individuals' ECG signal.

The DWT is a prevalent technique for frequency and time analysis. Wavelet transformation is a linear function which decomposes a signal into components at different resolutions (or scales). Let $\psi(t)$ be a real (or complex valued function) $\in L^2(R)$. The $\psi(t)$ function can be considered as a wavelet, if and only if, its Fourier transform $\hat{\psi}(\omega)$ satisfies the following equation [43]:

$$\int_{-\infty}^{\infty}\left(\frac{|\hat{\psi}(\omega)|^2}{|\omega|}\right) = F_{\psi} < \infty \tag{1}$$

This tolerability clause implies that:

$$\int_{-\infty}^{\infty}\psi(t)dt = 0 \tag{2}$$

This means that $\psi(t)$ is oscillatory which its area is equal to zero. Let $\psi_x(t)$:

$$\psi_x(t) = \frac{1}{\sqrt{x}}\psi\left(\frac{t}{x}\right) \tag{3}$$

be the dilation of $\psi(t)$ by a scale factor of $x > 0$. In the above expression, $\frac{1}{\sqrt{x}}$ is utilized for energy normalization. Wavelet transform utilizes a series of small wavelets with confined duration in order to decompose a signal. Therefore, the wavelet transform of a function $f(t) \in L^2(R)$ at scale x and position l can be written as:

$$W_f(x,l) = \frac{1}{\sqrt{x}}\int_{-\infty}^{\infty} f(t)\psi^*\left(\frac{t-l}{x}\right)dt \tag{4}$$

where x is the scale factor, l is the translation of $\psi(t)$ and * denotes the complex conjugate of $\psi(t)$.

The non-stationary nature of ECG signals allows one to extend principal functions produced by shifting and scaling of a single prototype function denoted as the mother wavelet. Various wavelet families including Haar and Daubechies exist in the literature and have been broadly utilized for the ECG feature extraction. Haar wavelet is the simplest form of wavelets. Haar wavelet is simple to understand and easy to compute, while some detailed information cannot be captured using it. Daubechies wavelet is theoretically more complex than Haar and has higher computational overhead. But it is more reliable as it can capture details that are missed by the Haar wavelet [28].

In this article, the Daubechies wavelet transform is used for the ECG feature extraction due to the higher reliability it offers. More specifically, Daubechies DB4 wavelet is chosen due to the resemblance of its scaling function to the shape of ECG signals [44]. R peak detection is the core of the Daubechies DB4 wavelet feature extraction where the other fiducial points are extracted with respect to the location of the R peak points. DB4 has four wavelet and scaling function coefficients. Each step of the wavelet transform uses the *wavelet function* to the input data. If the main dataset has N values, the wavelet function needs to be applied in order to calculate $N/2$ differences which reflect change in the data. In the ordered wavelet transform, the wavelet values are saved in the upper half of the N element input vector. The scaling and wavelet functions are computed by taking the inner output of the coefficients and four data values. The scaling function coefficients (h) and the wavelet function coefficient (g) values can be written as:

$$\begin{aligned} h_0 &= \frac{1+\sqrt{3}}{4\sqrt{2}} = -g_3 \qquad h_1 = \frac{3+\sqrt{3}}{4\sqrt{2}} = g2 \\ h_2 &= \frac{3-\sqrt{3}}{4\sqrt{2}} = -g_1 \qquad h_3 = \frac{1-\sqrt{3}}{4\sqrt{2}} = g_0 \end{aligned} \tag{5}$$

Daubechies DB4 scaling (a) and wavelet (c) functions can be denoted as:

$$\begin{aligned} a_i &= h_0 S_{2i} + h_1 S_{2i+1} + h_2 S_{2i+2} + h_3 S_{2i+3} \\ c_i &= g_0 S_{2i} + g_1 S_{2i+1} + g_2 S_{2i+2} + g_3 S_{2i+3} \end{aligned} \tag{6}$$

Each iteration in DB4 step computes a scaling function value and a wavelet function value. The index i is incremented by two with each iteration, and new scaling and wavelet function values are computed. It should be mentioned that a normal ECG signal consists of observable P waves, QRS complex and T waves (See Fig. 2). In a normal sinus rhythm, the heart rate for an adult ranges between 60-100 beats per minute. All the main intervals on such an ECG recording are also within normal ranges. Nevertheless, cardiac abnormalities may also be observed in various datasets. These abnormalities usually occurs when patients are suffering from specific cardiovascular diseases, such as myocardial infraction, super vascular arrhythmia, malignant ventricular arrhythmia, and

other dangerous types of arrhythmia. Even normal subjects' ECG signals may have some variations due to anxiety, stress, and physical exercises. In these scenarios, the peak values of some waves may not be detectable within one heartbeat using the most common order of the Daubechies wavelet, that is DB4. Hence, the intended main ECG features cannot be extracted and computed. In such scenarios, it is found that DB6 and DB9 are the best candidates among different Daubechies scales to extract features from abnormal types of ECG signals [28], [45]. This is because these Daubechies scales keep certain details and squaring of the remaining signal approximation which result in reliable detection of the R peak points. Once the R peak points of an abnormal ECG signal are detected (using the aforementioned DB scales), other main peak values can be detected with respect to the position of R. Based on the above discussion, the optimum choice of the DB scales relies on the application and the type of ECG signals need to be used. This means that if some of the main features of an ECG signal cannot be extracted by one order of the Daubechies wavelet transform, another scale may provide more detail and accurate results. Thus, there will be low chance that the efficiency of the ECG-based cryptographic key generation approaches is affected. It should be also mentioned accuracy and reliability is more efficient with the higher Daubechies scales. While, the higher Daubechies scales require more coefficients as well as processing time.

1) QRS COMPLEX AND R PEAK DETECTION

The detection of the R peak is the first step of feature extraction. In an ECG signal, the R peak has the highest amplitude among all waves. The QRS complex detection involves specifying the R peak of the heartbeat. Most of the energy of the QRS complex lies between 3-40 Hz and the detection of the QRS complex relies on modulus maxima of the Wavelet Transform. This is due to the fact that modulus maxima and zero crossings of the Wavelet Transform correspond to the sharp edges of an ECG signal. The QRS complex generates two modulus maxima with opposite signs having a zero crossing between them. In a normal ECG signal, the Q and S points occur about 0.1 second before and after the occurrence of the R peaks, respectively. The left point denotes as the Q point and the right point denotes the S point. The QRS width can also be computed from the onset and the offset of the QRS complex. The onset can be defined as the beginning of the Q wave and the offset can be defined as the ending of the S wave.

2) P AND T PEAKS DETECTION

The P wave generally comprises of modulus maxima pair with opposite signs. The T wave also has similar characteristics to the P wave. For the P and the T peak detections, the lower and higher frequency ripples of the signal need to be removed. To detect the P wave, this pair needs to be searched within a window prior to the onset of the QRS complex. The search window starts at about 200 ms before the onset of the QRS complex and ends after the onset of the QRS complex. The zero crossing among the modulus maxima pair corresponds to the peak points of the P wave. The extremum of the signal after the zero crossings of each R peak is denoted as T.

