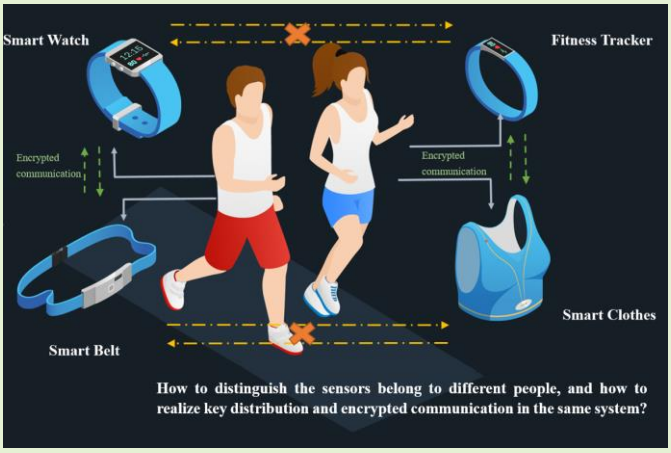
A Novel Hybrid Approach-based on Heartbeat and Accelerometer Signals for Enhanced Security in WBSNs

Guixiang Yan, Guanghe Zhang, Fanghua Liu, Oluwarotimi Williams Samuel, Senior *Member, IEEE*, Majed Aborokbah, Jiquan Guo, Liqing Zhu, Sikang Wei

***Abstract*—In Wireless Body Sensor Networks (WBSNs), ensuring secure and efficient key distribution is critical, particularly given the limited computational and energy resources of the sensors. Existing methods often struggle to balance security with these resource constraints, especially in environments involving physiological data such as acceleration (ACC) and electrocardiogram (ECG) signals. For the first time, this study proposes a novel hybrid approach that integrate fuzzy commitment with ACC signal noise and ECG features for efficient key generation and distribution in WBSNs. By employing a low-pass filter to process ACC signal noise, we generated highly random binary sequences, leveraging the inherent randomness of the signal for secure key generation. Concurrently, an optimized coding scheme was built for ECG feature construction to ensure secure key distribution between devices. Extensive experiments, including entropy analysis and National Institute of Standards and Technology (NIST) statistical tests, confirm the robustness and security of our method. The proposed scheme achieves a false acceptance rate (FAR) of 5.23%, demonstrating superior performance across multiple databases in comparison to benchmark approaches. This novel dual-key generation strategy that combines the unpredictability of ACC noise with the individual-specific traits of ECG signals, can significantly enhance the security, applicability, and versatility of WBSNs.**



***Index Terms*—Acceleration, Cardiovascular, Electrocardiogram, Key distribution, Wireless body sensor networks.**

I. Introduction

IN recent years, Wireless Body Sensor Networks (WBSNs) have shown a wide range of application prospects, thanks to the development of modern communication technology and the Internet of Things. These networks include wearable, implantable, and mobile sensor devices, as well as the remote healthcare systems they enable, which serve to improve people's health and lifestyles[1, 2]. WBSNs continuously monitor physiological indicators such as heart rate, body temperature, blood pressure, heart sound, electrocardiogram (ECG) signal, photoplethysmography (PPG) signal, and motion through sensors, and the hub node can visualize or remotely transmit this data. These physiological data are widely in use in fields such as telemedicine [3-6], remote psychological support [7, 8], sports rehabilitation [9-12], fitness training [13, 14], and other fields[15]. As the transmitted data is the user's physiological information, it is sensitive and private. Ensuring safe and efficient transmission of such information is of utmost importance. Because of this characteristic, sensors in WBSNs are often resource constrained, especially for implantable devices[16]. Traditional schemes such as public key cryptography and Advanced Encryption Standard (AES), which require a large number of operations, are not suitable for securing data transmission in WBSNs. This limitation necessitates the need for a more advanced and efficient approach for securing data during transmission in WBSNs.

The secure communication of data between sensors based on physiological characteristics is a promising research field and it has attracted a lot of research attention in recent years. Physiological features such as fingerprints, iris patterns, face recognition, gait, ECG, PPG, and electroencephalograms (EEG) are commonly used for key generation, key distribution, and security authentication of WBSNs sensors [17-25]. This is partly these physiological characteristics are universal, unique, persistent, and effective. In addition, gait-based schemes usually use acceleration (ACC) signals from sensors to extract features [21, 26, 27], and these schemes often require users to take specific actions, such as shaking hands and walking with a certain posture, thus increasing the burden on users. When

Manuscript received XXX; revised XXX; accepted XXXX. Date of publication XXX; date of current version XXX.. The associate editor coordinating the review of this article and approving it for publication was XXX. (Corresponding author : Guanghe Zhang.)

Guixiang Yan, Guanghe Zhang, and Fanghua Liu are with the School of Computer and Information Engineering, Jiangxi Normal University, Nanchang 330022, Jiquan Guo, Liqing Zhu,and Sikang Wei are with the School of Digital Industry, Jiangxi Normal University, Shangrao 334000, China (e-mail: guanghezhang@163.com).

Oluwarotimi Williams Samuel with the School of Computing and Data Science Research Centre, University of Derby, Derby, United Kingdom . He is also with the INTI International University, Maleysia.
-(e-mail: o.samuel@derby.ac.uk)

Aborokbah, Majed is with the Faculty of Computers and Information Technology University of Tabuk, Tabuk, Saudi Arabia. (e-mail: m.aborokbah@ut.edu.sa)

Digital Object Identifier XXX

extracting gait features from ACC signals, computationally complex analytical methods, such as principal component analysis (PCA), are needed. This approach is inefficient when applied to sensor networks that are characterized by limited computing resources and energy. The inter-pulse-interval (IPI) is a physiological feature that can be easily extracted from cardiac electrical signals [23, 24, 28, 29]. Previous research have focused on establishing security protocols for telemedicine with most of the studies considering ECG-based security protocols in the resting state though the performances of such schemes in daily activities has not been comprehensively studied. In heartbeat-based schemes, the discrete wavelet transform (DWT) can easily extract IPI from ECG signals. When combined with fuzzy commitment, it can determine whether the collected signal belongs to the same individual or not. However, in the active state, the low entropy of binary sequences produced by existing security schemes significantly reduces reduces the overall security of the scheme. ACC signals in the active state are easy to obtain and exhibit good time-variance and randomness. To achieve an optimally balanced security scheme that could be adopted in WBSNs that are often constrained with limited computing resources, our proposed hybrid approach seeks to generate a set of highly secured keys from ACC signal noise. Besides, the key distribution aspect is realized by combining fuzzy commitment with the IPI vector block coding method, which was proposed in this study. Therefore, this paper proposes a novel hybrid key generation and distribution system for WBSNs, and the system is realized by combining ACC signal noise with IPI to achieve secure communication between sensors in the network.

The main contributions of this paper are summarized as follows:

- In this paper, we propose a novel hybrid method that is robust, scalable, and efficient. This method efficiently and securely distributes keys not only in the context of resting telemedicine but also in daily activities to secure WBSNs resources.
- The proposed approach clearly demonstrated how features from ACC and ECG signals could be adequately extracted and fused to generate and distribute secured keys for securing WBSNs resources.
- Extensive evaluation results of the proposed method's performance indicated superior performance to the commonly used IPI-based ECG signal schemes for secure key generation and distribution in WBSNs.

In the remaining part of the paper, Section II contains an overview of the work and Section III describes the proposed system's model. In Section IV, we detail the proposed key generation and distribution scheme, which aims to provide secure and efficient information transmission for WBSNs while avoiding conflicts between different WBSNs. Section V presents the evaluation results and Section VI is the conclusion of the paper.

II. Related Works

Prior works on WBSNs security have proposed schemes based on establishing a shared secret key using the body's physiological values, such as heart rate and temperature. Much prior works rely on the ECG signal, which is a voltage signal that is easily measured by the electronic sensor devices and requires relatively low processing [30, 31]. The idea of extracting keys from physiological values to secure wearable devices was first proposed in [32]. Physiological signals such as ECG and EEG are suitable candidates for key generation because they provide a continuous source of true randomness. In other words, these physiological values can be viewed as a source of entropy within the human body, constantly generating and broadcasting (unpredictable) random bits. Randomness of physiological values has been documented in a large amount of medical literature[33, 34]. To secure wearables using heartbeat based signals as a random source for key generation, Poon et al. proposed a scheme using ECG and PPG-based peak intervals called IPI [17]. By using hamming distances to match different sensors equipped on the same individual. False acceptance rate and false rejection rate are used to evaluate the security of the scheme. After that, Bao et al. [30] proposed the use of the m-IPI cascade to obtain the random number generating key, which improved the efficiency of key generation. Zheng et al. [35] employed the use of time intervals of Q, R, S, P and T peaks of ECG signals to generate random numbers, which resulted in higher randomness and efficiency of key generation. Xu et al. [36] proposed to carry out the significant bit analysis of IPI entropy and build a normal mapping model based on the statistical properties of IPI to generate more uniformly distributed random numbers to secure wearable devices. Seepers et al. [37] further studied the properties of bit-by-bit entropy in the IPI of the ECG signal, analyzed the influence of each bit in IPI on generating random numbers, and finally selected three digits in the middle part to generate random numbers, obtaining random numbers with high information entropy. Sandeep Pirbhulal et al. [23] utilized a mathematical method of cyclic block coding driven by IPI to generate 16-bit strings with good randomness. Seepers et al. [38] proposed the solution of using Inter-multi-Pulse-Interval (ImPI) to deal with m-health, using multiple IPI to increase the entropy of key generation, and one IPI can generate only one bit. One main limitation of this method is that it takes a lot of time to generate secured keys. All of these heartbeat-based methods are capable of generating keys with reliable randomness and security regardless of whether they are fast or slow. However, they all have the similar limitation, that is, they are all suitable for key or random number generation in the resting state, and the schemes in the non-resting state are rarely investigated, constituting a research gap that needs to be addressed.

