Extracting Randomness From The Trend of IPI for Cryptographic Operators in Implantable Medical Devices

Hassan Chizari
Emil Lupu

Abstract

Achieving secure communication between an Implantable Medical Device (IMD) and a gateway or programming device outside the body has showed its criticality in recent reports of vulnerabilities in cardiac devices, insulin pumps and neural implants, amongst others. The use of asymmetric cryptography is typically not a practical solution for IMDs due to the scarce computational and power resources. Symmetric key cryptography is preferred but its security relies on agreeing and using strong keys, which are difficult to generate. A solution to generate strong shared keys without using extensive resources, is to extract them from physiological signals already present inside the body such as the InterPulse Interval (IPI). The physiological signals must therefore be strong sources of randomness that meet five conditions: *Universality* (available on all people), *Liveness* (available at any-time), *Robustness* (strong random number), *Permanence* (independent from its history) and *Uniqueness* (independent from other sources). However, these conditions (mainly the last three) have not been systematically examined in current methods for randomness extraction from IPI. In this study, we firstly propose a methodology to measure the last three conditions: Information secrecy measures for *Robustness*, Santha-Vazirani Source *delta* value for *Permanence* and random sources dependency analysis for *Uniqueness*. Then, using a large dataset of IPI values (almost 900,000,000 IPIs), we show that IPI does not have *Robustness* and *Permanence* as a randomness source. Thus, extraction of a strong uniform random number from IPI values is impossible. Thirdly, we propose to use the trend of IPI, instead of its value, as a source for a new randomness extraction method named Martingale Randomness Extraction from IPI (MRE-IPI). We evaluate MRE-IPI and show that it satisfies the *Robustness* condition completely and *Permanence* to some level. Finally, we use the NIST STS and Dieharder test suites and show that MRE-IPI is able to outperform all recent randomness extraction methods from IPIs and achieves a quality roughly half that of the AES random number generator. MRE-IPI is still not a strong random number and cannot be used as key to secure communications in general. However, it can be used as a one-time pad to securely exchange keys between parties of communication. The usage of MRE-IPI will thus be kept at a minimum and reduces the probability of breaking it. To the best of our knowledge, this is the first work in this area which uses such a comprehensive method and large dataset to examine the randomness of physiological signals.

1. Introduction

Implantable Medical Devices (IMDs) provide a new perspective to healthcare systems and numerous benefits for patients as they enable early detection of complications, early identification of at-risk patients and early recognition of suboptimal IMD functions [1]. Moreover, with IMDs, providing healthcare without affecting the patient's life becomes feasible (e.g. Diabetics and Dementia patients [2]). It also has been shown that remote monitoring of the patients using IMDs is very cost effective for the healthcare system [3].

There are three classes of implants: Fashion Trend, Life Enhancing and Life Preserving [2]. The first category belongs to the implants which are designed to make the life more comfortable such as pet chips [4] and key implants for unlocking doors or computers [5]. This category is usually based on RFID devices. Life enhancing implants are devices such as cochlear or dental implants. This category of implants is mostly without battery, though a new generation of devices are equipped with battery and sensors to collect information from the body and send it outside (e.g. collecting PH level and pressure in a knee [6]). The third category is life preserving implants. In this category, implants are mostly equipped with batteries and, in newer generations, are actively communicating with the outside world and exchange information with their gateway device. The focus of this paper is on the life preserving IMDs which have sensing, computation and communication capability.

Once an IMD is able to communicate by sending sensed data and receiving commands, the security of the device becomes a main concern. The security of IMDs is an emerging research area and many studies have highlighted its criticality. For instance, [7] showed how an attack to a brain's IMD could take control of the implant and alter the victim's emotions. In another example, Reuters reported vulnerabilities in insulin pumps created by Johnson & Johnson [8], where an attacker is able to intercept the communication and/or cause the wrong dosage of insulin to be delivered. More recently, the Guardian [9] reported that more than half a million people may be at risk because of the vulnerabilities found in St. Jude pacemakers. The challenge in securing communication between an IMD inside the body and a gateway outside the body is that usage of asymmetric cryptography is not preferred [10], [11]. This is due to the resource hungry nature of public key cryptography, while IMDs are highly restricted in size [12], material [13], energy usage [14] and computation and communication power [15]. Thus, many studies proposed symmetric encryption as a low resource intence cryptosystem for IMDs.

Based on the report published by WhiteScope [16], more than 8000 vulnerabilities have been found in examining only seven models of pacemakers. The main reasons for this high number of vulnerabilities were, firstly, not using encryption methods at all or secondly, using static (permanent) keys in encryption. To use temporary keys, IMDs should be able to generate agreed strong cryptographic keys each time the secure communication is needed. A solution proposed in [17], amongst others, is for the IMD and the gateway/programmer device to measure a body physiological signal at the same time and create a secret key from it. Then, without any key exchanging process, they are sharing the same secret key. This method is called Physiological Value-Based (PVS) security [18]. In this scheme, the security of the cryptosystem depends on the randomness of the physiological signal which is used to create a strong secret key.