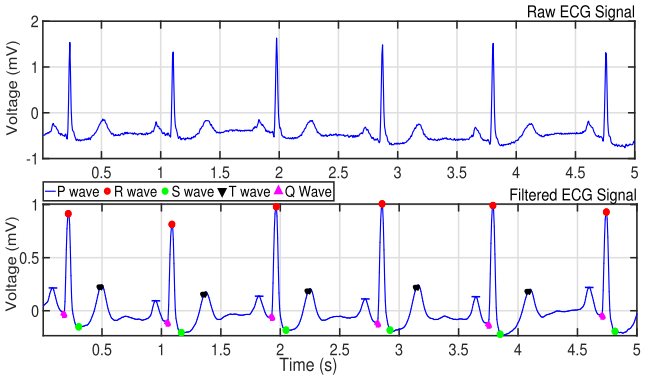

FIGURE 2. An ideal raw ECG signal and the filtered ECG signal with the main fiducial points indicated.

3) PR, RR, PP, QT, AND ST INTERVALS

The PR interval is specified as the interval between the onset of the P wave and the onset of the R wave. The RR interval is defined as the time elapsed between the adjacent R peaks. Heartrate can be calculated as the reciprocal of the RR interval, that is, the time difference between two R peak points. The PP interval is specified as the interval between the adjacent P waves due to atrial depolarization. The PP interval is utilized to calculate the atrial rate. The ST interval is denoted as the interval between the offset of the S-wave and offset of the T-wave. The QT interval is computed by finding the difference between the onset of the Q wave and the offset of the T wave. These intervals are utilized as the main ECG features in this article.

In [17], we presented two different ECG-based cryptographic key generation approaches which use singular ECG feature, that is IPI. Our first approach, IPI-PRNG, relied on a pseudo-random number generator and consecutive IPI sequences. The second approach, IPI-AES, relied upon the AES block cipher in counter mode, using IPI as the seed generator for the AES algorithm. It should be noted that, more explanations and details regarding our IPI-PRNG and IPI-AES approaches can be found in [17]. The following section presents our proposed cryptographic key generation utilizing several ECG features. The proposed approach extends our previous work by reducing the key generation execution times yet providing high security levels. Our proposal is motivated by the fact that to alleviate the key generation execution times, while preserving high security levels, other main features of an ECG signal in addition to IPI can be exploited.

C. GENERATING CRYPTOGRAPHIC KEYS UTILIZING SEVERAL ECG FEATURES (SEF)

In this section, we present a new cryptographic key generation approach, called *SEF*, which employs other main features of an ECG signal rather than using just singleton IPI.

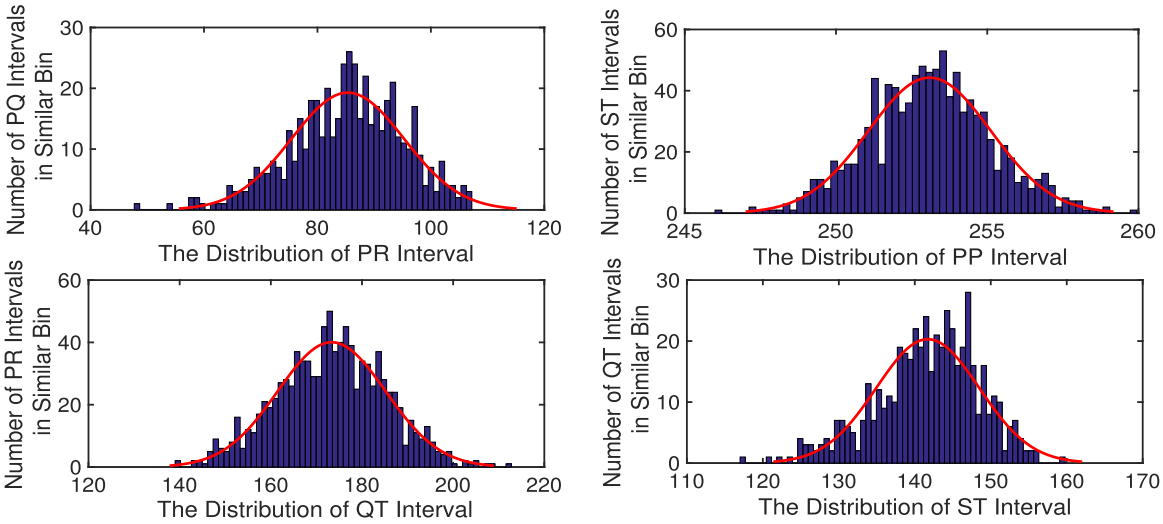

FIGURE 3. The normal distribution of PR, PP, QT, and ST intervals.

We describe and justify in more detail the selected features to be used along with the IPI feature of the ECG signal for generating cryptographic keys.

The SEF cryptographic key generation approach uses all of the main ECG features from one heartbeat cycle. The utilized features are PR, RR (also known as IPI), PP, QT and ST. The major reason to use such features is that P, Q, R, S and T waves are noticeable within an ECG signal rhythm for which PR, RR, PP, QT and ST intervals are known as the main and normal components of an ECG waveform [6]. In cardiology, the PR interval is the period which extends from the beginning of the onset of atrial depolarization (P wave) until the beginning of the onset of ventricular depolarization (the QRS complex). The PR interval is normally between 120 to 200 ms in duration. The PP interval is the distance between consecutive P waves due to atrial depolarization. The PP interval is utilized to calculate the atrial rate. In a normal ECG signal, the PP interval and the RR interval are equivalent. Thus, atrial rates and ventricular rates are not independently separated.

In an abnormal ECG signal, for example, when there is an atrioventricular dissociation due to complete heart block, the atrial rate is different from the ventricular rate. This causes for the PP interval to be shorter than the RR interval, meaning that atrial rate is greater than the ventricular rate. The normal PP interval is more than 180-190 ms in duration [6]. The QT interval is measured as the time between the initiation of the Q wave and the termination of the T wave in the heart's electrical cycle. The QT interval demonstrates electrical re-polarization and depolarization of the ventricles. The QT interval is an important feature of the ECG in a sense that it is a marker for the potential of ventricular tachyarrhythmias as well as a risk factor for sudden death. Similar to the RR interval, the QT interval relies on the heart rate. This means that the faster the heart rate, the shorter the RR and QT intervals. This variation can be corrected by normalizing the QT interval according to the heart rate. It should be mentioned that, specifying whether or not the QT interval is normal is not totally a straightforward task as the duration differs according to the patient's heart rate. To allow for this, the corrected QT interval (QTc) must be calculated using Bazett's equation [38]:

$$QTc = \frac{QT}{\sqrt{RR}} \tag{7}$$

where QT is the measured QT interval, QTc is the corrected QT interval, and RR is the computed RR interval. The normal corrected QT interval is below 0.46 for women and below 0.45 for men. In this article, for the sake of simplicity, we have not considered the QT interval correction presented above. Finally, the ST segment specifies the time that ventricles pump the blood to the lungs and the body. The ST segment connects the QRS complex and the T wave which also serve as the base-line from which to measure the amplitudes of the other waveforms. The normal ST segment has a duration of 80-120 ms. In [17], we presented that the fluctuation of the RR interval fits into the normal distribution which indicates the randomness of RR intervals. This finding was also supported by our measurement of entropy, the NIST benchmark, and the Chi-square test presented in [4] and [7]. Likewise, in this section, we show that the distributions of PR, PP, QT and ST intervals also fit into the normal distribution. Thus, these features can be utilized along with RR interval for ECG-based cryptographic key generations. The feasibility of using the PR, PP, QT, and ST intervals is based on the fact that all these features should also fulfill the property of randomness. We examined this property by collecting 30 seconds ECG data of different subjects obtained from the Physiobank database [46]. From the collected ECG data, we have computed all of the consecutive ECG features and plotted their histograms. As can be seen from Figure 3, similar to the RR interval, the distribution of PR, PP, QT and ST intervals also fit into the normal distribution. Hence, these additional main ECG features also fulfill the property

of randomness. This is an essential property to ensure that the cryptographic keys which are generated from these ECG intervals are random. Moreover, in [17], we extracted a fixed number of 8 bits from each IPI. This was done using a Pulse Code Modulation (PCM) [47] binary encoder. PCM is a digital interpretation of an analog signal which takes samples of the amplitude of the analog signal at certain intervals. The sampled analog data then is quantized and represented as a digital n-bit binary number. Bit 1, most significant bits, is the first bit that specifies the polarity of the sample. Bit "0" represents negative polarity and bit "1" represents positive polarity. Bits 2, 3, and 4 reveal the segment where the sample data is placed. Bits 5, 6, 7, and 8, least significant bits, define the quantized value of the sample inside one of the segments.