Indeed, our tests have shown that using heartbeat as a random source above works well when the system is at rest; but, when the system is in active, its key randomness and security are significantly decreased. Furthermore, as we show in Section IV of this research, these heartbeat-based methods are unable to assist in the development of secure keys for data transmission in wearable devices while they are in active. Notable research that take into account generating keys in active states are reviewed as follows. The Martini Synch was proposed by Kirovski et al. [39] and it was the first study to generate a public key based on ACC signals of common vibrations between two devices that need shaking together. Qi et al. [40] developed a secure wrist-worn smart device pairing

scheme by using device active signals generated by handshakes to negotiate reliable keys between users. This task involves the additional step of shaking hands to confirm a match. Cornelius et al. [41] integrated sensors on different parts of the body, picking up signatures of activity to determine whether the device is on the same body. The method using supervised learning here requires a lot of computation and pre-training, and is not suitable for most resource-constrained sensor networks. Xu et al. [42] proposed a key generation protocol for portable mobile devices based on Gait. This requires the use of blind source separationto extract the gait information from noisy ACC signals, which consumes computing resources and energy. Sun et al. [21] propose a lightweight method to extract common features based on gait and implement group key generation in combination with fuzzy vault. However, it is also necessary to use the PCA method which requires a lot of calculation when extracting gait features. The above method of generating the key in the active state has two main problems: one is that the user needs to carry out some specific operations, and the other is to increase the user's use burden. Gait feature extraction is relatively difficult, computation-intensive and energy consuming. This makes these methods unsuitable for resource-constrained WBSNs. In particular, rehabilitation scenarios may involve more resource-constrained sensor devices, such as implantable devices or external chest straps, which will require ACC energy consumption, thus, affecting user satisfaction.

During active state, the ACC signal can be used to quickly generate a large number of random sequences that change with time. Therefore, we use the noise of the ACC signal rather than the more difficult to obtain gait features to generate the key for communication between WBSNs sensors. Although the performance of key generation systems based on heartbeat signals is poor in non-resting states, it can still reduce user load and enhance user experience compared to certain additional operations[43]. In practical applications, it is important to accurately determine whether the sensor is part of the same entity, ensuring accurate communication and preventing crosstalk between WBSNs. This can be achieved by integrating fuzzy commitment with electrical signals from the heart. We aimed to build a lightweight security solution that is more universal and efficient in terms of securing WBSNs resources. Therefore, we propose a novel hybrid key generation system based on ACC signal noise, combined with ECG signals vectorization block encoding and fuzzy commitment, realizing efficient key distribution to better secure wearable devices.

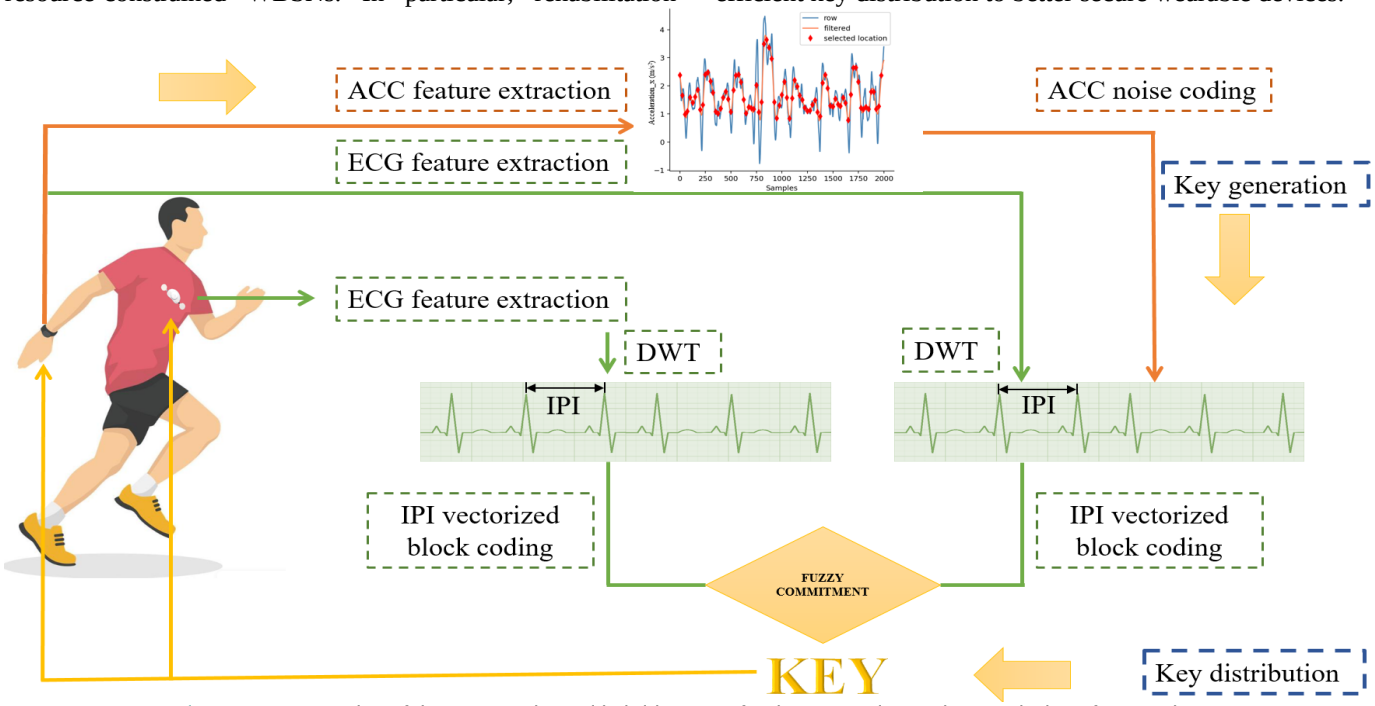


Fig 1. Representation of the proposed novel hybrid system for the generation and transmission of secure keys

III. System Model

In this section, the components and operational procedure of the proposed novel hybrid secure key generation scheme are presented. We have modeled the WBSNs system as a hub node and several sensor nodes throughout the body, where the hub node represents a smart ring or watch. The sensor node sends the collected data to the hub node and executes the instructions from the hub node. In the WBSNs, the hub node uses ACC calculation to generate the key and collects ECG signals to calculate IPI, while the sensor node uses IPI vectorized block coding to realize key sharing through fuzzy commitment. The specific workflow of the system is described in Fig 1.

In WBSNs ACC signals and ECG signals are the most frequently collected data types. ACC signals, in particular, produce numerous sampling sequences over a specified period, which are instrumental for gait-based applications. However, extracting gait characteristics from these ACC signals necessitates substantial processing, thereby intensifying the energy and computational constraints inherent to sensors within WBSNs. To mitigate this challenge, we propose an innovative approach that harnesses the random noise inherent in ACC signals. By processing this noise through a straightforward

routine, we generate a cryptographic key that enhances the security of WBSNs, leveraging the ACC signal's natural variability to establish a secure communication channel.

Furthermore, we integrate an optimized coding scheme for ECG feature with fuzzy commitment to implement a robust key generation and distribution mechanism suitable for WBSNs during their active state. The ECG-derived key function as session keys, providing an additional layer of security by ensuring that each communication session is protected by a unique key. The system uses the noise feature of the ACC signal to encode the communication key. Like [20][29], the system uses the IPI extracted from the ECG signal by DWT, and then encodes the IPI vectorized block to generate the session-specific key. This dual-key approach enhances the security of WBSNs by combining the unpredictability of ACC noise with the individual-specific traits of ECG signals. The detailed procedures for feature extraction from ACC and ECG signals, as well as the coding schemes employed, are outlined in Section IV of this paper. This comprehensive approach not only addresses the security challenges of WBSNs but also optimizes the utilization of the sensors' limited resources.

IV. Key Generation and Distribution in WBSNs

A. Analyzing ECG signals

Before actually generating the key, the ECG signal characteristics are analyzed in the active state. IPI extracted from ECG signals is usually considered the interval between R-peaks in two heartbeat intervals. As a common physiological feature of the human body, IPI has been used in many previous studies as an important random source for protecting the security of WBSNs. However, the above studies are mostly based on ECG signals collected in the resting state. As far as we know, there are few comprehensive studies examining ECG signals as a random source for protecting wireless body area networks in the active state. In this section, we compare the distribution of the most commonly used ECG signature, IPI, for securing wireless body area networks across different databases in active and resting states.

Fig 2 displays the distribution of IPI in different activity states, including high-intensity cycling (s3hb), low-intensity cycling (s3lb), running (s3r), and walking (s3w). The ECG signals were collected by the chest sensor in the WRIST [44] database. Our analysis revealed a leftward shift in the distribution interval of IPI during the active state. This was due to an accelerated heartbeat and a shortened heartbeat period, resulting in a smaller IPI value, measuring the interval between R-peaks of heartbeat signals. We observed varying degrees of convergence and an upward shift in the frequency of IPI distribution in the active state. Specifically, in the s3r record, the IPI distribution around 550 accounted for 70% of the total IPI. It is important to note that this observation is limited to the given record and may not be representative of the entire dataset.There is a medical explanation for the phenomenon mentioned. The randomness of the electrical signals of the heart stems from heart rate variability (HRV), which is controlled by the sympathetic and parasympathetic nerves. HRV can be affected by various factors such as age, sex, emotional state, and exercise [45-47]. The inhibitory effect of exercise on HRV is a disadvantage for using IPI to generate random sequences to secure wireless body area networks. If the distribution of IPI is too concentrated, most schemes that generate random sequences based on IPI will produce a context-dependent random sequence that is easier for an attacker to predict.