Several physiological signals have been proposed in the literature as a source of randomness for generating secret keys including electroencephalograms (EEG) [19], electrocardiogram (EKG) [20] and Photoplethysmogram (PPG) [21], Electrocardiography (ECG) [22] and InterPulse Intervals (IPI) [17]. IPI is the time difference between two peaks of an ECG signal. As shown in Fig. 1, there are three peaks for every heart beat in the ECG signal named Q, R and S. So, three IPI values could be extracted from the time difference between each two corresponding peaks (Q-Q, R-R, S-S). Among these, R has the highest peak and is the easiest one to detect. So in the rest of this paper we refer to the R-R time difference whenever IPI is mentioned.

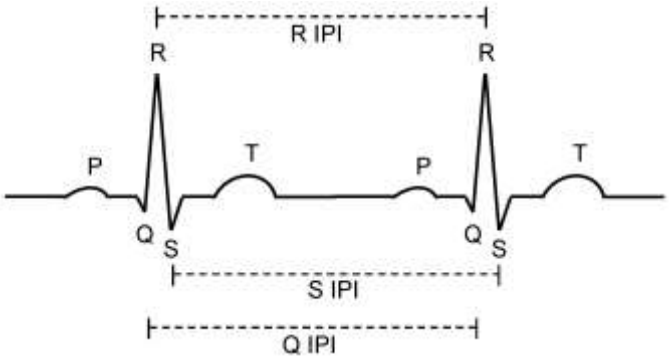


Fig. 1: QRS peaks of Heartbeat (Source [23])

The contributions of this paper are, firstly, proposing a comprehensive methodology to examine the randomness of physiological signals. Although we focus here on IPI, the methodology can be used more broadly on other signals as well. Secondly, using a large dataset with almost 900,000,000 IPI records, we show that despite current claims, IPI is not a strong source of randomness. Thirdly, we develop a new randomness extraction method using a Martingale Stochastic Process applied to IPI trend values, which proves to be stronger than other methods proposed in the literature. To the best of our knowledge, this is the first work in this area that introduces and uses a comprehensive evaluation method to examine the strength of a physiological signal as a source of randomness.

This paper is organized as follows: in the next section, we discuss the assumptions and requirements for the PVS method. Next, we present current randomness extraction methods from IPI. After that, we evaluate the randomness of IPI using a comprehensive methodology. Then, we present our proposed randomness extraction method followed by evaluating its strength compared to current methods. In final section, we conclude the paper by summing up our findings.

2. Requirements

In PVS methodology, the gateway outside of the body initiates a request for communication to the IMD. Then, both devices start to measure a physiological signal. There are several assumptions here. Firstly, the physiological signal should be measurable from inside and outside the body. However, to preserve the privacy and security of IMD, the physiological signal should not be measurable from a distance of the body. This is based on the idea that if a device gets very close to the body, preferably touching the skin for a specific duration of time, it means that the gateway can be trusted. So, the physiological signal should be measurable from outside of the body but not from a distance.

The second assumption in PVS methodology is that measuring the PVS signal does not consume a considerable amount of the implant's energy. Since IMDs are limited in their computing resources including energy, measuring physiological signals should be practically feasible. The third assumption is that the gateway and the IMD are synchronized i.e. that they measure the physiological signal at the same time in order to produce the same key. Based on the type of signal used, a soft or a hard synchronization may be needed. Again, due to the limitations in IMDs, soft synchronization is more feasible as it needs less resources compared to a hard synchronization. After generating the secret key in both devices, if it is strong enough, it can be used as a session key. Otherwise, it can be used to exchange a strong session key with the gateway. Among physiological signals, IPI can be easily measured inside and outside of the body. Touching the body would be enough and measuring the IPI does not require additional equipment such as for EEG signals. IPI can also be collected with soft synchronization as after handshaking, both devices need to wait for the first heartbeat R-peak to start the measurement. The question that remains is how strong will be the secret key generated from IPI?

A physiological signal is a good source of randomness for generating secret keys if it satisfies five conditions [24]. The first condition is the *Universality* referring to the availability of the signal on all people. The second condition is its *Liveness* that is its availability for measurement anytime anywhere. The third condition is that the extraction of a new secret key should be always possible from the physiological signal (*Permanence*). For example, if the secret key s_1 is generated from a physiological signal at the time t_1, s_n generated at time t_n should not be guessable based on $\{s_1,s_2,...,s_{n-1}\}$. If a physiological signal does not have the feature of *Permanence*, it can only be used once or very occasionally, because repetitive usage of it provides enough information for an adversary to guess it. The next condition is its *Uniqueness*, which means that the physiological signal on two different subjects should be accounted as two independent sources of randomness. Considering the availability of physiological signals for the subject *i* ($p_i = \{s_{i,1},s_{i,2},...,s_{i,n}\}$), $s_{j,n}$ is the physiological signal at time *n* for subject *j*. Based on the *Uniqueness* condition, $s_{j,n}$ (subject *j*) should not be guessable based on information (p_i) from subject *i*. *Robustness* is the last condition which shows that computationally guessing the secret key should not be feasible whether or not the adversary has some information about the physiological signal.