In this article, we enhance our approach by using a dynamic technique which can specify the optimized number of bits that can be extracted from each ECG feature. In this regard, our comprehensive analyses have revealed that the alteration range of each ECG feature differs whitin each dataset. This is due to the fact that each ECG feature offers different Standard Deviations (SDs) and mean values. These variations are visible for the PR, PP, QT, and ST features as shown in Figure 3. As a result, extracting a fixed number of bits (e.g., 8 bits) per ECG feature is not an efficient and optimum solution. Therefore, an efficient technique is required where the number of binary values per ECG feature can be extracted as optimum as possible while considering the variation range of SDs and mean values per ECG feature. Based on the discussion above, we utilize a dynamic technique in order to specify the optimized number of bits which need to be extracted from each ECG feature. The used technique enables to extract optimal binary values and ensures the randomness property as the binary sequences are produced based on the real-time variation of the measured ECG signal [27]. The utilized technique to determine the number of optimum bits (M) can be defined as:

$$\mu(FX_i) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$SD(FX_i) = \sigma(FX_i) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \tag{9}$$

$$C_v = \frac{\sigma(FX_i)}{\mu(FX_i)} \tag{10}$$

$$M = \lceil \frac{\ln(\sigma(FX_i))}{\ln(2)} \rceil + \lceil C_v \rceil \tag{11}$$

where FX_i represents a set of any one of the PR, PP, QT, and ST features from one sampled ECG dataset in the i_th heartbeat, x_i represents each value in the dataset, μ is the mean value of the dataset, Σ is the summation, N is defined as the number of values in the dataset, σ indicates the standard deviation of a dataset, and C_v is the coefficient of variation which is defined as the ratio of the standard deviation to the mean value. The main reason to use the ln function in the equation (14) is that from the information theory point of view, ln provides a solution for determining the number of optimal bits needed in a code (even when the code is not known). Since the SD and mean values of each main feature within one ECG dataset are different, the number of extracted optimum bits vary accordingly. In the j_{th} heartbeat, the efficient number of binary bits B_{opt} that can be extracted efficiently from one ECG feature can be defined as:

$$B_{opt} = GET\_BITS\_FROM\_F_{LSB}(FX_j, lsb, M) \tag{12}$$

F_{LSB} is a function which extracts M bits from Least Significant Bits (LSB) of its input FX_i. By exploiting the aforementioned technique, optimum binary values can be extracted from the required main ECG features per heartbeat cycle. The extracted binary values per heartbeat cycle then need to be concatenated to form an m-bit binary sequence. Finally, to generate an n-bit sequence using the SEF approach, binary sequences which are produced from k consecutive heartbeats are required to be concatenated.

Our study also reveals that the variation range of all of the main ECG features differs in different ECG datasets. To give an example, the number of optimum binary values which can be extracted from the PR feature of Normal Sinus dataset is not identical to the number of the binary values which can be extracted from PR feature of the European ST-T dataset. Table 1 presents the results of different subject groups which we have investigated for this purpose. We have selected 10 of the most-known ECG recording and cardiovascular disease datasets from the open source Physiobank database [46]. In this regard, from each of the following 10 datasets, 5 subjects are randomly chosen for this study. The last dataset, that is, the motion artifact ECG, includes short duration ECG signals recorded from one healthy 25-year-old male performing different physical activities. The selected datasets are: (i) Motion Artifact Contaminated ECG Database, sampled at 500 Hz per second with 16-bits resolution, (ii) Super Vascular Arrhythmia (Arrhyth.) sampled at 125 Hz, (iii) Malignant Ventricular Arrhyth. sampled at 250 Hz, (iv) MIT-BIH Long-Term sampled at 360 Hz, (v) Atrial Fibrillation sampled at 250 Hz, (vi) MIT-BIH Arrhyth. sampled at 360 Hz, (vii) Myocardial Infraction sampled at 125 Hz, (viii) MIT-BIH Noise Stress sampled at 360 Hz, (viiii) European ST-T Database sampled at 250 Hz, and (x) Normal Sinus sampled at 128 Hz. The main motivation to select these datasets is the fact that they are among the most recognized ECG recordings and prevalent cardiovascular diseases according to Physiobank [46]. Moreover, no recognizable ECG recording nor a specific patient having one of these cardiovascular diseases is found among each dataset. Thus, any bias that can help in the identification of a specific subject cannot be found. It should be also mentioned that in a motion artifact contaminated ECG database, there is no other information than the subject's age and gender available. Our experiments to extract the ideal number of binary values from all of the main ECG features of each ECG dataset are presented in Table 1. As can be deduced from our measurements, the optimum number of binary values which can be extracted

TABLE 1. Optimum binary sequences produced from main general features of ECG signals of subjects with different heart health conditions.

ECG Dataset	Binary Value Extracted Per ECG Feature (bit)					Total Binary Values Extracted from One Heartbeat Cycle (bit)
	PR	RR	PP	QT	ST	
Motion Artifact ECG	2	4	4	4	2	16
Super Vascular Arrhyth.	2	3	4	3	2	14
Malignant Ventricular Arrhyth.	2	3	3	2	3	13
MIT-BIH Long-Term	2	4	4	3	3	16
Atrial Fibrillation	2	3	4	3	3	15
MIT-BIH Arrhyth.	3	4	4	3	2	16
Myocardial Infraction	3	3	3	3	2	14
MIT-BIH Noise Stress	2	3	4	3	2	14
European ST-T	3	3	4	3	2	15
MIT-BIH Normal Sinus	2	4	4	3	3	16

from various features of one ECG dataset totally differs from one dataset to another. This is due to the utilization of the aforementioned technique (where the optimum number of bits can be extracted from each main ECG feature) instead of a fixed number of bits representation since each feature of the ECG has different mean and SD values.

According to the above discussion, in the SEF key generation approach, depending on the length of the cryptographic key n that needs to be generated, approximately $\lceil \frac{n}{16} \rceil$ consecutive ECG heartbeat cycles need to be detected. From the detected heatbeats, all of the main ECG features (PR, RR, PP, QT and ST) from a t-second segment of a patient's ECG data need to be computed. To achieve this goal, the following tasks are required to be performed: (i) for a specified period of time t, the main fiducial points or peaks of a sensed ECG signal (P, Q, R, S, and T) should be extracted utilizing a generic feature extraction function, (ii) from the detected fiducial points, the required x consecutive ECG features (PR_1, RR_1, PP_1, QT_1, ST_1), (PR_2, RR_2, PP_2, QT_2, ST_2), ..., (PR_x, RR_x, PP_x, QT_x, ST_x) should be computed, (iii) from the computed main ECG features, the amount of optimum binary values per ECG feature needs to be calculated. This should be done using an equation where the ideal binary values per ECG feature, that is $m_1, m_2, \ldots, m_x$, will be selected based on their mean values and SDs, and (iv) the generated m_i-bit binary sequences from each ECG feature then need to be concatenated in order to form an n-bit binary sequence. The generated n-bit binary sequence is considered as the main cryptographic key generated using this approach. It should be mentioned that the produced n-bit binary sequence using the SEF approach underlays the SEF-PRNG and SEF-AES approaches presented in the following sections.