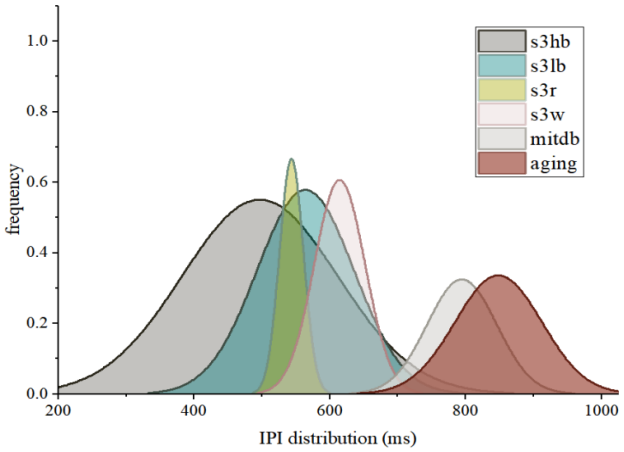


Fig 2 The distribution of IPI in different activity states

To investigate the impact of activity status on IPI-based schemes, we selected four typical encoding schemes (Chizari [28]、Xu [36]、Zhang [48] and Seepers [49]) and used them to encode data from the MITDB [50] and WRIST databases. We evaluated the degree of impact quantitatively using Shannon entropy (2), collision entropy (3), and minimum entropy (4). Shannon entropy is commonly used to quantify information uncertainty. In this context, we measure the confidentiality of the generated sequence. Collision entropy, which is the Rényi entropy with α equal to 2, describes the probability of no collision between the generated sequences as a measure of conditional safety. Minimum entropy is the limit of convergence used to describe the unpredictability of a source. In this case, it is used to measure unconditional confidentiality. The pr[X=x] in the equations represents the probability in $X = [0, 1]$.

$$H_{Sh}(X) = -\sum_{x \in R(X)} \Pr[X = x] \log(\Pr[X = x])) \tag{2}$$

$$H_{\alpha = 2}(X) = \frac{1}{1-\alpha} \sum_{x \in R(X)} \Pr[X = x]^{\alpha} \tag{3}$$

$$H_{\infty}(X) = min_{x \in R(X)} \left\{ log \frac{1}{\Pr[X = x]} \right\} \tag{4}$$

The comparison of the three entropies of the four schemes in Fig 3 reveals that all four schemes show that the 128-bit random binary sequence generated by the WRIST active database exhibits lower information entropy, collision entropy, and minimum entropy. This indicates that the random binary sequence generated from WRIST database parameters in the active state provides significantly weaker security for wireless body area networks compared to the resting state MITDB database.

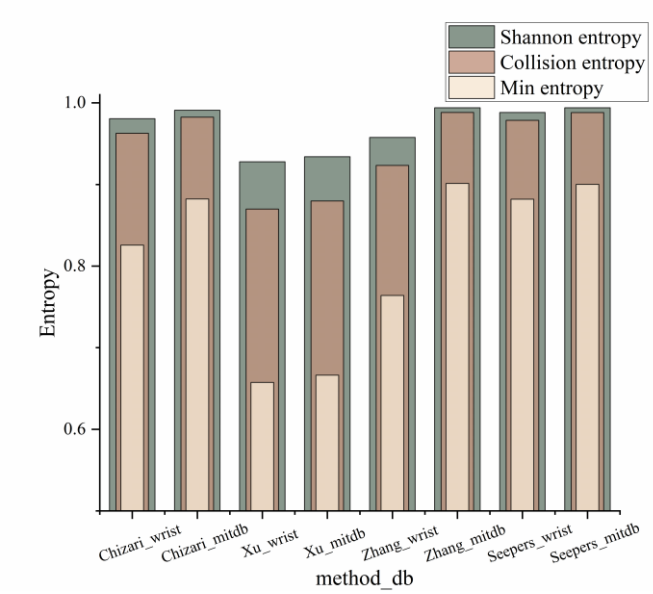


Fig 3 The manifestation of different entropies
The entropy of active database is lower than that of resting database.

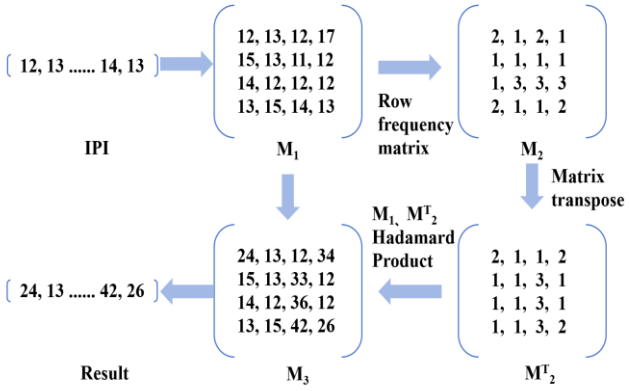


Fig 4 IPI vectorization transformation

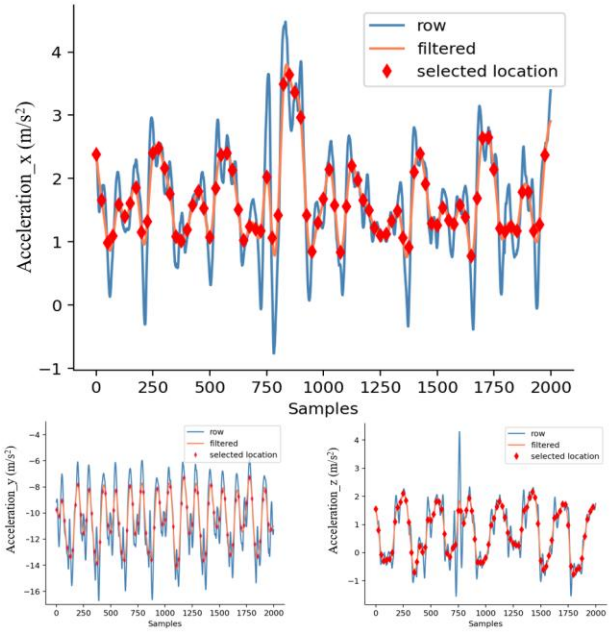


Fig 5 ACC noise coding

B. Generate binary sequence base on IPI

Most schemes based on IPI analyze each IPI as an independent entity or separate the significant bits of a single IPI. However, this approach ignores the fact that IPI is generated as an ordered string when generating random binary sequences. Our model takes the order of the IPI sequence into account, with the goal of obtaining an unordered binary string. Therefore, we suggest trying the method of reshuffling sequences with multiple duplicate IPIs. To optimize the problems presented in the previous section, we utilized the method proposed in Fig 4 which we call vectorization transformation. First, every 16 vectorized IPIs are transformed into a 4x4 matrix named M_1, then the row frequency vector of M_1, named M_2, is generated. By taking the transpose of M_2 and performing the Hadamard product with M_1, we obtained M_3. After restoring M_3 to the IPI sequence, we obtained a final IPI sequence with irregular changes in value, which is used for subsequent random number generation. This is because the frequency in an IPI sequence is random.

For the IPI sequences after vectorization transformation, a new quantization method called block coding is used to convert them into binary random sequences. All IPIs are grouped into blocks of size 4, and the mean (μ) and variance (σ) within each block are calculated. Each IPI is then mapped to the corresponding relation in the TABLE I and encoded as a 4-bit binary sequence. The binary numbers generated by multiple IPIs are spliced together to form the final sequence required to combine the fuzzy commitment for key distribution.

TABLE I
BINARY SEQUENCE COMPARISON TABLE

Domain	Binary Sequence	Domain	Binary Sequence
(-∞, μ-1.534σ)	0000	(μ, μ+0.157σ)	1000
(μ-1.534σ, μ-1.151σ)	0001	(μ+0.157σ, μ+0.319σ)	1001
(μ-1.151σ, μ-0.887σ)	0010	(μ+0.319σ, μ+0.489σ)	1010
(μ-0.887σ, μ-0.675σ)	0011	(μ+0.489σ, μ+0.675σ)	1011
(μ-0.675σ, μ-0.489σ)	0100	(μ+0.675σ, μ+0.887σ)	1100
(μ-0.489σ, μ-0.319σ)	0101	(μ+0.887σ, μ+1.151σ)	1101
(μ-0.319σ, μ-0.157σ)	0110	(μ+1.151σ, μ+1.534σ)	1110
(μ-0.157σ, μ)	0111	(μ+1.534σ, +∞)	1111

C. Key generation base on ACC

In contrast to gait-based schemes, processing ACC signals requires complex procedures. We utilize the noise present in the ACC signal to generate numerous time-varying random binary sequences. These sequences are then employed as keys to encrypt the information transmitted between sensors. To process the x, y, z triaxial acceleration, a second-order low-pass Butterworth filter of 3Hz was used in Fig 5, as human activity is typically concentrated within this frequency range. Next, a

feature point was selected every 25 sampling points, and the noise of the ACC signal was calculated as the difference between the two signal values before and after filtering. Through noise coding, signal value differences greater than 0 are quantized to 1, and differences less than 0 are quantized to 0. The resulting quantized feature points are then cascaded together as the key, with every 128 points included.

D. Key distribution

Fuzzy commitment was first proposed by Juels et al. [51]and then Hao et al. [52]applied it to the field of biometric encryption. It uses error-correcting code technology to correct deviations in transmitted information caused by sampling interference, transmission interference, or other factors. By selecting the appropriate error correction code(ECC), the transmitted key is encoded. Here we use BCH code, named after its inventors: Bose, Chaudhuri, and Hocquenghem. This is a widely used cyclic code that can correct a variety of errors. BCH code is usually represented as BCH (n, k, t), where n represents the bit of information transmission, k represents the effective information load, and t represents the error correction capability of BCH coding.

The specific process is delineated below:Initially, the hub node utilizes the collected ACC signal to generate a communication key (*KEY*) via noise coding,performs error correction coding on the *KEY* to produce an ECC (*Kecc*),and then hashes the generated *Kecc* to create a hash value (*hash(KEY)*).A random binary sequence (BS_T) as session key, equivalent in length to *Kecc*, is derived following the encoding of the transmitter's signal by an IPI vectorized block encoding.The subsequent XOR operation between BS_T and *Kecc* generates the transmission template, as depicted in (1).

$$F(KEY,BS_T) = \{BS_T \oplus K_{ecc},\ hash(KEY)\} \quad (1)$$

The receiver and transmitter concurrently collect the ECG signal, subsequently generating a random binary sequence (BS_R) equivalent in length to *Kecc* post IPI vectorization block encoding. Post-reception of the template, an XOR operation involving the generated random sequence BS_R and ($BS_T \oplus Kecc$) yields (*Kecc'*). A minor discrepancy exists between the generated BS_R and BS_T due to the distinct body locations where the transmitter 's and receiver's ECG signals are collected. These discrepancies are addressed during subsequent ECC decoding, with the corrected version being generated post-ECC decoding as *(KEY')*. The receiver's *KEY'* undergoes identical hashing as the transmitter's, with the resultant hash *(hash(KEY'))* compared against the template's *hash(KEY)*. Concordance between the two hashes signifies the completion of key distribution. It is evident that accurate decryption of the *KEY* is feasible solely when the disparity between BS_R and BS_T falls within the BCH's error correction capacity, and the randomness inherent in sequences BS_R and BS_T plays a pivotal role in key distribution. Numerous studies have shown that signal sampling frequency, user physiological state, the length of the generated sequence, and the coding method all affect the properties of the generated random sequence. Subsequent sections of this manuscript will concentrate on elucidating the genesis of the random sequences within our methodology. The fuzzy commitment key distribution process in the approach is described in Fig 6.