The *Robustness* of a source is calculated using information secrecy measures, which determine the strength of the secret key against an adversary who tries to guess it. Considering the knowledge of the adversary of the secret key, three scenarios can be distinguished. In the best-case scenario, the adversary does not have any information about the secret key and tries to guess it blindly. This situation is called *Perfect Secrecy*. In the second scenario, (*Conditional Secrecy*), the adversary has some information correlated with the key. *Unconditional Secrecy* is the worst-case scenario where adversary knows the distribution histogram of the secret keys. This helps adversary to find which values could be the best guess for determining the secret key. Different methods are used to measure the strength

of the secret key in each of these scenarios. Furthermore, the *Probabilistic Bound* is a fourth information secrecy measure, which shows the distance between the secret key distribution and a uniform distribution [25].

Among physiological signals, IPI has some unique properties which make it one of the methods most often proposed in the literature to be used as the source of randomness for generating secret keys. Firstly, it has the condition of *Universality* as everyone has heartbeat. There are two exceptions here. First one is the flat line heart pulse in emergency situation and the second one is the controlled heartbeat given by a peacemaker. Both of these situations are excluded from the scope of this article. The second property of IPI which makes it a good source of randomness is that it has the *Liveness* condition as well, as the heartbeat signal is always available for everyone (excluding two situations which mentioned above). Thirdly, the detection of IPI does not need complex hardware or software analysis and is simple to implement in an IMD. Lastly, it can be measured in almost every location inside the body and outside the body by touching the skin. So, if IPI is a strong source of randomness, it can be used in a cryptosystem. Although it has been claimed in many studies that IPI is a strong randomness source, its *Permanence*, *Uniqueness* and *Robustness* have not been examined.

3. Related Work

Using IPI as a source of randomness has been proposed by [17], where a random extraction algorithm is needed to convert IPI value to a random number. A few randomness extractor algorithms from IPI have been proposed in the literature including using the XOR function [26], gray-coding [27] and using the frequency domain [28], [24], [29]. In some studies, a combination of algorithms is used for randomness extraction. For instance, [30], [31], [32] used accumulation, modulo, contract mapping and gray-coding for the extractor and [33] proposed a combination of concatenation, quantisation and gray-coding.

Regardless of the extraction method used, it needs to be evaluated for the quality of the generated randomness. Several extracting methods did not perform any randomness test to examine the quality achieved (e.g. [34], [35], [28], [24], [36], [37], [29]). Other randomness extraction studies make an attempt to measure the quality of the proposed method. However, in these works, two aspects have been somewhat ignored. To evaluate the quality of a randomness extractor, the dataset and the methodology of evaluation are the key points. For instance, [27] evaluated the randomness property of their algorithm with only 5 minutes of ECG data of 10 subjects using NIST Statistical Test Suite (STS) [38] randomness test. [30], [31], [32] tested their algorithms using 5 minutes of ECG signal of 40 subjects with NIST STS. In another work, [22] used a histogram analysis on 1500 consecutive IPI values. [39] tested their proposed methods with 100 subjects' ECG data with Entropy test. [33], to evaluate the randomness of algorithms, used Temporal Ratio [40] method over 5 minutes ECG data of 50 subjects.

So current evaluation methods for examining the randomness of IPI are limited to using a few randomness tests functions against a very small dataset of IPI values. In order to have a complete evaluation of the strength of a randomness source, first of all, conditions such as *Permanence*, *Uniqueness* and *Robustness* (including *Perfect Secrecy*, *Conditional Secrecy*, *Unconditional Secrecy* and *Probabilistic Bound*) of the random source must be examined. Secondly, a large data set of IPIs is needed for evaluation of aforementioned measures. In all previous works, the maximum number of subjects to examined were 100 and the largest number of IPI readings from one subject was 1500 consecutive values. This is far below the number of IPI values which are needed to examine the strength of randomness. For instance, to measure the *Unconditional Secrecy* in *Robustness* condition (Min-Entropy [41] of a string with size 16 which will be discussed later), considering the bestcase scenario where the distribution of the source is uniform, at least $1000 * 2^{16} = 65{,}536{,}000$ samples of IPIs are needed to provide a confidence interval of 95% in the result. None of the current randomness extraction methods from IPI used such methods and large datasets to evaluate their algorithms. In contrast to previous works (e.g. [34], [35], [28], [24], [36], [37], [29]), we gathered a large dataset of IPI values. Moreover, we propose methods for measuring all the conditions to examine the strength of the IPI as a randomness source. Additionally, we develop a randomness extraction algorithm, compare its strength against these conditions and report it.