1) STRENGTHENING SEVERAL ECG FEATURE-BASED KEY GENERATION THROUGH PRNG (SEF-PRNG)

Similar to the IPI-PRNG, the SEF-PRNG approach also consists of two main phases: (i) generating an n-bit binary sequence from each subject's ECG data. To do this, as discussed previously, about $\lceil \frac{n}{16} \rceil$ heartbeat cycles of a patient's ECG data needs to be collected. From the collected data, consecutive PR, RR, PP, QT, and ST features each of which encoded into its optimum x-bit binary value (using the previously mentioned technique) need to be computed. After that, the aforementioned steps in SEF approach need to be performed in such a way that for each subject, an n-bit binary sequence is generated. (ii) a Pseudo Random Number Generator (PRNG) is used to generate a random n-bit binary sequence. To generate a random n-bit binary sequence, the Fibonacci Linear Feedback Shift Register (LFSR) is employed. We have utilized the Fibonacci LFSR function of MATLAB similarly as we did in the IPI-PRNG approach to produce a random n-bit binary sequence. Once the n-bit random binary sequence is generated (using the Fibonacci LFSR function), the main cryptographic key can be generated. If SEF_n is the n-bit binary sequence generated from ECG and and $FLFSR_n$ is the n-bit random binary sequence generated using the Fibonacci LFSR, the main n-bit cryptographic key is produced by XORing the outputs of phases (i) and (ii).

2) STRENGTHENING SEVERAL ECG FEATURE-BASED KEY GENERATION THROUGH AES (SEF-AES)

Similarly as IPI-AES, the SEF-AES approach also uses the AES [19] block cipher in counter mode as the cryptographic pseudo-random number generator to generate n-bit cryptographic keys. In SEF-AES, to generate an n-bit cryptographic key, two n-bit binary sequences need to be generated as the main seeds of the AES algorithm. The first seed is considered as input data (plaintext) of the AES and the second one is considered as the encryption/decryption key. To generate these two seeds, we exploit the SEF key generation approach as the seed generator. To do this, $\lceil \frac{n}{8} \rceil$ consecutive heartbeat cycles of a patient's ECG signal need to be collected. From the collected data, consecutive PR, RR, PP, QT and ST features are encoded into their optimum x-bit binary values The produced x-bit binary sequences from each heartbeat cycle further need to be concatenated to form a $2n$-bit binary sequence. After that, the $2n$-bit binary sequence needs be divided into two n-bit binary sequences. The first sequence is used as the input data (plaintext) and the second one is used as the AES encryption key. At the final stage, the output of the AES-n algorithm (ciphertext) is considered as the main n-bit cryptographic key generated utilizing the subjects' ECG signals.

V. EXPERIMENTS AND RESULTS

In this section, we assess the security level and performance of our proposed ECG-based cryptographic key generation approaches in terms of distinctiveness, test of randomness, temporal variance, and key generation execution time. We conduct our experiments on both normal and abnormal ECG signals obtained from the publicly available and widely used database, that is, Physiobank [46]. PhysioBank comprises of databases of multi-parameter neural, cardiopulmonary, and other biomedical signals from patients and healthy subjects with a variety of conditions including sudden cardiac death, irregular heartbeat (arrhythmia), congestive

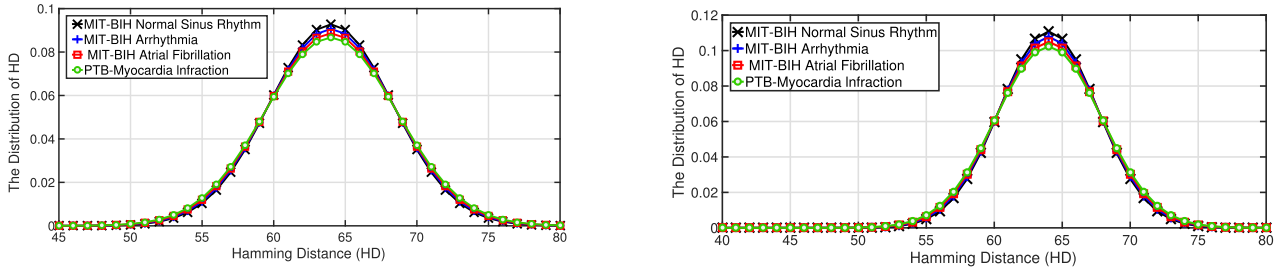

FIGURE 4. The distribution of hamming distance of any two 128-bit cryptographic keys generated using IPI-AES and SEF-AES approaches for subjects with different heart health conditions. (a) The distribution of hamming distance between any two 128-bit cryptographic keys generated using IPI-AES approach for subjects with different heart health conditions. (b) The distribution of hamming distance between any two 128-bit cryptographic keys generated using SEF-AES approach for subjects with different heart health conditions.

heart failure, sleep apnea, and epilepsy. Our experiments are carried out on both normal and abnormal ECG signals which are obtained from 239 subjects studied by the Beth Israel Hospital Laboratory in Boston and Physikalisch-Technische Bundesanstalt (PTB), the National Metrology Institute of Germany. The employed ECG signals include: (i) ECG signals of of 18 subjects (5 men, aged 26 to 45, and 13 women, aged 20 to 50) with Normal Sinus Rhythm. The recordings are digitized at 128 samples per second with resolution over a 10 mV range. (ii) ECG signals of 48 subjects with Arrhythmia (22 women of age 23 to 89 and 26 men of age 32 to 89) which they were recorded by a two-channel ambulatory ECG system. The recordings are digitized at 360 samples per second with 11-bit resolution over a 10 mV range per patient. (iii) ECG signals of 25 subjects with Atrial Fibrillation. The individual recordings are each 10 hours in duration, and contain two ECG signals each digitized at 250 samples per second with 12-bit resolution over a range of 10 mV. (iv) ECG signals of 148 subjects with Myocardial Infraction (89 men aged 17 to 87 and 59 women aged 19 to 83). Each signal is digitized at 1000 samples per second, with 16 bit resolution over a range of 16 mV. We have captured 100 different samples of 5 minute long ECG data for each subject and evaluated the efficiency of our approach in terms of distinctiveness, test of randomness and temporal variance. The collected ECG signals are filtered using a low-pass filter with a 30 Hz threshold frequency. Such a filter reduces the environmental noise and provides a smoother signal for further analysis. For our experiment, we have generated 128-bit cryptographic keys using the aforementioned approaches. We have implemented and analyzed our key generation approaches utilizing MATLAB [48].