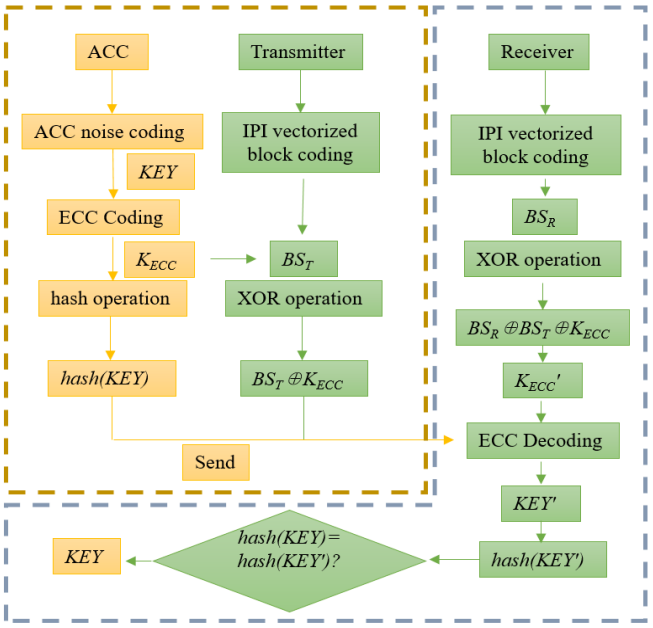


Fig 6. Fuzzy commitment key distribution process

V. Experimental and Scheme Analysis

A. Experimental setup

The system was analyzed using four publicly available data sets from PhysioNet [53]: WRIST PPG during Exercise. The databases include wrist PPG recordings during walking, running, and cycling, as well as chest ECG recordings that collect movement information using both accelerometers and gyroscopes. The data set consists of 19 samples from eight subjects in various activity states, with a sampling frequency of 256Hz. The AGING (Autonomic Aging) [54] database includes resting multi-channel ECG signals sampled at 1000Hz from 1121 healthy volunteers, with the first 400 being used for analysis. The MITDB (MIT-BIH Arrhythmia Database) contains 48 two-channel ECG records with a sampling frequency of 360Hz. The NSRDB [53] (MIT-BIH Normal Sinus Rhythm Database) includes 18 normal human ECG records sampled at a frequency of 360Hz.

The experiments were conducted on PC environments with an Intel Core i7-8750 H CPU, 8 GB RAM, and a NVIDIA Geforce GTX 1060 with Max-Q Design GPU, using the Kali Linux 3.0. The platform ran National Institute of Standards and Technology (NIST) statistical tests, while all other test and analysis platforms ran on Windows 10 using Python 3.9.

B. ACC Generation Sequence Test

The study generated a 128-bit random sequence using triaxial ACC noise from 19 subjects in WRIST. The sequence was then tested by NIST, with the experimental results showing that 9 items in the NIST test were passed in TABLE II. This indicates that the encoding method based on ACC signal noise can generate a random binary sequence with good randomness. The sequence is suitable for use as a random source to generate keys to protect the security of WBSNs in the active state. ACC signals are particularly easy to collect in the active state and generate random sequences quickly, making them more suitable for protecting the security of WBSNs. It is important to

note that this statement is objective and does not contain any subjective evaluations.

TABLE II
ACC NOISE CODING NIST TEST
The results were able to show that randomness is suitable as a key through 9 NIST tests

NIST test items	Pass rate	P value
Approximate Entropy	1	1
Block Frequency	0.992579	0.554335
Cumulative Sums	0.993197	0.634938
FFT	0.970315	0.433955
Frequency	0.992579	0.554335
Longest Run	0.946197	0.368787
NonOverlappingTemplate	0.892799	0.892807
Runs	0.90538	0.357707
Serial	0.908782	0.48237

C. Vectorization Transformation Analysis

Based on the previous analysis of ECG signals and IPI, the distribution of IPI during the active state differs from that in the resting state. In the active state, the distribution is more concentrated and exhibits a higher repetition rate. This concentration and repetition adversely affect the randomness and security of the binary sequences generated by most IPI-based schemes. A more concentrated distribution increases the likelihood that subsequent binary sequences can be guessed by attackers, while a higher repetition rate reduces the number of significant bits in the binary sequence. To ensure that a binary random sequence is well-distributed and has a low repetition rate, we apply the vectorization transformation method for optimization.

TABLE III
REPETITION RATE AFTER TRANSFORMATION
The results show that the repetition rate of IPI can be reduced after transformation

Repetition rate			
Before		After	
AGING	28.09%	AGING	25.76%
NSRDB	48.31%	NSRDB	40.79%
MITDB	46.53%	MITDB	41.64%
WRIST	66.61%	WRIST	55.40%

First, the repetition rate of IPIs in each database is counted, since most IPI-based security schemes require between 32 and 128 to generate a 128-bit binary sequence. Here, we group all IPIs in the four databases and calculate the repetition rate within 100 consecutive IPIs. Each 100-bit IPI is counted separately. If the quantity counted is greater than 1, the quantity counted is set to 1 to obtain a non-duplicate set. The size of the statistical set is subtracted from 100 to obtain the number of duplicate IPIs, and the number of duplicate IPIs is divided by 100 to obtain the repetition rate within the group. The IPI recurrence rate of the database is obtained. In the TABLE III shows the change of the repetition rate of the four databases before and after vectorization transformation after applied the vectorization transformation we set, the repetition rate of IPI decreased to varying degrees across different databases. Notably, the repetition rate of the WRIST database decreased from 66.61% to 55.40%, representing a reduction of over 10% in IPI repetition rate.

Chizari[28], Xu[36], Zhang[48], and Seepers[49] encoding schemes were used to test the Shannon entropy, collision entropy, and minimum entropy of the MITDB and WRIST databases. Fig 7, shows the performance of the three types of entropy after the vectorization transformation. The performance of the four coding methods on the WRIST database is better after the vectorization transformation, particularly in the Chizari and Xu scheme where the Min entropy increment is over 0.5. Additionally, there is a slight increase in Shannon entropy and collision entropy. The MITDB database positively affects the three entropy values, except for the Xu_mitdb group due to its unique coding scheme that uses normally distributed maps. Our vectorization transformation can improve the unpredictability of generating random sequences based on IPI schemes in the active state, enhance confidentiality and conditional security, and improve the security of most IPI-based security schemes in the resting state.

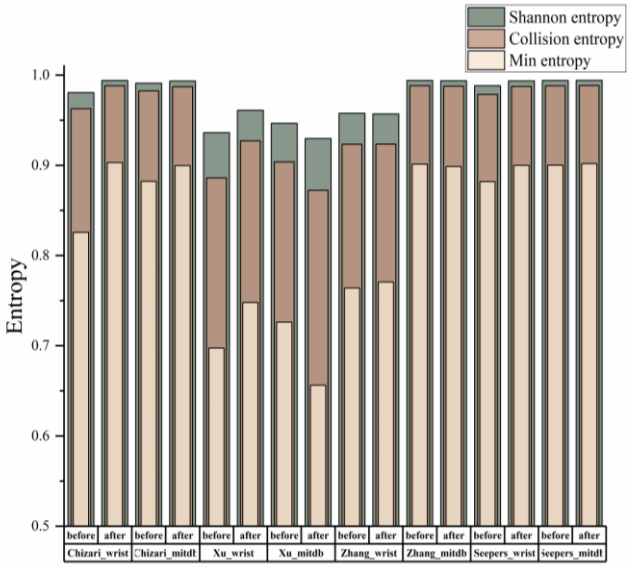


Fig 7 Entropy test after transformation

The results show that the entropy of generated random sequence can be increased after the transformation

We conducted NIST tests on 128-bit random binary sequences generated by different coding schemes on MITDB and WRIST databases. TABLE IV calculates the pass rates and compares them with the pass rates before vectorization transformation. The data with pass rates higher than 0.05 were bolded. Block Frequency and the Cumulative Sums and Frequency test are discussed. For instance, in the Frequency test, Chizari's method had a pass rate of only 0.7160 in the WRIST database, which is significantly lower than the 0.9434 pass rate in the MITDB database. However, after vectorization transformation, the pass rate in the WRIST database increased to 0.9870, a 27.1% increase, and higher than the 0.9659 pass rate in the MITDB database. Our vectorization transformation method can improve the NIST test pass rate of various coding schemes, thereby enhancing the quality of generated binary random sequences. Specifically, our scheme significantly

improves the NIST pass rate of non-resting signals in the WRIST database, enabling it to better adapt to different states, including resting and non-resting, and ultimately enhancing the security of WBSNs.

D. Block Size Analysis

Based on the previous analysis, it was found that the WRIST active database has a 66.61% repetition rate for IPI sequences. Additionally, we used Jaccard distance to measure the correlation between IPI sequences. Jaccard distance is the complement of Jaccard similarity, and the Jaccard similarity index is used to measure the similarity between two sets. The Jaccard similarity index is defined as the number of elements intersected by the number of elements in the union (5). The Jaccard distance measures the dissimilarity between two sets and is the complement of Jaccard similarity coefficient. It is defined as 1 minus the Jaccard similarity coefficient(6). In the WRIST database, we group IPI sequences of different active states with varying amplitudes and calculate their Jaccard distances. It is important to note that since the IPI sequence is sequential, the set elements used in our calculation also have serial numbers. For example, [1,2,3,1] should be considered in the calculation of intersection and union as [(1,1),(2,2),(3,3),(4,1)]. The intersection of [1,2,3,1] and [1,2,1,3] is [(1,1),(2,2)], while the union set is [(1,1),(2,2),(3,3),(4,1),(3,1),(4,3)]. The Jaccard distance can be calculated as 0.66.

$$J(A,B)=\frac{|A\cap B|}{|A\cup B|} \tag{5}$$

$$d_J(A,B)=1-J(A,B)=\frac{|A\cup B|-|A\cap B|}{|A\cup B|} \tag{6}$$

TABLE IV
NIST TEST AFTER TRANSFORMATION
The results show that the passing rate of NIST test can be improved after the transformation.