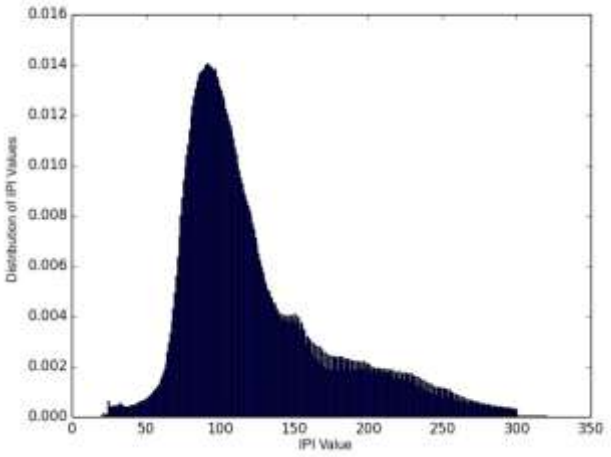


Fig. 2: Histogram analysis of IPIs

4. IPI Randomness

A. Dataset

Using PhysioNet [42], we have created a dataset of IPIs containing 4338 subjects and a total of 895,621,566 IPI values. This dataset comprises a wide range of subjects including healthy subjects resting, healthy subject during Cardio test, subjects with heart problem and failure, infants, children, young, middle age and senior subjects both male and female. We did not restrict the dataset selection from PhysioNet's datasets and the aim was to collect as much as possible IPI data. Whenever possible, the IPI signal is obtained from audited signal files (ATR files), or from non-audited annotation files (QRS, WQRS, ECG and XYZ files). Otherwise, using the QRS procedure of PhysioNet in Matlab, IPIs are extracted from DAT files.

We have extracted the IPI distribution histogram from this dataset (see Fig. 2). The minimum value of IPI in this histogram is 20 which is equivalent to 300*bpm* = 60/0.20 (heartbeat per minute) and the maximum is 330, equivalent to 18*bpm* = 60/3.30. To convert an IPI value to a binary representation, an 8-bit string is used for conversion of *ipi* = *IPI* − 20. We subtracted IPI from 20, so *ipi* starts from 0. Thus, the *ipi* value will be from 0 to 310, which requires 9 bits to represent in binary form. However, as shown later in the paper, the most significant bit *ipi* does not provide much randomness and has been removed. So, in the following sections and the remainder of this work we use an 8-bit representation of the *ipi* value.

B. String Size

To apply the measures of *Permanency*, *Uniqueness* and *Robustness*, we need to consider the string size of concatenated measures. Considering a series of IPI values, we define the string $Z_k = [ipi_1 \cdot ipi_2 \cdot ... \cdot ipi_n]$ as the concatenation of $ipi_j = \{0,1\}^k$, where k is the number of bits from each *ipi* value ($0 < k \leq 8$). For example, consider the series of IPI values: 160, 125, 132, 171, 148 and 130. Then, deducting 20 will give us *ipi* = {140,105,112,151,128,110} and using only the two least significant bits of each *ipi* (k = 2) and concatenating them, we obtain Z_2 = [000100110010]. To examine the randomness of Z_2, all the measurement methods need the distribution of bits in Z_2. If we look at $s = \{0,1\}^1$ for Z_2, we have $D_{Z2,1} = \{8,4\}$, which means 8 zeros and 4 ones. For the distribution of the string $s = \{0,1\}^2 = \{00,01,10,11\}$, there are four combinations to consider. To calculate $D_{Z2,1}$, Z_2 is parsed twice. In the first parse, we have $a_{Z2,1}$ = {00,01,00,11,00,10}. To make sure that all possible patterns of bits in Z_2 have been observed, we use the circulation method which has been used in several randomness test suites (e.g. [43], [44]) to create the distribution histogram. Thus, we go to the second parse and rather than starting from the first bit in Z_2,

we start from the second bit and then we have $a_{Z2,2}$ = {00,10,01,10,01,00}. For the last bit in Z_2, we concatenate it with the first bit of Z_2 to have 00 at the end of $a_{Z2,2}$. Now, looking at both $a_{Z2,1}$ and $a_{Z2,2}$, we have $D_{Z2,2}$ = {5,3,3,1}. With the same process, when s = {0,1}^{3}, three parses on Z_2 will be performed and the distribution of Z_2 will be $D_{Z2,3}$ = {2,3,2,1,3,0,1,0}. In theory, to calculate the distribution for string s = {0,1}^{n}, n must be $1 \leq n < \infty$. However, in practice, the maximum size of n is associated with the size of dataset. As discussed in the first section, the maximum value for n in this article is 16.

C. Robustness

IPI as a source of randomness has the robustness property if knowing its probabilistic distribution (partially or fully) would not help in predicting its next value. Based on the information secrecy measures [25], we measure *Perfect Secrecy* by Shannon Entropy (Eq. 1) [45] which quantifies the encoded length of the source. In this mode, the adversary has no knowledge from the distribution of the source. We measure *Conditional Secrecy* using Renyi Entropy [46] or its descendant Collision Entropy (Eq. 2) [47] which bounds the collision probability between samples. The second measure of *Conditional Secrecy* is Guessing Entropy (Eq. 3) [48] which shows the difficulty of guessing the value of a random variable. *Unconditional Secrecy* quantifies unpredictability of the source and we measure it using Min-Entropy (Eq. 4) [41]. Indeed, in *Unconditional Secrecy*, the adversary has complete knowledge of the distribution histogram of the random source. So, it knows which output from the random source has the highest probability to occur. The last information secrecy measure is *Probabilistic Bounds* which calculates the distance between the distributions of the random source and uniform distribution over the same range (Eq. 5). Considering $X \in \{0,1\}^n$, a randomness extractor Ext : $\{0,1\}^n \rightarrow \{0,1\}^k$ such that $Ext(X)$ is distributed in $\{0,1\}^k$, then the entropies of a random variable X are defined as:

$$H_{Sh}(X) = -\sum_{x \in R(X)} Pr[X = x].log(Pr[X = x]) \qquad (1)$$

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

$$G(X) = \sum_{x \in R(X)} Pr[X = x](x + 1) \qquad (3)$$

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

$$||P_x - P_y||_1 = \sum_{x \in R(X)} |P_x[X = x] - P_y[X = x]| \qquad (5)$$

Many researchers used all the 8 bits of an IPI (e.g. [34]) as the source of randomness, however, some studies are only considering a subset. For instance, [35], [36] used the first 4 bits of an IPI and [39] used the first 2 bits of the IPI. To identify which combination of bits of an IPI is the best source for randomness, in all measurements, we examined 8 scenarios, where in the first scenario only one bit (the least significant bit) is the source of randomness. Similarly, in scenario n ($n \in \{1..8\}$), the first n least significant bits of IPI are used as the source of randomness. Corresponding to these 8 scenarios, we created 8 datasets from the main *ipi* database. The first dataset contains the first least significant bit of an IPI. Dataset No. 2 contains the two least significant bits of an IPI and so on until Dataset No. 8 which contains all the 8 bits of the IPI value.

The result of Shannon Entropy analysis of IPI is presented in Fig. 3. As shown, the dataset which contains the two least significant bits of IPI (Dataset 2) has the highest Shannon Entropy value. It is also clear that even by increasing the length of the string in the entropy calculation, the Shannon Entropy of dataset 2 is still close to one. This makes sense as the main source of randomness in IPI is the small range of fluctuations between IPI values. The worst Entropy belongs to dataset 8 where all 8 bits of IPI are being used.
As Dataset 2 has a Shannon Entropy of almost 1, in the condition of *Perfect Secrecy* where the adversary has zero knowledge about the random source distribution, it has almost perfect random quality. The next step is to measure the entropy when the adversary has partial information about the random source (*Conditional Secrecy*).

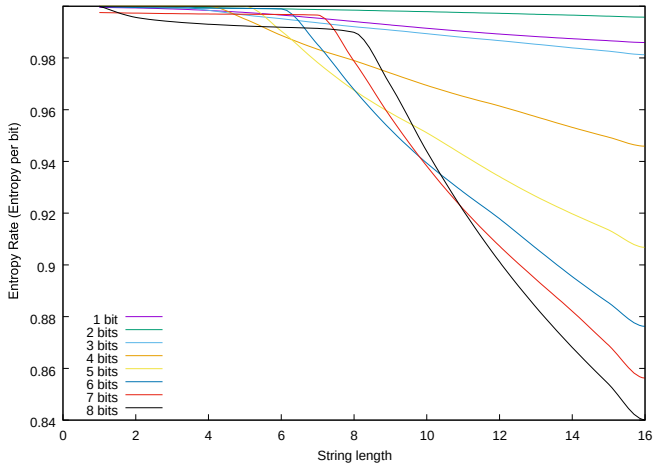


Fig. 3: Shannon Entropy of selected bits of IPI in various string lengths

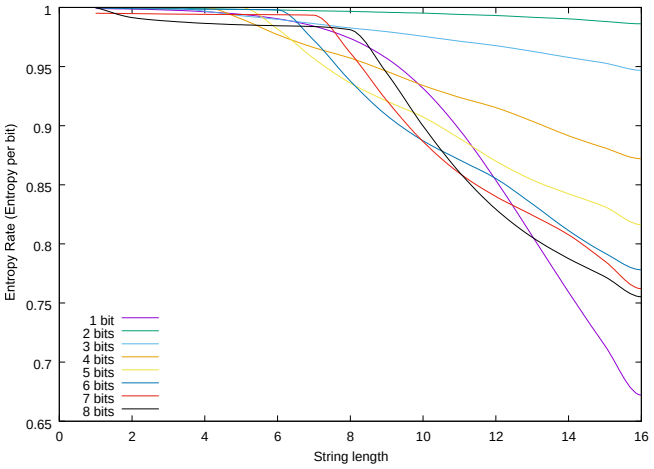


Fig. 4: Collision Entropy of selected bits of IPI in various string lengths

Fig. 4 shows the Collision Entropy results which are almost similar to those of the Shannon Entropy with a small decrease. Once again, Dataset 2 has the highest entropy value and up to the string length of 16 is still over 0.95. Collision Entropy shows the diversity of string patterns in the dataset and thus, Dataset 2 shows a very high diversity. Collision Entropy or in general Renyi Entropy is a measure for *Conditional Secrecy* where the adversary knows a value that has some correlation with the random value. In this situation, also, Dataset 2 shows an almost perfect form of randomness.