A. DISTINCTIVENESS

The first experiment is to determine whether the cryptographic keys generated utilizing the presented approaches are distinctive for different individuals. Distinctiveness indicates that the generated keys should be significantly different for different subjects, at any given time. Hamming Distance (HD) is utilized as the main metric in order to evaluate the difference between any two cryptographic keys of equal length. For two sufficiently long binary sequences, the distribution of HD should be centered at half of the length of the binary sequences. This indicates that these sequences are randomly generated [5]. The reason is that any bit of a random binary number should have equivalent probability to be zero or one. Hence, the average of HD of a sufficiently large and random set of n-bit binary sequences is anticipated to be about $n/2$, provided that the binary sequence is distinctive. For two different bits, i and j, which are extracted from the same position of two independently generated cryptographic keys (K), the probability $P(K_i, K_j)$ can be represented as [5]:

$$P(K_i, K_j) = 0.25 \quad K_i = 1, 0 \;\&\; K_j = 1, 0 \tag{13}$$

$$HD_d = \sum_{P_1 \neq P_2} \frac{(\mid ECG_{i,P_1} - ECG_{i,P_2} \mid)}{\mid sig \mid^2} \tag{14}$$

To evaluate the distinctiveness of different keys generated using the presented approaches, we use the average Hamming Distance metric, as defined in Equation (17).

HD_d is the computed Hamming Distance between the cryptographic keys generated using ECG signals of different subjects, $\mid sig \mid$ is the length of the used physiological signal set, i defines the ECG index, and P_1 and P_2 defines the patient's indexes. We have investigated the distinctiveness of the cryptographic keys generated utilizing our SEF, IPI-PRNG, IPI-AES, SEF-PRNG, and SEF-AES approaches and compared the results with the conventional IPI approach. We have sampled the ECG signals of each subject over 100 random start-times. The average HD between the cryptographic keys of the two different subjects generated at the same start-time is then calculated.

The HDs between different subjects' cryptographic keys are calculated (See Figures 4a and 4b). The results of our distinctiveness calculations show that the average HD between the cryptographic keys generated from the ECG signals of two different subjects using IPI, SEF, IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES are 47.76% ($\approx$ 62 bits), 48.13% ($\approx$ 62 bits), 49.09% ($\approx$ 63 bits), 49.41% ($\approx$ 63 bits), 49.84% ($\approx$ 64 bits), and 49.93% ($\approx$ 64 bits), respectively.

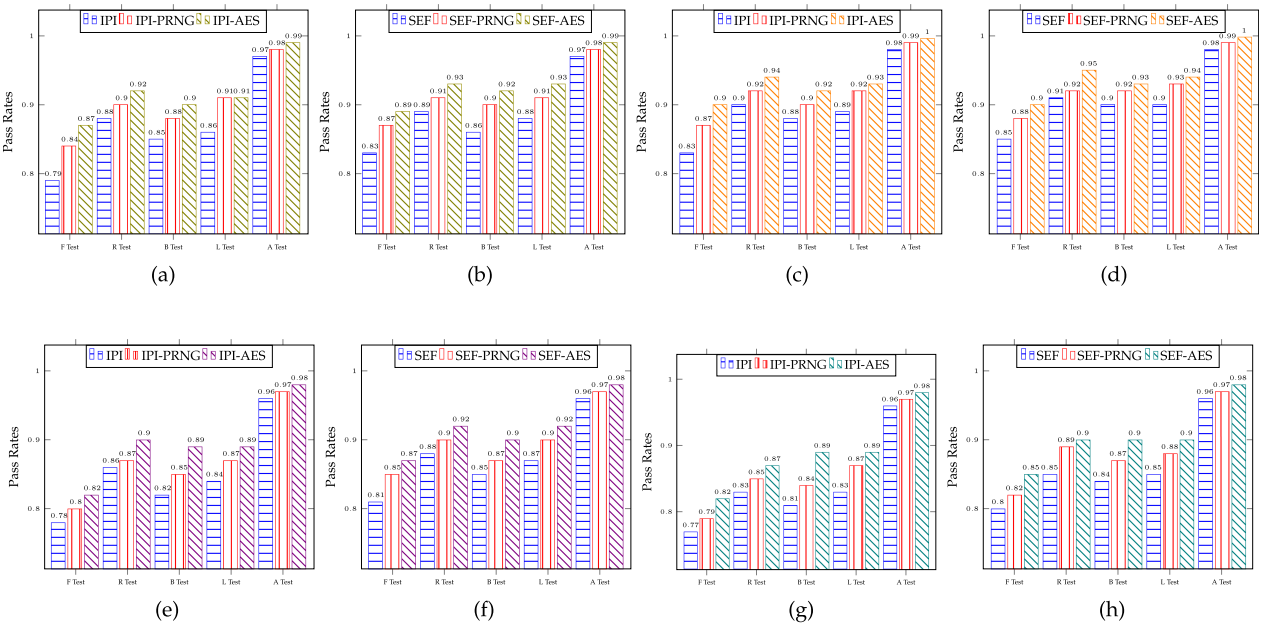

FIGURE 5. NIST pass rate comparison of different ECG-based cryptographic key generation approaches for subjects with different heart health conditions. (a) NIST Tests, MIT-BIH Arrhythmia. (b) NIST Tests, MIT-BIH Arrhythmia. (c) NIST Tests, MIT-BIH Normal Sinus Rhythm. (d) NIST Tests, MIT-BIH Normal Sinus Rhythm. (e) NIST Tests, MIT-BIH Atrial Fibrillation. (f) NIST Tests, MIT-BIH Atrial Fibrillation. (g) NIST Tests, PTB-Myocardial Infarction. (h) NIST Tests, PTB-Myocardial Infarction.

B. TEST OF RANDOMNESS

Generating distinctive and long keys is not sufficient as it is also necessary to ensure that the keys are sufficiently random and cannot be predicted easily. Randomness is related to Shannon entropy. Entropy is a measure of uncertainty for many cryptographic purposes. The Shannon entropy equation can be written as [49]:

$$H(r) = -\sum_{i=1}^{n} P(ECG_i) \log_2 P(ECG_i) \tag{15}$$

r is an information source with n mutually exclusive events, $P(ECG_i)$ is the probability of the ith event. According to this evaluation metric, the randomness level of a binary sequence increases when $H(r)$ closes to 1.

We have evaluated the randomness of the 128-bit cryptographic keys generated using the SEF, IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES approaches. Then, we have compared our results with the conventional IPI approach. The randomness of the generated keys is evaluated from two perspectives: (i) Shannon entropy and (ii) the pass rates of the NIST statistical benchmark. To evaluate randomness from the Shannon entropy point of view, we have computed the entropy of the keys generated from each subject's ECG signal over 100 random start-times using IPI, SEF IPI-PRNG, SEF-PRNG, IPI-AES, and SEF-AES approaches. The randomness of the generated cryptographic keys are also evaluated using the NIST benchmark. The NIST benchmark is developed for cryptographic random and pseudo-random number generator applications. The results of the NIST statistical tests are pass rates (also called P-values) which indicate the probability of randomness of the generated cryptographic keys. If a P-value is less than the threshold, that is, 1% the randomness hypothesis fails.

Five main tests proposed by NIST for evaluating randomness are utilized in this article. They are the frequency test (F-Test), the runs test (R-Test), the frequency test within a block (B-Test) and the test for the longest run of ones in a block (L-Test). Description of the above-mentioned tests can be found in more detail in [26] and they are briefly summarized as follows: (i) The F-Test specifies whether the number of 0s and 1s in the input sequence are approximately the same as would be anticipated for a real random sequence. (ii) The R-Test specifies if the number of runs of 0s and 1s of different lengths is as anticipated for a random sequence. Run, refers to an uninterrupted sequence of identical bits. (iii) The B-Test specifies whether the frequency of 1s in an N-bit block is approximately $N/2$, as would be expected under an assumption of randomness. (iv) The L-Test specifies if the length of the longest run of 1s in the tested sequence is consistent with the length of the longest run of 1s that would be anticipated in a random sequence. (v) The A-Test compares the frequency of overlapping blocks of two adjacent lengths, that is, l and $l + 1$ versus the expected result for a random sequence.