		Chizari[28]		Seepers[49]		Xu[36]		Zhang[48]	
Test items		before	after	before	after	before	after	before	after
Approximate	MITDB	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Entropy	WRIST	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Block	MITDB	0.9434	0.9659	0.9895	0.9905	0.5924	0.3564	0.9873	0.9839
Frequency	WRIST	**0.7160**	**0.9870**	**0.9300**	**0.9802**	**0.5159**	**0.6410**	0.6232	0.6380
Cumulative	MITDB	0.9509	0.9738	0.9896	0.9900	0.5738	0.3459	0.9880	0.9858
Sums	WRIST	**0.7407**	**0.9870**	**0.9261**	**0.9881**	0.4899	0.6261	0.6101	0.6454
FFT	MITDB	0.9535	0.9539	0.9834	0.9839	**0.8739**	**0.9312**	0.9856	0.9842
	WRIST	0.9383	0.9481	0.9805	0.9960	0.8638	0.8872	0.9826	0.9911
Frequency	MITDB	0.9434	0.9659	0.9895	0.9905	0.5924	0.3564	0.9873	0.9839
	WRIST	**0.7160**	**0.9870**	**0.9300**	**0.9802**	**0.5159**	**0.6410**	0.6232	0.6380
LongestRun	MITDB	0.7459	0.7866	0.9889	0.9903	0.1120	0.0342	0.9848	0.9849
	WRIST	**0.6914**	**0.8442**	0.9689	0.9921	0.1014	0.1187	0.8029	0.8042
NonOverlappingTemplate	MITDB	0.9253	0.9239	0.8816	0.8816	0.9446	0.9528	0.8810	0.8813
	WRIST	0.9034	0.9112	0.8843	0.8811	0.9520	0.9405	0.9043	0.9006
Runs	MITDB	0.4333	0.3920	0.9891	0.9891	0.5848	0.5180	0.9879	0.9884
	WRIST	0.5062	0.2987	0.9805	0.9802	0.5797	0.6202	**0.6870**	**0.7418**
Serial	MITDB	**0.7038**	**0.7737**	0.9855	0.9845	0.0002	0.0000	0.9806	0.9797
	WRIST	**0.8148**	**0.8701**	0.9611	0.9861	0.0000	0.0000	0.8145	0.8561

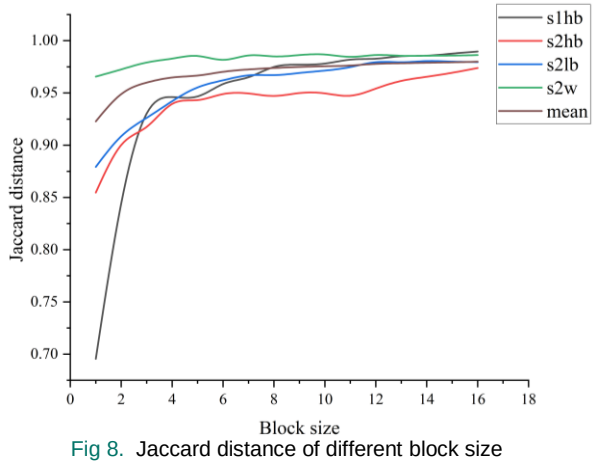


Fig 8. Jaccard distance of different block size

After our analysis it is appropriate to set the block size to 4.

The Jaccard distance of various grouping methods was tested based on block sizes ranging from 1 to 16. This was done to determine the impact of different block sizes on the Jaccard distance and the repetition rate of sequential IPI groups. To ensure fairness in the experiment, only the last 50 sets of each grouping method were compared.

Fig 8 displays the experimental results. The Jaccard distance significantly increases for block sizes 1-4, increases with block size for 4-6, and steadily increases for 6-16. The figure displays the Jaccard distance of the first several samples from the WRIST database. The sets compared are s1hb, s2hb, s2lb, s2w, and mean, which represent the high-intensity bicycle pedal of the first sample in WRIST, high-intensity bicycle pedal of the second sample, low-intensity bicycle pedal, walking, and the average data of all 19 samples, respectively. The Jaccard distance is a measure of the difference between sets, with a greater distance indicating a larger difference. When the block size of s1hb is 1, the Jaccard distance is only 0.6955, which is equivalent to no block processing. However, when the block size is 3 or 4, the Jaccard distance increases to 0.9303 and 0.9460, respectively. Furthermore, the average data from 19 sample populations indicated that an increase in block size within the range of 1-4 resulted in a significant increase in Jaccard distance. This suggests that grouping IPI sequences can increase the differentiation between blocks and subsequently enhance the differentiation between sequences, resulting in the generation of binary random sequences.

The IPI sequence was partitioned and mapped to 4-bit binary numbers with a normal distribution based on the order within the block. The mapping relationship between the mean

(μ) and variance (δ) element was calculated according to the IPI sequence within the block, as shown in TABLE I. Our sequence was processed using a method similar to Xu's scheme. The Gray encoding was not used in this case because our experiments have shown that it is more appropriate to use the encoding in the corresponding table in our scheme. As illustrated in Fig.9 below, we tested Shannon entropy, collision entropy, and minimum entropy on four databases using both Xu's[36] coded comparison table and our own coded comparison table, generated using Xu's subsequent random number generation method. The results indicate that our scheme outperforms Xu's Method in terms of the three types of entropy across all four databases. Additionally, NIST tests were conducted and our scheme is expected to perform better in these tests.

After determining the encoding table and studying the impact of varying block sizes on the Jaccard distance of IPI sequences, we analyzed the effect of block size on the difference of IPI sequences. This section will examine the impact of different block sizes on the generation of binary sequences using our scheme. The study measured the Shannon entropy, collision entropy, and minimum entropy of 128-bit binary sequences with IPI block sizes of 1, 4, 8, and 16 on four databases. The results in Fig 10 indicate that samples with a block size of 1 consistently performed the worst in all four databases for all three entropies, which aligns with the Jaccard distance test results of the IPI sequence described above. In the four test groups (1, 4, 8, and 16), the databases exhibit an initial increase followed by a decrease, indicating that excessively large block sizes can impact the entropy of generating random binary sequences. Therefore, we selected the test group with an IPI block size of 4. The Shannon entropy, collision entropy, and minimum entropy measured in all test databases were the highest. In the AGING database, our scheme calculated three entropy values above 0.9, with Shannon entropy and collision entropy being close to 1. This outperforms all other schemes we previously measured. For our scenario, we set the IPI block size to 4 to achieve optimal confidentiality, conditional security, and unpredictability of random binary sequences. In the entropy test, it was found that our coding scheme can produce a binary sequence representing the active state of the WRIST database with a higher entropy value than other coding schemes. This feature makes our scheme suitable for a wider range of application scenarios and enhances the security of WBSNs.

We investigated the impact of various packet sizes on the binary sequence produced by our scheme to pass the NIST random number test. We evaluated the NIST test pass rates for 128-bit binary sequences generated with IPI block sizes of 1, 4, 8, and 16 on four databases, respectively. TABLE V displays six NIST test pass rates, and the group with the highest pass rate for each test in each database is highlighted in bold. All items passed the Approximate Entropy test. The Block Frequency, Cumulative Sums, and Frequency tests, as well as three other test items, achieved the maximum pass rates with a block size of 4 across all four databases. In addition, when the IPI sequence block size is 4, the pass rate of the FFT project reaches the maximum except for the MITDB database, which is consistent with our previous entropy test results. In the sample with an IPI sequence block size of 4, the pass rates of Block Frequency and Cumulative Sums are close to 100%. Our scheme performed well on the WRIST database, obtaining higher NIST test pass rates in Block Frequency, Cumulative Sums, and Frequency compared to the MITDB and NSRDB datasets. This demonstrates that our scheme is capable of producing random binary sequences of equal or superior quality in the active state compared to the resting state. This enhances the security of WBSNs.

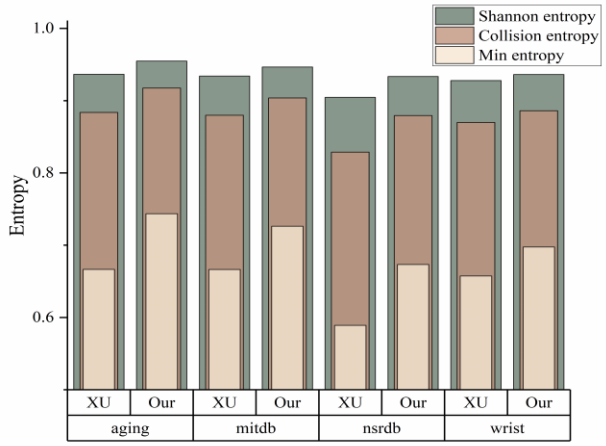


Fig 9. Entropy test in four databases

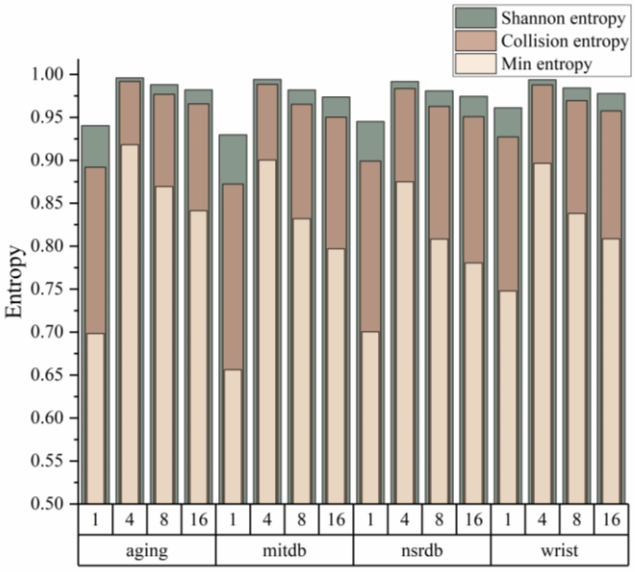


Fig 10. Entropy test in different block size

In the entropy test, better performance is achieved when the block size is set to 4.