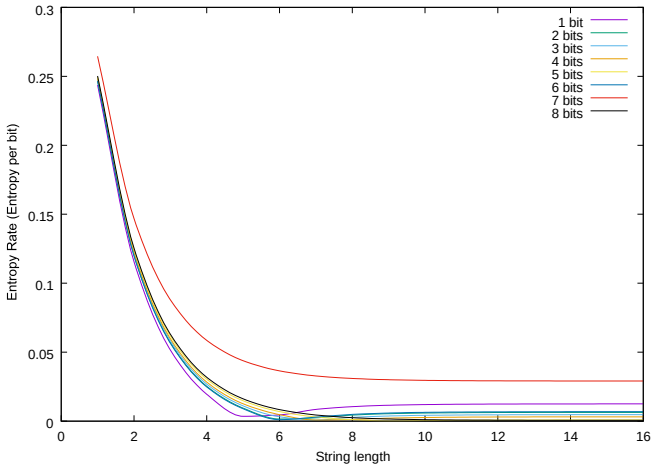


Fig. 5: Guessing Entropy of selected bits of IPI in various string lengths

The second measure of *Conditional Secrecy* is the Guessing Entropy (Fig. 5), where the value of entropy is subtracted from 0.5. The guessing entropy shows the difficulty of guessing the random value and the entropy rate of the guessing entropy is the probability of guessing the right value for one bit. So, the value 0.5 for the guessing entropy rate shows that the adversary is not able to have a good guess about the bit and the chance to be correct is 50%. Thus, we used 0.5
as the benchmark line and deduct the guessing entropy rate from it. Now a value of zero in the curve means that the probability of guessing the next bit is 0.5. By increasing this value, the probability of guessing the next bit is increasing. As shown, for all datasets, the Guessing Entropy (subtracted from 0.5) is very close to zero which means the probability of guessing the next output from the source is 0.5. In this test, the closest values to 0 are for datasets 2,3,4 and 5.

Min-Entropy is the measure of *Unconditional Secrecy*, where the adversary knows the distribution histogram of the random source. Min-Entropy results (Fig. 6) shows that IPI is not performing well in almost all datasets. As shown, the value of the entropy rate drops to lower than 0.8 when the string size increases to 16 in all datasets. However, Dataset 2 still has the highest Entropy value compared to the others. Min-Entropy is a measure of the predictability of the string, where values close to one indicate that the source is unpredictable. For IPI these results show that the source is not highly unpredictable.

The last step in analysing the *Robustness* of the randomness source is measuring the *Probabilistic Bound*. In this process, we calculate the distance between the random variable and a uniform distribution using Eq. 5. A value close to zero denotes a smaller distance to a uniform distribution which means better value for the *Probabilistic Bound*. As shown in Fig. 7, the closest dataset of IPIs to a uniform distribution belongs to Datasets 1 and 2. Especially, in Dataset 1, in all string lengths, the cumulative distance to a uniform distribution is less than 0.1.