As shown in Figures 5, in all approaches the entropy values as well as the NIST pass rates are close to 1 signifying that the distribution of 0s and 1s in the generated keys among the 6 approaches are quite uniform. In addition, we find out that the randomness of abnormal ECG signals is slightly worse than the normal ones. This is due to the fact that for some abnormal ECG signals their ECG feature patterns were

TABLE 2. Execution time comparison of different ECG-based key generation approaches to produce 128-bit cryptographic keys.

Processor	Execution Time, Single Iteration (ms)						Execution Time, Total (s)					
	IPI [4], [7]	IPI-PRNG	IPI-AES	SEF	SEF-PRNG	SEF-AES	IPI [4], [7]	IPI-PRNG	IPI-AES	SEF	SEF-PRNG	SEF-AES
ARM Cortex-M3	57.2	66.1	95.3	37.4	41	61.9	0.9	1.1	1.5	0.3	0.4	0.5
ATSAMD21G18A	169.2	192.7	238.1	103.1	131.9	172	2.7	3.1	4	0.9	1.1	1.3
Atmel ATmega128L	210.9	244.8	303	129.4	147.7	199.5	3.3	3.9	4.8	1.1	1.2	1.6
STM32F7	11.8	13.7	16.8	7.9	9.2	11.6	0.2	0.2	0.3	0.07	0.08	0.1
STM32F4	24.3	28.2	40.7	14.2	18.3	26.7	0.4	0.4	0.6	0.2	0.2	0.3
STM32F3	36.5	42.4	61.1	25	30.1	40.5	0.6	0.7	1	0.2	0.3	0.4
STM32L4	54.8	63.6	91.7	34.3	40.7	59.8	0.9	1	1.4	0.3	0.4	0.5
STM32F2	60.3	70.6	101.9	39.5	43.1	63.7	1	1.2	1.7	0.3	0.4	0.6
STM32F1	89.9	104.2	150.4	59.2	71.3	101	1.4	1.7	2.4	0.5	0.6	0.9
STM32F0	144.6	167.4	211.5	90.8	104.6	139.8	2.3	2.7	3.4	0.8	0.9	1.2
STM32L1	165.3	184.4	231.9	102.5	124.3	162.1	2.7	3	3.9	0.9	1	1.3
STM32L0	187.4	225.2	278.9	114.6	133.4	178.2	3	3.3	4.5	1	1.1	1.5

irregular and sometimes hard to be detected. Compared to the normal ECG signals, abnormal signals are more chaotic and have larger variation resulting in less reliable ECG features. For normal ECG signals, the IPI and SEF approaches have in average the entropy of about 0.98, the IPI-PRNG and SEF-PRNG approaches, have in average the entropy of about 0.99, and the IPI-AES and SEF-AES approaches offer the entropy of ~ 1. The results of the test of randomness revealed that there is no significant difference between the results of entropy nor the NIST pass rates of any two different cryptographic keys generated using the strengthened IPI-based and the SEF approaches. The cryptographic keys generated using the IPI-PRNG, SEF-PRNG, IPI-AES and SEF-AES approaches provide better randomness in terms of entropy as well as NIST pass rates compared to the IPI approach and the SEF approaches. We have found out that the cryptographic keys which are generated utilizing the strengthened ECG features (IPI or SEF) offer better results in terms of randomness, that is ~ 1 entropy, as well as in terms of NIST pass rates than just utilizing singleton ECG features. A high level of randomness prevents the cryptographic keys from being easily predicted by any malicious activity. As a result, cryptographic keys generated using our proposed approaches meet the design goal of randomness.

C. TEMPORAL VARIANCE

Being different for the same subject at different time intervals is another main requirement of a binary sequence to be used as a cryptographic key. Temporal variance measures the resemblance between two cryptographic keys that are generated using a bio-signal (i.e., the ECG signal in this context) of the same subject at different time intervals. The analysis of the temporal variance also indicates that medical data of one subject which is encrypted using a robust cryptographic key cannot be decrypted effortlessly using a non-real time ECG signal from the same subject.

We evaluated the temporal variance of different 128-bit cryptographic keys which are generated using the IPI, SEF, IPI-PRNG, SEF-PRNG, IPI-AES and SEF-AES approaches. This is to ensure that a new measurement of a subject's ECG will not lead to the same key. We have sampled ECG signals of each subject over 100 random start-times. The average HDs between the keys of the same subject generated at different start-times are then calculated. To compute temporal variance, the average HD between cryptographic keys that are generated utilizing the ECG signal of the same subject at different start-times is computed.

The HD equation being utilized for computing the temporal variance of the generated keys can be written as [5]:

$$HD_s = \sum_{P_1=P_2} \frac{(\mid ECG_{i,P_1}^{t_1} - ECG_{i,P_2}^{t_2} \mid)}{\binom{\mid sig \mid}{2}} \tag{16}$$

HD_s is the hamming distance computed between the cryptographic keys generated from the ECG signal of the same subject at different time intervals. t_1 and t_2 define different start-times.

The results of our experiment show that the average HD between the cryptographic keys which are generated via the ECG signal of the same subject at different time intervals using IPI, SEF, IPI-PRNG, SEF-PRNG, IPI-AES and SEF-AES are 47.71% ($\approx$ 62 bits), 48.02% ($\approx$ 62 bits), 48.96% ($\approx$ 63 bits), 49.33% ($\approx$ 63 bits), 49.79% ($\approx$ 64 bits), and 49.9% ($\approx$ 64 bits), respectively. Similar to the computed results presented in the distinctiveness section, when employing strengthened ECG features (either IPI-based or SEF approach), the distribution of HDs of any two binary sequences generated from the ECG signal of the same subject does not change significantly. The normalized distribution of HDs of two cryptographic keys that are generated using strengthened IPI-AES and SEF-AES approaches are centered at 64. Similarly, the normalized distribution of HDs of two cryptographic keys that are generated using strengthened IPI-PRNG and SEF-SEF approaches are centered at 63. For IPI and SEF approaches, the normalized distribution of HDs of two cryptographic keys are centered at 62. The main reason for such similarities between the HD results (with just negligible percentage differences) is due to the fact that our main goal is to alleviate the key generation execution time while preserving the achieved high security level in terms of temporal variance. The average HD between the cryptographic keys of the same subject generated using the IPI-PRNG,

SEF-PRNG, IPI-AES, and SEF-AES approaches present better results compared to the IPI and SEF approaches. This is because ECG feature based cryptographic key generation approaches which are strengthened using the PRNG and AES algorithms appear to better distinguish the same subject's cryptographic key. Particularly, ECG feature based cryptographic key generation approaches which are strengthened using the PRNG and AES algorithms can increase the security level of the generated keys as the correct keys cannot be easily obtained via a brute-force attack. Therefore, the cryptographic keys which are generated using our proposed approaches meet the design goal of temporal variance.

D. KEY GENERATION EXECUTION TIME

To investigate the feasibility and key generation execution overhead of our approaches compared to the conventional IPI approach, we have examined the execution time required to generate 128-bit ECG-based cryptography keys. For this purpose, we utilized different processors ranging from tiny micro-controllers (e.g., STM32L0 with 32 MHz operating frequency) to reasonably powerful embedded microprocessors (ARM Cortex-A7). The considered processors are widely used in different medical domains depending on the power-performance requirements. Our experiments are carried out on ECG recordings obtained from the mentioned MIT-BIH Arrhythmia dataset, sampled at 360 Hz.