E. Binary sequences randomness analysis

The randomness of the binary sequence generated by IPI vectorization block encoding is crucial for our scheme, which integrates fuzzy commitment with IPI vectorization block encoding for key distribution. The randomness of the generated binary sequence is directly related to the system's security, as our communication process depends on this session key to distribute the actual communication key. As discussed previously regarding vectorization transformation and block size, we set the block size to 4 and generated a 128-bit binary sequence after vectorizing the IPI features of the ECG signal to achieve optimal key performance. We processed ECG signals from the AGING, MITDB, NSRDB, and WRIST databases, as referenced in [28], [36], [48], and [49], within our scheme, and

conducted NIST tests on the generated random binary sequences. The experimental results show that our scheme surpasses others on three metrics across all databases. In Table VI, we present the complete test results, highlighting in bold the areas where our scheme demonstrates superior performance. The results demonstrate that the binary sequence produced by our method possesses sufficient randomness. This randomness allows it to serve as a component of fuzzy commitment, enabling key distribution.

Additionally, we tested and compared the performance of Shannon entropy, collision entropy, and minimum entropy of our scheme under the aforementioned conditions. Fig 11 clearly shows that the performance of our scheme in four databases is superior to other schemes in terms of the three kinds of entropy, especially in the WRIST database, where the entropy measures of our scheme are significantly higher compared to those of other schemes, indicating a better performance. These results indicate that our IPI vectorization block encoding enhances the confidentiality, security, and unpredictability of binary sequences generated in the active state compared to other schemes, thereby ensuring better security for WBSNs.

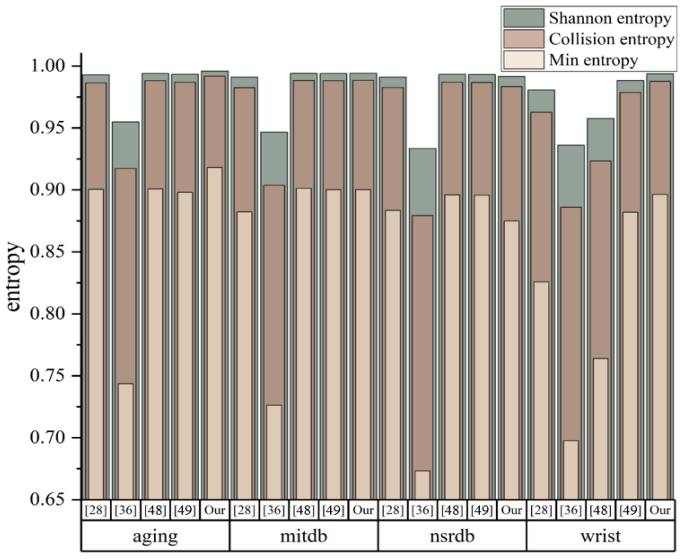


Fig 11. Entropy test in different method
In the entropy test, our method performs better than other methods on multiple databases.

TABLE V
NIST TEST IN DIFFERENT BLOCK SIZE
In the NIST test, better performance is achieved when the block size is set to 4.

Approximate Entropy	Block Frequency	Cumulative Sums	FFT	Frequency	NonOverlapping Template	block size	db
1.0000	0.4766	0.4561	0.8882	0.4766	**0.9469**	1	
1.0000	**0.9985**	**0.9989**	**0.8904**	**0.9985**	0.9161	4	AGING
1.0000	0.9158	0.9048	0.8561	0.9158	0.9289	8	
1.0000	0.8596	0.8305	0.8121	0.8596	0.9341	16	
1.0000	0.3564	0.3459	**0.9312**	0.3564	**0.9528**	1	
1.0000	**0.9963**	**0.9973**	0.8847	**0.9963**	0.9224	4	MITDB
1.0000	0.8495	0.8394	0.8714	0.8495	0.9325	8	
1.0000	0.7526	0.7325	0.8639	0.7526	0.9369	16	
1.0000	0.5114	0.4863	0.9041	0.5114	**0.9431**	1	
1.0000	**0.9954**	**0.9943**	**0.9041**	**0.9954**	0.9178	4	NSRDB
1.0000	0.8813	0.8744	0.8904	0.8813	0.9312	8	
1.0000	0.7580	0.7363	0.8721	0.7580	0.9345	16	
1.0000	0.6409	0.6261	0.8872	0.6409	**0.9405**	1	
1.0000	**0.9970**	**0.9985**	**0.8932**	**0.9970**	0.9218	4	WRIST
1.0000	0.8961	0.8843	0.8754	0.8961	0.9324	8	
1.0000	0.8220	0.8056	0.8783	0.8220	0.9360	16	

TABLE VI
NIST TEST IN DIFFERENT CODING METHOD

Approximate Entropy	Block Frequency	Cumulative Sums	FFT	Frequency	NonOverlapping Template	Runs	Method	db
1.0000	0.9680	0.9748	0.9435	0.9680	0.9168	0.6531	[28]	
1.0000	0.9709	0.9715	0.9829	0.9709	0.8823	0.9782	[49]	
1.0000	0.9856	0.9869	0.9843	0.9856	0.8819	0.9860	[48]	AGING
1.0000	0.6137	0.5789	0.8305	0.6137	0.9421	0.7224	[36]	
1.0000	**0.9985**	**0.9989**	0.8904	**0.9985**	0.9161	0.7595	Our	
1.0000	0.9434	0.9509	0.9535	0.9434	0.9253	0.4333	[28]	
1.0000	0.9895	0.9896	0.9834	0.9895	0.8816	0.9891	[49]	
1.0000	0.9873	0.9880	0.9856	0.9873	0.8810	0.9879	[48]	MITDB
1.0000	0.5924	0.5738	0.8739	0.5924	0.9446	0.5848	[36]	
1.0000	**0.9963**	**0.9973**	0.8847	**0.9963**	0.9224	0.6160	Our	
1.0000	0.9524	0.9524	0.9905	0.9524	0.9037	0.6476	[28]	
1.0000	0.9794	0.9779	0.9912	0.9794	0.8809	0.9735	[49]	
1.0000	0.9759	0.9748	0.9869	0.9759	0.8798	0.9781	[48]	NSRDB
1.0000	0.4261	0.3783	0.9022	0.4261	0.9493	0.6174	[36]	
1.0000	**0.9954**	**0.9943**	0.9041	**0.9954**	0.9178	0.8575	Our	
1.0000	0.7160	0.7407	0.9383	0.7160	0.9034	0.5062	[28]	
1.0000	0.9300	0.9261	0.9805	0.9300	0.8843	0.9805	[49]	
1.0000	0.6232	0.6101	0.9826	0.6232	0.9042	0.6870	[48]	WRIST
1.0000	0.5159	0.4899	0.8638	0.5159	0.9520	0.5797	[36]	
1.0000	**0.9970**	**0.9985**	0.8932	**0.9970**	0.9218	0.7971	Our	

VI. Performance and Security Analysis

A. Key Distribution Performance Analysis

(1).Key distribution performance

Key distribution is critical in WBSNs communications. To achieve secure and convenient key distribution, leveraging the inherent communication means of the human body is advantageous. We modeled body sensors as ECG leads in various positions and used the collected ECG signals for key negotiation among multiple sensors. This section implemented a fast and secure key distribution system in WBSNs using the fuzzy commitment model and vectorization encoding of IPI. To ensure accuracy, we removed unsynchronized and unavailable samples from the four databases and randomly selected 322 samples for validation analysis of the fuzzy commitment model.

In addition to correctly matching all sensors to a system, it is also crucial for WBSNs to differentiate between systems to prevent interference. Fig 12 presents the normalized Hamming distance analysis of signals collected by different leads on the same subject and different subjects, based on 127 random sequences. The normalized Hamming distances between random sequences generated for different subjects follow a normal distribution centered around 0.5, indicating that these sequences are effective in distinguishing between different WBSNs systems. In contrast, our coding method generates predominantly random sequences with normalized Hamming distances ranging from 0 to 0.2 when comparing ECG signals collected from the same subjects using different leads. Moreover, sequences with normalized Hamming distances of 0 (indicating identical sequences) represent more than 20% of all test sequences. These results suggest that these sequences are well-suited for use in WBSNs systems belonging to the same network.

Upon a detailed analysis of the performance of our proposed approach, we identify two crucial parameters: the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) for the key distribution scheme based on fuzzy commitment. FAR represents the probability of incorrectly identifying a non-system sensor as part of the system and thus distributing the correct key to it, whereas FRR represents the probability of incorrectly recognizing a system sensor as a non-system sensor and consequently refusing to distribute the correct key. Fig 13 illustrates the FAR and FRR achievable with varying error correction capabilities of BCH in our solution. At low error correction capability thresholds, the FAR approaches 0. To achieve optimal performance, we selected BCH (127,8,43) as the error correction code for our system, at an Equal Error Rate (EER) point where FAR = 0.052.

(2). Algorithm complexity analysis

Our complexity analysis is carried out in three stages of IPI vectorized block coding, namely: ECG wavelet processing to extract IPI, IPI vectorization transformation, and the final *BS* generation process. As analyzed in[55], the complexity of fast wavelet transform is $O(n)$, where n is the size of the sampled data. The second step is to construct matrix $M1$ for IPI and carry out vectorization transformation. This process does not involve complex matrix-solving problems but requires only the calculation of frequency, one transpose, and one Hadamard product. Therefore, the algorithm complexity is $O(l)$, where l is the number of IPI. The third step is to perform the final coding operation, which requires calculating the mean and variance. The algorithm complexity is also related to the number of IPI ($O(l)$). Since the number of IPI after feature extraction is much smaller than the size of the sampled data, our total algorithm complexity is $O(n)$.