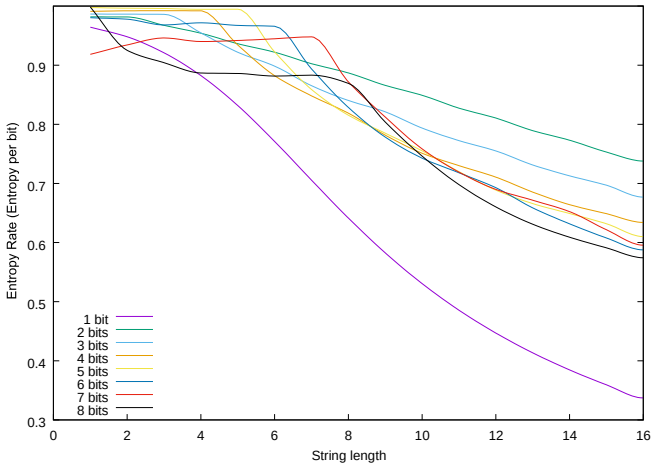


Fig. 6: Min-Entropy of selected bits of IPI in various string lengths

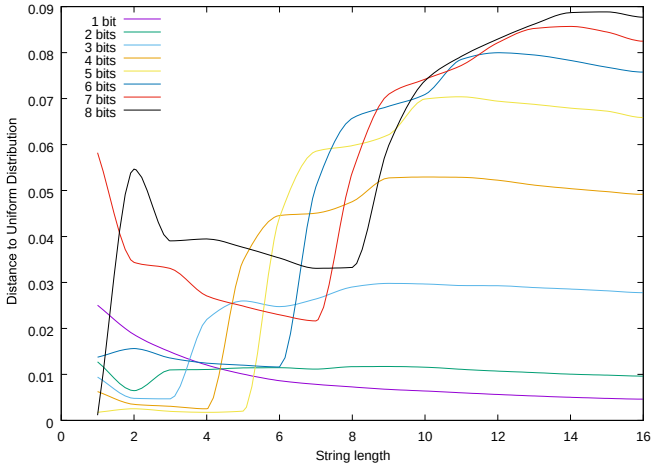


Fig. 7: Uniformity Check for selected bits of IPI in various string lengths

The *Robustness* analysis of IPI using the information secrecy measures reveals two points. Firstly, that if the adversary has no knowledge or limited knowledge about the distribution of the IPI, then the IPI can be used as a very robust source of randomness. However, it seems reasonable to consider that the histogram of the IPI distribution is not hard to collect (see Fig. 2). If the adversary has the knowledge about the IPI distribution histogram, then the IPI is not a very robust source of randomness despite the claim made by many researchers (e.g. [23]). The second point from the *Robustness* analysis is that Dataset 2, which contains the two least significant bits of IPI values, is a more robust randomness source compared to the other datasets.

D. Permanence

IPI as a randomness source has the *Permanence* condition if knowing the history of the heartbeat of one person would not help in predicting his/her future heartbeats. To measure the *Permanence*, we propose to use the Santha-Vazirani method. A randomness source is called a Santha-Vazirani source (SV-source) [49] if the outcome of last generated bit is related to the previous outcomes.
For source X and $\delta \in [0,1]$, we have:

$$\forall i \in n, \forall x_i \in \{0,1\} \rightarrow \frac{1-\delta}{2} \leq Pr[X_i = x_i | \forall x_{i-1}] \leq \frac{1+\delta}{2} \quad (6)$$

where δ is the bias for the new bit x_i, which has some dependencies to the previous bits in the source $\{0,1\}^{i-1}$. In a simpler form we have:

$$\forall x, y \in \{0,1\}^n \rightarrow \frac{Pr[X = x]}{Pr[Y = y]} \leq \frac{1+\delta}{1-\delta} \quad (7)$$

The best possible δ value is zero for any string length which demonstrates that the source is not SanthaVazirani. If δ is equal to zero, the probability of having zero or one is always 0.5, no matter how much data is available. To evaluate the predictiveness of source *X* from Eq. 7, we calculated the maximum and minimum of $Pr[X = x]$ for $\forall x \in \{0,1\}^n$ where $n = 1..16$ using the 8 datasets of IPI values. Then, using Eq. 7, we calculated the δ value of SV-source and results are presented in Fig. 8.

As shown in Fig. 8, IPI is a SV-source as there is a great dependency of the new outcome from the source to its history. Once again, Dataset 2 has the lowest δ value compared to other datasets. However, for all the datasets, when the string length is more than 10, δ is almost equal to one. This means that with enough history, the adversary is able to predict the next random value with the probability very close to 1.

It has been mathematically proven that the extraction of a uniform random bit from a SV-source is impossible [49]. From this, we conclude that the IPI value has not the condition of *Permanence* as a source of randomness to be used in a crypto-system

E. Uniqueness

IPI as a randomness source has the *Uniqueness* condition if having one person's heartbeat would not help to predict the heartbeat of another person. In short, the random sources should be independent from each other. To measure the dependency of different subjects' IPI values from each other, we propose to use the dependency analysis of random sources presented by [50].

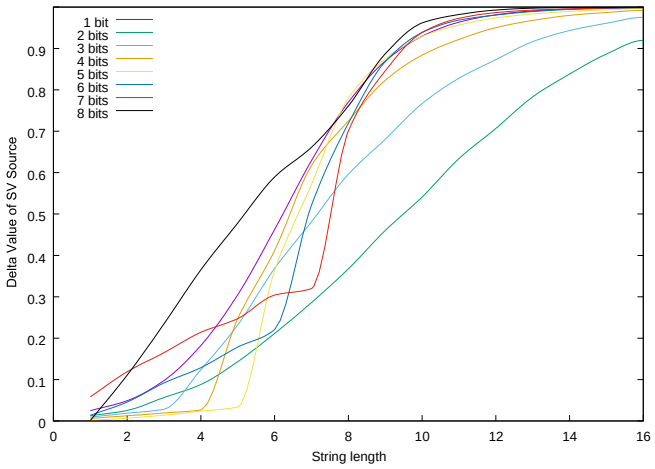


Fig. 8: δ value of SV-source for various string lengths of IPIs

As shown in Eq. 9, the summation of entropies of two randomness sources are bigger or equal to the entropy value of their combination as one source. In Eq. 9 two sources are independent from each other only and if only $lime_{indp} \rightarrow \infty$.

$$H(X,Y) \leq H(X) + Y(Y) \tag{8}$$

$$H(X) = -\sum_{t} p_x(t) \log p_x(t)$$

$$H(Y) = -\sum_{t} p_y(s) \log p_y(s)$$

$$H(X,Y) = \sum_{t,s} p_{x,y}(t,s) \log p_{x,y}(t,s)$$

$$e_{indp} = H(X) + H(Y) - H(X,Y) \tag{9}$$

To examine the independence of IPI values of different sources to each other, we selected 1360 subjects from the IPI dataset. These subjects have more than 100,000 consecutive IPI values because the dependency analysis between random sources needs a large sample size. From this pool of 1360 subjects, for 10,000 times, we selected two random subjects and calculate the e_{indp}. The box plot of e_{indp} values is presented in Fig. 9. As shown, Datasets 1, 2 and 3 are showing the condition of *Uniqueness* completely. For Dataset 4, the average value of e_{indp} is almost zero, despite a few outliers. For other datasets, the dependency between two random sources is shown with high average values and outliers.