Table 2 presents the computed key generation execution times of our IPI-PRNG, IPI-AES, SEF, SEF-PRNG, and SEF-AES approaches as well as the conventional IPI approach. The execution times are presented in both single iteration and total times. Single iteration execution time indicates the time required to produce an x-bit binary sequence from one heartbeat cycle. Total execution time means the sum of single iteration execution times until successive iterations of the operations yields the desired result, that is, generates the desired 128-bit ECG-based cryptographic keys. To give an example, considering a subject with the ECG heartrate of 60 bpm, the specific STM32L0 microcontroller requires about 187.4 ms, 225.2 ms and 278.9 ms execution times per iteration for the IPI, IPI-PRNG, and IPI-AES approaches, respectively. These are the times these three approaches require to produce an 8-bit binary sequence from one ECG heartbeat cycle. As discussed earlier, to generate 128-bit ECG-based cryptographic keys, it is required for IPI, IPI-PRNG and IPI-AES approaches to compute 16 heartbeat cycles from a subject's ECG signal. Thus, the total key generation execution times of IPI, IPI-PRNG, and IPI-AES approaches are computed as: $187.4 * 16 = 3$ (s), $225.2 * 16 = 3.3$ (s), and $278.9 * 16 = 4.5$ (s), respectively. The same microcontroller requires about 114.6 ms, 133.4 ms, and 178.2 ms execution times for the SEF, SEF-PRNG, and SEF-AES approaches to produce 16-bits binary sequences from one ECG heartbeat cycle. However, as presented earlier, to generate 128-bit ECG-based cryptographic keys, the SEF, SEF-PRNG and SEF-AES approaches need to compute 8 heartbeat cycles from a subject's ECG signal. As a result, the total key generation execution times of SEF, SEF-PRNG, and SEF-AES approaches are calculated as $114.6 * 8 = 1$ (s), $133.4 * 8 = 1.1$ (s), and $178.2 * 8 = 1.5$ (s), respectively, which are considerably lower than their counterparts. The key generation execution times of SEF, SEF-PRNG and SEF-AES are in average 1.8 times times faster than IPI, IPI-PRNG and IPI-AES approaches. This is due to the fact that in IPI, IPI-PRNG and IPI-AES in total 8 bits can be extracted from one ECG heartbeat cycle, while in SEF, SEF-PRNG and SEF-AES approaches in total 16 bits can be extracted from the same heartbeat cycle. Thus, by utilizing additional ECG features, the latency of ECG-based key generation approaches can be significantly reduced. As can be seen from the results of distinctiveness, test of randomness, temporal variance and execution time, there is a clear trade-off between execution time and security level for different approaches. the IPI-AES and SEF-AES approaches show higher security levels in comparison to the SEF, IPI-PRNG, SEF-PRNG and the conventional IPI approach. However, such a high security level increases the execution time on average by 41.2% and 38.8% compared to the IPI-based and the SEF approaches, respectively. In this context, the IPI-PRNG and SEF-PRNG better balance the trade-off as they offer a higher security level while imposing a much lower execution time overhead, that is, on average 12.3% and 9.6% compared to the IPI-based and the SEF approaches, respectively. It should be mentioned that the efficiency of the proposed approaches highly depends on the application domain in which the approaches are utilized. As generating keys is performed in an on-demand way and not in every message transaction, the delay imposed by it might be more tolerable for some applications compared to others. Therefore, the IPI-AES and SEF-AES approaches can be a better alternative for applications where high security level is demanded and the latency can be tolerated. Another observation which can be made from Table 2 is the significant difference in execution time for different processors. This is mainly due to the difference in the processing power and memory available for each processor. This can guide designers and developers to adjust their demanded security level with the available processing power or vice versa.

VI. CONCLUSIONS

We presented a low-latency approach for generating secure ECG feature based cryptographic keys. Most existing key generation approaches are not directly applicable to BANs. The reason is that sensors used in BANs are extremely resource-constrained and demand a low-latency key generation time as well as a high security level. To alleviate these limitations, we proposed a robust key generation approach employing several ECG features, called SEF. Our SEF approach utilizes 4 main reference-free ECG features comprising of PR, RR, PP, QT, and ST. A dynamic technique is used to specify the optimum number of bits that can be extracted from each main ECG feature. We consolidated and strengthened the SEF approach with cryptographically secure pseudo-random number generator techniques. The Fibonacci

linear feedback shift register and the AES algorithm are implemented as pseudo-random generators to enhance the security level of our approach. The security evaluation of the generated keys was made in terms of distinctiveness, test of randomness, temporal variance, as well as using the NIST benchmark. Our approach is applied to normal and abnormal ECG signals. The analyses showed that the strengthened key generation approach offers a higher security level in comparison to existing approaches which rely only on singleton ECG features. Our analyses also reveal that the normal ECG signals have slightly better randomness compared to the abnormal ones. Cryptographic keys which are generated from normal ECG signals using the SEF approach have in average the entropy of about 0.98. Cryptographic keys that are produced using the strengthened SEF approach offer the entropy of ~ 1. In addition, the reinforced key generation approach has also better P-value NIST pass rates compared to state-of-the-art approaches which rely only on singleton ECG features. We also found out that our approach is approximately 1.8 times faster than existing IPI-based key generation approaches. Future work includes investigating and analysis of other physiological signals within a BAN. This is to realize how the generated cryptographic keys can also be used by other bio-sensors to provide intra-BAN communication security.

REFERENCES

[1] R. J. Anderson, "A security policy model for clinical information systems," in *Proc. IEEE Symp. Secur. Privacy*, May 1996, pp. 30–43.

[2] M. S. Siddiqui and C. Hong, "Security issues in wireless mesh networks," in *Proc. Int. Conf. Multimedia Ubiquitous Eng.*, 2007, pp. 717–722.

[3] A. Bhargava and M. Zoltowski, "Sensors and wireless communication for medical care," in *Proc. Int. Workshop Database Expert Syst. Appl.*, 2003, pp. 956–960.

[4] C. C. Y. 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.

[5] D. K. Altop, A. Levi, and V. Tuzcu, "Towards using physiological signals as cryptographic keys in body area networks," in *Proc. Int. Conf. Pervasive Comput. Technol. Healthcare*, 2015, pp. 92–99.

[6] F. Agrafioti, J. Gao, and D. Hatzinakos, "Heart biometrics: Theory, methods and applications," in *Biometrics*, J. Yang, Ed. Rijeka, Croatia: InTech, 2011. [Online]. Available: https://www.intechopen.com/books/biometrics/heart-biometrics-theory-methods-and-applications, doi: 10.5772/18113.

[7] G.-H. Zhang, C. C. Y. 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.

[8] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[9] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *J. Med. Syst.*, vol. 39, no. 10, p. 115, 2015.

[10] K. V. R. Ravi, R. Palaniappan, C. Eswaran, and S. Phon-Amnuaisuk, "Data encryption using event-related brain signals," in *Proc. Int. Conf. Comput. Intell. Multimedia Appl.*, vol. 1. 2007, pp. 540–544.

[11] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with dna binary strands," *Biosystems*, vol. 57, no. 1, pp. 13–22, 2000.

[12] S. D. Bao, C. C. Y. 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.

[13] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol.*, Aug./Sep. 2010, pp. 2034–2036.

[14] 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.*, Apr. 2011, pp. 1862–1870.

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

[16] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for implantable medical devices using modified one-time pads," *IEEE Access*, vol. 3, pp. 825–836, 2015.

[17] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "Cryptographic key generation using ECG signal," in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2017, pp. 1024–1031.