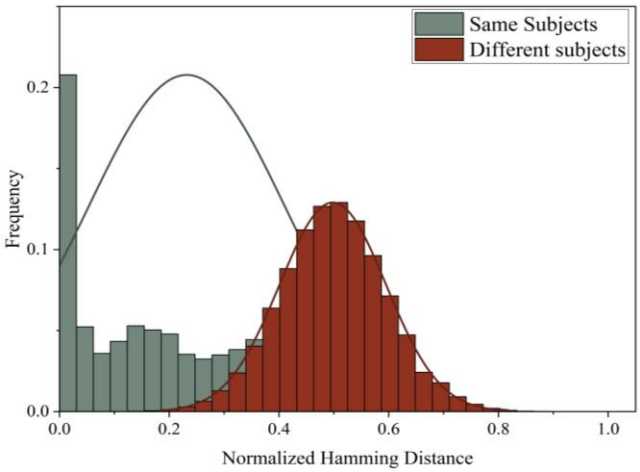


Fig 12. Normalized Hamming Distances of Subjects

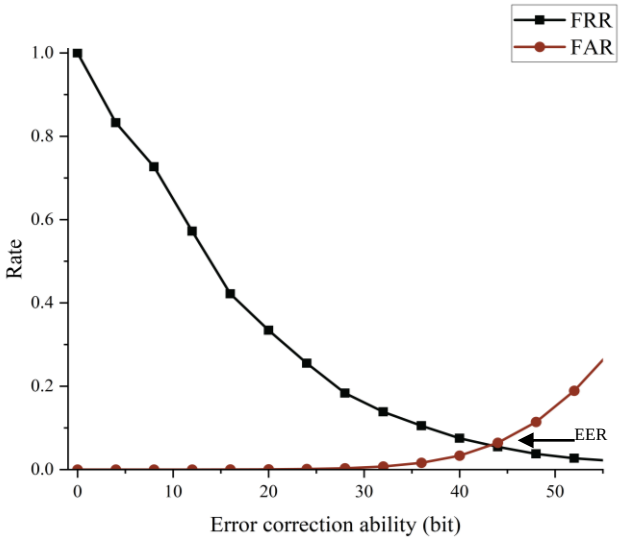


Fig 13. Performance of Key Distribution.

(3). Comparison with State-of-the-Art

TABLE Ⅶ

Comparison of Our Proposed Scheme With [21] [28]

Scheme	[21]	[28]	Our
Biometric	Gait	ECG	ACC,ECG
Main processing algorithm	PCA	DWT	DWT
Main algorithm complexity	$\approx O(n^3)$	$O(n)$	$O(n)$
Security analysisyes	yes	no	yes
Quantization used sample	Multiple	Single	Multiple
Key generation during	activities	resting	activities,resting
User-friendliness	no	no	yes

This study proposes a novel hybrid method for key generation and distribution in WBSNs that addresses the limitations of current methods, which often struggle to balance the computational and energy constraints of sensors with security. We compare our proposed scheme with recent methods using biometric data such as gait and ECG signals in TABLE Ⅶ. Specifically, our scheme combines ACC signals with ECG signals, using wavelet transform as the main processing algorithm in the signal processing phase and IPI vectorized block encoding in the coding phase. The algorithm complexity of this method is about $O(n)$, just as we calculated before, which is significantly lower than that of other methods, such as PCA-based gait analysis ($\approx O(n^3)$) [56]. Unlike schemes that are limited to activity or rest states, our approach effectively generates keys during both activity and rest, enhancing user-friendliness. In addition, our scheme uses multiple samples for quantization during coding, which ensures the robustness of the key generation process. The performance analysis confirmed the superiority of our approach, achieving a 5.23% FAR and demonstrating high entropy and randomness through extensive experiments, including entropy analysis and NIST statistical tests. This dual-key strategy takes advantage of the unpredictability of ACC noise and the individual characteristics of ECG signals, which not only improves the security and efficiency of WBSNs key distribution but also ensures that it is suitable for various physiological states without disturbing users. Therefore, our approach provides a more user-friendly and secure alternative to existing gait-based and ECG-based key generation schemes.

B. Security Analysis

(1). Immutability: The proposed scheme ensures immutability due to the use of hash-based *hash(KEY)* authentication during template transfer. Once the data is transmitted from the sender, any alteration to the template will result in a failure of authentication. This guarantees that the key distribution process remains secure and the integrity of the transmitted data is maintained.

(2). Template Security: During the key distribution process, we use templates as described by Equation (1) to transmit all necessary information. The security of these templates is guaranteed by the randomness of the generated binary sequences (BS). An attacker would need to know all 127 bits of the BS to extract the actual key. Our NIST tests and entropy analysis confirm that the generated BSes exhibits sufficient randomness and high entropy. Additionally, the chaotic nature and variability of heart rate signals further complicate the extraction of ECG signals used to generate the BS, thereby enhancing template security.

(3). Forward and backward safety: Our scheme has strong forward and backward safety because the ECG signal itself has time-varying characteristics. Even if the signal of the current time can be obtained, it is not possible to infer the signal before or after this signal. Similarly, assuming the attacker can obtain the ECG signal collected by a previous user, they cannot infer the signal that the user is currently communicating with based on this prior signal. In our experimental analysis, collision entropy describes this property, ensuring that even if the current key is exposed, previous and future keys will not be compromised. Moreover, the relevant information of the current key cannot be obtained from the previous key. The high collision entropy indicates that our scheme is robust in maintaining both forward and backward security of the key.

(4). Against Impersonation Attacks: The complexity of accurately simulating ACC noise and ECG signals provides significant resistance to such attacks. Recent studies show that ACC signals can be simulated by capturing human movements through computer-aided vision. However, the noise signal used in our scheme, which is based on ACC, is harder to imitate than the ACC signal. ECG signals are equally difficult for impostor nodes to capture. The inherent randomness and variability of these physiological signals make it difficult for attackers to forge the necessary biometric data to fool the system.

(5). Against Replay Attacks: In our scheme, the ECG signal is collected synchronously in real time, and the BS as the session key is a one-time key. Each time the key is distributed, it must be re-collected and encoded. The attacker cannot replay the intercepted template through the corresponding hash match, ensuring it will not be cracked by replay attacks. The dynamic nature of key generation based on current physiological signals ensures that any captured data is useless for future authentication attempts.

(6). Against Brute Force Attacks: Our scheme is robust to brute force attacks, as evidenced by our FAR and FRR analyses. The FAR is close to 0 when the error-correcting capability is set between 1 and 30. Our FAR, which balances security and performance, is 5.23%, indicating a low probability of unauthorized access through exhaustive guessing. Additionally, shortening the key's validity period and implementing other measures can further improve resistance to brute force attacks. The high entropy and complexity of the generated binary sequences further enhance the system's resistance to such attacks.

VII. Conclusions and Future Work

This study presents an innovative hybrid approach for key generation and distribution in WBSNs, utilizing ACC signals noise, ECG signals, and the fuzzy commitment technique. By applying a low-pass filter to extract noise from the ACC signals of the three-axis accelerometer, we generated high-entropy random binary sequences. Leveraging the inherent randomness and unpredictability of this ACC signal noise, we designed a robust key generation scheme. Moreover, we developed an optimized feature extraction and coding scheme based on ECG signals to facilitate secure key distribution between different devices in WBSNs. By synchronously collecting ECG signals from multiple devices and extracting feature vectors based on the IPI, we integrated these common features with fuzzy commitment to achieve efficient and secure key distribution. Our analysis confirmed that the binary sequences generated using acceleration noise and IPI vectorization block encoding exhibit high entropy and robustness. Experimental results demonstrated that the proposed method for extracting feature vectors from IPI is both robust and distinguishable within and

between classes, achieving a FAR of 5.23%, thereby validating the effectiveness of our key distribution method.

Future research will focus on conducting online tests in real-world scenarios using both ACC and ECG signals in conjunction with the proposed key generation and distribution methods. Additionally, we will investigate potential attacks, such as ACC signal posture imitation and ECG signal synthesis using machine vision techniques. Further research will extend the application of these security methods to a broader range of scenarios, aiming to enhance the overall security of devices within WBSNs.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their kind suggestions for improving the quality of this paper.

REFERENCES

[1] T. N. Nguyen, V. Piuri, L. Y. Qi, S. Mumtaz, and W. H. C. Lee, "Guest Editorial Innovations in Wearable, Implantable, Mobile, & Remote Healthcare With IoT & Sensor Informatics and Patient Monitoring," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 5, pp. 2152-2154, May 2023.

[2] I. Nassra and J. V. Capella, "Data compression techniques in IoT-enabled wireless body sensor networks: A systematic literature review and research trends for QoS improvement," *Internet of Things*, vol. 23, Oct 2023, Art. no. 100806.

[3] P. Y. Kong, "Cellular-Assisted Device-to-Device Communications for Healthcare Monitoring Wireless Body Area Networks," (in English), *IEEE Sensors Journal*, vol. 20, no. 21, pp. 13139-13149, Nov 1 2020.

[4] E. Ar-Reyouchi, K. Ghoumid, D. Ar-Reyouchi, S. Rattal, R. Yahiaoui, and O. Elmazria, "Protocol Wireless Medical Sensor Networks in IoT for the Efficiency of Healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10693-10704, Jul 2022.

[5] M. Ramadan and S. Raza, "Secure Equality Test Technique Using Identity-Based Signcryption for Telemedicine Systems," *IEEE Internet of Things Journal*, vol. 10, no. 18, pp. 16594-16604, 2023.

[6] Y. B. Choi, J. S. Krause, H. Seo, and K. E. Capitan, "Telemedicine in the USA: Standardization through information management and technical applications," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 41-48, Apr 2006.

[7] I. R. Galatzer-Levy and J. P. Onnela, "Machine Learning and the Digital Measurement of Psychological Health," *Annual Review of Clinical Psychology*, vol. 19, pp. 133-154, 2023.

[8] K. Ueafuea *et al.*, "Potential Applications of Mobile and Wearable Devices for Psychological Support During the COVID-19 Pandemic: A Review," *IEEE Sensors Journal*, vol. 21, no. 6, pp. 7162-7178, 2021.