[18] M. Goresky and A. M. Klapper, "Fibonacci and Galois representations of feedback-with-carry shift registers," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2826–2836, Nov. 2002.

[19] J. Daemen and V. Rijmen, "Specification of Rijndael," in *The Design of Rijndael*. Berlin, Germany: Springer, 2002, pp. 31–50.

[20] 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.

[21] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. IEEE Military Commun. Conf.*, Nov. 2008, pp. 1–7.

[22] F. Miao, L. Jiang, Y. Li, and Y.-T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Sep. 2009, pp. 2458–2461.

[23] A. Banerjee, K. Venkatasubramanian, and S. K. S. Gupta, "Challenges of implementing cyber-physical security solutions in body area networks," in *Proc. Int. Conf. Body Area Netw.*, 2009, Art. no. 18.

[24] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[25] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," in *Proc. IEEE Annu. Conf. Eng. Med. Biol. Soc.*, Jan. 2005, pp. 2455–2458.

[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22 Rev 1a, 2001.

[27] G. Zheng *et al.*, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 3, pp. 655–663, May 2017.

[28] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ECG)," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 6, pp. 1400–1411, Jun. 2017.

[29] P. Li *et al.*, "High-performance personalized heartbeat classification model for long-term ECG signal," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 1, pp. 78–86, Jan. 2017.

[30] L. Sun, Y. Lu, K. Yang, and S. Li, "ECG analysis using multiple instance learning for myocardial infarction detection," *IEEE Trans. Biomed. Eng.*, vol. 59, no. 12, pp. 3348–3356, Dec. 2012.

[31] S. Kiranyaz, T. Ince, and M. Gabbouj, "Real-time patient-specific ECG classification by 1-D convolutional neural networks," *IEEE Trans. Biomed. Eng.*, vol. 63, no. 3, pp. 664–675, Mar. 2016.

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

[33] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. N. Plataniotis, "Analysis of human electrocardiogram for biometric recognition," *EURASIP J. Adv. Signal Process.*, vol. 2008, p. 148658, Dec. 2007.

[34] H.-S. Choi, B. Lee, and S. Yoon, "Biometric authentication using noisy electrocardiograms acquired by mobile sensors," *IEEE Access*, vol. 4, pp. 1266–1273, 2016.

[35] F. Porée, G. Kervio, and G. Carrault, "ECG biometric analysis in different physiological recording conditions," *Signal, Image Video Process.*, vol. 10, no. 2, pp. 267–276, 2016.

[36] Y. N. Singh and P. Gupta, "ECG to individual identification," in *Proc. IEEE Conf. Biometrics, Theory, Appl. Syst.*, Sep./Oct. 2008, pp. 1–8.

[37] D. F. Dickinson, "The normal ECG in childhood and adolescence," *Heart*, vol. 91, no. 12, pp. 1626–1630, 2005.
[38] H. C. Bazett, "An analysis of the time-relations of electrocardiograms," *Ann. Noninvasive Electrocardiol.*, vol. 2, no. 2, pp. 177–194, 1997.
[39] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Generat. Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016.
[40] S. R. Moosavi *et al.*, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Sci.*, vol. 52, pp. 452–459, Jan. 2015.
[41] A. M. Rahmani *et al.*, "Smart e-health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in *Proc. 12th Annu. IEEE Conf. Consum. Commun. Netw.*, Jan. 2015, pp. 826–834.
[42] J. Granados, A.-M. Rahmani, P. Nikander, P. Liljeberg, and H. Tenhunen, "Towards energy-efficient HealthCare: An Internet-of-Things architecture using intelligent gateways," in *Proc. Int. Conf. Wireless Mobile Commun. Healthcare*, 2014, pp. 279–282.
[43] J. S. Sahambi, S. N. Tandon, and R. K. P. Bhatt, "Using wavelet transforms for ECG characterization. An on-line digital signal processing system," *IEEE Eng. Med. Biol. Mag.*, vol. 16, no. 1, pp. 77–83, Jan./Feb. 1997.
[44] A. A. R. Bsoul, S.-Y. Ji, K. Ward, and K. Najarian, "Detection of P, QRS, and T components of ECG using wavelet transformation," in *Proc. IEEE Int. Conf. Complex Med. Eng.*, Apr. 2009, pp. 1–6.
[45] S. Z. Mahmoodabadi, A. Ahmadian, and M. D. Abolhasani, "ECG feature extraction using Daubechies wavelets," in *Proc. Int. Conf. Vis., Imag., Image Process.*, 2005, pp. 343–348.
[46] A. L. Goldberger *et al.*, "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.
[47] H. S. Black and J. O. Edson, "Pulse code modulation," *Trans. Amer. Inst. Electr. Eng.*, vol. 66, no. 1, pp. 895–899, Jan. 1947.
[48] *MATLAB, R2016a*. MathWorks Inc., Natick, MA, USA, 2016.
[49] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.

SANAZ RAHIMI MOOSAVI (S'15) received the M.Sc. (Tech.) degree in information technology, networked systems security from the Department of Information Technology and Communication Systems, University of Turku, Finland, in 2013, where she is currently pursuing the Ph.D. degree with the Department of Future Technologies. Her research interests include security and privacy, Internet of Things, smart healthcare systems, and lightweight cryptography techniques.

ETHIOPIA NIGUSSIE (S'06–M'11–SM'15) received the B.Sc. degree in electrical engineering from Addis Ababa University, Ethiopia, in 2000, the M.Sc. degree in electrical engineering from the KTH Royal Institute of Technology, Sweden, in 2004, and the D.Sc. (Tech.) degree in communication systems from the University of Turku, Finland, in 2010. She is currently an Adjunct Professor of self-aware networked systems with the University of Turku. Her current research interests are self-aware and adaptive systems design, security for low-power wireless networks, including hardware-enabled and smart healthcare systems.

MARCO LEVORATO (S'06–M'09) received the B.S. and M.S. degrees in electrical engineering (*summa cum laude*) from the University of Ferrara, Italy, in 2003 and 2005, respectively, and the Ph.D. degree in electrical engineering from the University of Padova, Italy, in 2009. He held post-doctoral appointments with Stanford University, the University of Southern California, and the KTH Royal Institute of Technology, Stockholm, Sweden. He is currently an Assistant Professor in computer science with the University of California at Irvine. He was a recipient of the Best Paper Award at the IEEE Globecom 2012, the UC Hellman Foundation Award, and has been twice nominated for the Best Young Researcher Award, Department of Information Engineering, University of Padova.

SEPPO VIRTANEN (S'00–M'04–SM'09) received the M.Sc. degree in electronics and information technology and the D.Sc. (Tech.) degree in communication systems from the University of Turku, Finland, in 1998 and 2004, respectively. Since 2009, he has been an Adjunct Professor of embedded communication systems with the University of Turku, where he also Heads the Master's Degree Programme in Information Security. His research currently focuses on information security issues in the communication and network technology domain, specifically focusing on design and methodological aspects of reliable and secure communication systems, and secure communication for IoT.

JOUNI ISOAHO received the M.Sc. (Tech.) degree in electrical engineering and the Lic.Tech. and Dr.Tech. degrees in signal processing from the Tampere University of Technology, Finland, in 1989, 1992, and 1995, respectively. Since 1999, he has been a Professor of communication systems with the University of Turku, Finland, where he is currently the Head of the Communication Systems Laboratory. His research interests include future communication system concepts, applications, and implementation techniques. His current special interests are in dynamically reconfigurable self-aware systems for future communication and interdisciplinary applications, including information security and dependability aspects.