[9] Y. Ke, "Location and Tracking Mode of Sports Rehabilitation Training With Self-Powered Sensors Based on Particle Swarm Optimization Algorithm," *IEEE Sensors Journal*, vol. 23, no. 18, pp. 20894-20903, Sep 2023.

[10] S. Yean, B. S. Lee, C. K. Yeo, C. H. Vun, and H. L. Oh, "Smartphone Orientation Estimation Algorithm Combining Kalman Filter With Gradient Descent," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 5, pp. 1421-1433, Sep 2018.

[11] A. Tolba and Z. Al-Makhadmeh, "Wearable sensor-based fuzzy decision-making model for improving the prediction of human activities in rehabilitation," *Measurement*, vol. 166, Dec 2020, Art. no. 108254.

[12] A. R. A. Laaraibi, G. Jodin, D. Hoareau, N. Bideau, and F. Razan, "Flexible Dynamic Pressure Sensor for Insole Based on Inverse Viscoelastic Model," *IEEE Sensors Journal*, vol. 23, no. 7, pp. 7634-7643, Apr 2023.

[13] A. Farrokhi, R. Farahbakhsh, J. Rezazadeh, and R. Minerva, "Application of Internet of Things and artificial intelligence for smart fitness: A survey," *Computer Networks*, vol. 189, Apr 2021, Art. no. 107859.

[14] L. Liang, Y. Duan, J. Che, C. Tang, W. Dai, and S. Gao, "WMS: Wearables-Based Multisensor System for In-Home Fitness Guidance," *IEEE Internet of Things Journal*, vol. 10, no. 19, pp. 17424-17435, 2023.

[15] G. Mehmood, M. Z. Khan, A. K. Bashir, Y. D. Al-Otaibi, and S. Khan, "An Efficient QoS-Based Multi-Path Routing Scheme for Smart Healthcare Monitoring in Wireless Body Area Networks," *Computers & Electrical Engineering*, vol. 109, Jul 2023, Art. no. 108517.

[16] G. Mehmood, M. Z. Khan, M. Fayaz, M. Faisal, H. U. Rahman, and J. Gwak, "An Energy-Efficient Mobile Agent-Based Data Aggregation Scheme for Wireless Body Area Networks," *Cmc-Computers Materials & Continua*, vol. 70, no. 3, pp. 5929-5948, 2022.

[17] 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 Communications Magazine*, vol. 44, no. 4, pp. 73-81, Apr 2006.

[18] G. Zheng *et al.*, "Finger-to-Heart (F2H): Authentication for Wireless Implantable Medical Devices," *IEEE J Biomed Health Inform*, vol. 23, no. 4, pp. 1546-1557, Jul 2019.

[19] S. Umer, A. Sardar, R. K. Rout, M. Tanveer, and I. Razzak, "IoT-Enabled Multimodal Biometric Recognition System in Secure Environment," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21457-21466, Dec 2023.

[20] D. M. Jiang, G. H. Zhang, O. W. Samuel, F. H. Liu, and H. Xiao, "Dual-Factor WBAN Enhanced Authentication System Based on Iris and ECG Descriptors," *IEEE Sensors Journal*, vol. 22, no. 19, pp. 19000-19009, Oct 2022.

[21] F. M. Sun, W. L. Zang, H. H. Huang, I. Farkhatdinov, and Y. Li, "Accelerometer-Based Key Generation and Distribution Method for Wearable IoT Devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1636-1650, Feb 2021.

[22] Y. Su, Y. Li, and Z. Cao, "Gait-Based Privacy Protection for Smart Wearable Devices," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 3497-3509, 2024.

[23] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay, and Y. T. Zhang, "Heartbeats Based Biometric Random Binary Sequences Generation to Secure Wireless Body Sensor Networks," *IEEE Trans Biomed Eng*, vol. 65, no. 12, pp. 2751-2759, Dec 2018.

[24] J. Q. Zhang, Y. S. Zheng, W. T. Xu, and Y. Y. Chen, "H2K: A Heartbeat-Based Key Generation Framework for ECG and PPG Signals," *IEEE Transactions on Mobile Computing*, vol. 22, no. 2, pp. 923-934, Feb 2023.

[25] J. F. Valenzuela-Valdés, M. A. López, P. Padilla, J. L. Padilla, and J. Minguillon, "Human Neuro-Activity for Securing Body Area Networks: Application of Brain-Computer Interfaces to People-Centric Internet of Things," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 62-67, Feb 2017.

[26] G. Revadigar, C. Javali, W. T. Xu, A. V. Vasilakos, W. Hu, and S. Jha, "Accelerometer and Fuzzy Vault-Based Secure Group Key Generation and Sharing Protocol for Smart Wearables," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 10, pp. 2467-2482, Oct 2017.

[27] A. Brüsch, N. Nguyen, D. Schürmann, S. Sigg, and L. Wolf, "Security Properties of Gait for Mobile Device Pairing," *IEEE Transactions on Mobile Computing*, vol. 19, no. 3, pp. 697-710, Mar 2020.

[28] H. Chizari and E. Lupu, "Extracting Randomness from the Trend of IPI for Cryptographic Operations in Implantable Medical Devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 875-888, Mar-Apr 2021.

[29] G. L. Zheng *et al.*, "Multiple ECG Fiducial Points-Based Random Binary Sequence Generation for Securing Wireless Body Area Networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 3, pp. 655-663, May 2017.

[30] S. D. Bao, C. C. Y. Poon, Y. T. Zhang, and L. F. Shan, "Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 6, pp. 772-779, Nov 2008.

[31] S.-D. Bao, Y.-T. Zhang, and L.-F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," *Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and*

Biology Society. IEEE Engineering in Medicine and Biology Society. Annual Conference, vol. 2005, pp. 2455-8, 2005.

[32] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," in *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on*, 2003.

[33] A. L. Goldberger, D. R. Rigney, and B. J. West, "Chaos and Fractals in Human Physiology," *Scientific American*, vol. 262, no. 2, pp. 42-49, 1990.

[34] M. G. Signorini, F. Marchetti, and S. Cerutti, "Applying nonlinear noise reduction in the analysis of heart rate variability," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 2, pp. 59-68, Mar-Apr 2001.

[35] 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.

[36] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *2011 Proceedings IEEE INFOCOM*, 2011.

[37] R. M. Seepers, J. H. Weber, Z. Erkin, I. Sourdis, and C. Strydis, "Secure key-exchange protocol for implants using heartbeats," *Proceedings of the ACM International Conference on Computing Frontiers*, 2016.

[38] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. De Zeeuw, "Enhancing Heart-Beat-Based Security for mHealth Applications," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 1, pp. 254-262, Jan 2017.

[39] D. Kirovski, M. Sinclair, and D. Wilson, "The Martini Synch: Device Pairing via Joint Quantization," *2007 IEEE International Symposium on Information Theory*, 2007.

[40] Q. Jiang, X. Huang, N. Zhang, K. Zhang, X. Ma, and J. Ma, "Shake to Communicate: Secure Handshake Acceleration-Based Pairing Mechanism for Wrist Worn Devices," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5618-5630, 2019.

[41] C. T. Cornelius and D. F. Kotz, "Recognizing whether sensors are on the same body," *Pervasive and Mobile Computing*, vol. 8, no. 6, pp. 822-836, Dec 2012.

[42] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu, "Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure On-Body Device Communication," in *2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2016.

[43] W. T. Xu, J. Q. Zhang, S. Q. Huang, C. W. Luo, and W. Li, "Key Generation for Internet of Things: A Contemporary Survey," *Acm Computing Surveys*, vol. 54, no. 1, Apr 2021, Art. no. 14.

[44] D. Jarchi and A. J. Casson, "Description of a Database Containing Wrist PPG Signals Recorded during Physical Exercise with Both Accelerometer and Gyroscope Measures of Motion," vol. 2, no. 1, p. 1, 2017.

[45] 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," *American Journal of Cardiology*, vol. 93, no. 3, pp. 381-385, Feb 2004.

[46] B. M. Appelhans and L. J. Luecken, "Heart rate variability as an index of regulated emotional responding," *Review of General Psychology*, vol. 10, no. 3, pp. 229-240, Sep 2006.

[47] M. P. Tulppo, T. H. Makikallio, T. E. Takala, T. Seppanen, and H. V. Huikuri, "Quantitative beat-to-beat analysis of heart rate dynamics during exercise," *The American journal of physiology*, vol. 271, no. 1 Pt 2, pp. H244-52, 1996 1996.

[48] 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. 176-82, Jan 2012.

[49] R. M. Seepers, J. H. Weber, Z. Erkin, I. Sourdis, and C. Strydis, "Secure key-exchange protocol for implants using heartbeats," presented at the Proceedings of the ACM International Conference on Computing Frontiers, Como, Italy, 2016. Available: https://doi.org/10.1145/2903150.2903165

[50] G. A. Moody and R. G. Mark, "The impact of the MIT-BIH arrhythmia database," *IEEE Engineering in Medicine and Biology Magazine*, vol. 20, no. 3, pp. 45-50, May-Jun 2001.

[51] A. Juels and M. J. A. Wattenberg, "A Fuzzy Commitment Scheme," *Proc. ACM Conference on Computer and Communication Security (CCS'99)*, pp. 28-36, 1999.

[52] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081-1088, Sep 2006.

[53] 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. E215-20, 2000 Jun 2000.

[54] A. Schumann and K. J. Bär, "Autonomic aging - A dataset to quantify changes of cardiovascular autonomic function during healthy aging," *Scientific Data*, vol. 9, no. 1, Mar 2022, Art. no. 95.

[55] G. J. B. o. t. A. M. S. Strang, "Wavelet transforms versus Fourier transforms," *Bull. Am. Math. Soc.,*, vol. 28, pp. 288-305, 1993.

[56] A. Sharma, K. K. Paliwal, S. Imoto, and S. Miyano, "Principal component analysis using QR decomposition," *International Journal of Machine Learning and Cybernetics*, vol. 4, no. 6, pp. 679-683, 2013/12/01 2013.