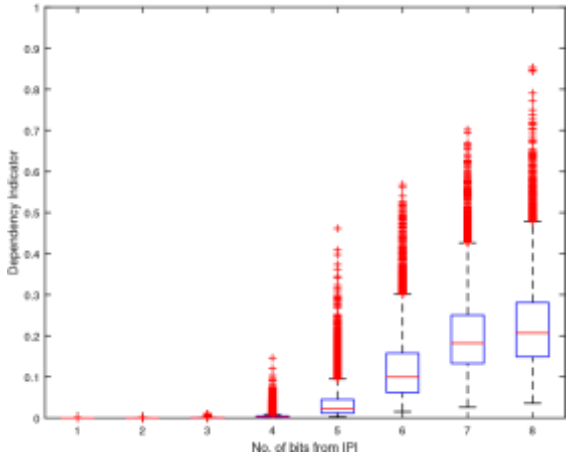


Fig. 9: Dependency analysis among IPIs from different subjects

In conclusion, despite the claim made in previous studies (e.g. [34], [35], [28], [24], [36], [37], [29]), the value of IPI is not a good source of randomness It provides *Robustness* to some level, but considering the worse case scenario (*Unconditional Secrecy*), it fails to provide *Robustness*. Moreover, IPI could not satisfy the *Permanence* condition as it is highly dependent on its history. Finally, IPI provides the *Uniqueness* as a random source which shows that every heart could be considered as an independent source compared to others. Among the 8 datasets used in this

experiment, Dataset 2 has better results, which shows that the two least significant bits of IPI are the better source of randomness compared to other combinations of bits. However, as discussed, even the two least significant bits of IPI do not provide a strong random number and thus not appropriate to be used in a crypto-system.

5. Martingale Randomness Extraction for IPI (MRE-IPI)

Rather than using the IPI values, which as we have shown above are not a good source of randomness, we propose to use the trend with which IPI is changing. Intuitively, whilst the value of IPI is affected by its previous values, the trend and rate of change are influenced by both physiological and contextual factors, activities, emotions and etc. A Martingale Stochastic Process [51] has been used in many applications of randomness such as extraction [52], developing computable randomness [53], algorithmic randomness theory [54] or even stock market analysis [55]. However, it has not been used to extract the randomness from IPI trend.

A Martingale is a sequence of random variables where the expectation of the next value is equal to the previous value. There are two main properties for a Martingale as follows:

TABLE I: Probabilistic distribution of all possible combination of bits for string length of 3

No.	String	Probability of occurrence
0	000	0.133567088
1	001	0.122682815
2	010	0.130448785
3	011	0.119522821
4	100	0.122658224
5	101	0.127181921
6	110	0.119505945
7	111	0.1244324

$$\forall n, \mathbb{E}(|X_n|) < \infty \qquad (10)$$

$$\forall n, \mathbb{E}(X_{n+1}) = X_n \qquad (11)$$

As shown in Eq 11, in a Martingale Stochastic Process the expectation of next value is equal to the previous value. So in order to use a Martingale on IPI, we must convert it to the a Martingale Stochastic Process. Then, we use this Martingale and extract the random variable from it. We called this algorithm as Martingale Randomness Extraction for IPI (MRE-IPI). To develop this stochastic process, extract the randomness and test it, we used Dataset 2 from previous section which contains the least two significant bits of IPI. From now on, for simplicity we refer to Dataset 2 as only *the dataset*. Moreover, to ensure that MRE-IPI is not biased on the IPI values in the dataset, the dataset is divided to two subsets randomly, one for randomness extraction analysis (training dataset) and another one for evaluating the proposed method (testing dataset). The training dataset consists of 2212 subjects with the total of 457,491,012 IPI values and the test dataset consists of 2126 subjects with the total of 438,130,554 IPI values.

The first step in MRE-IPI is to develop a conversion function $F : \{0,1\}^n \rightarrow \{0,1\}$ which can satisfy Eq. 11. In this situation, we prefer to use the minimum possible value for n, where n refers to the string length or the number of bits in the string. Using of large values for n, increases the number of IPI values needed to generate one random bit. For example, if n = 20, using 2 bits of an IPI, we need 10 IPI values to generate one bit in the Martingale Stochastic Process. Based on our analysis the optimum value for n is equal to 3. To do this, we calculated the probability distribution for all possible combinations of 3 bits for the training dataset as presented in Table I.

The best combination of strings that could provide the commutative probability of occurrence of 0.5 is:

- Group 1: $G_1 = \{000,011,101,110\}$, where $P(X = G_1) = 0.499777776$
- Group 2: $G_2 = \{001,010,100,111\}$, where $P(X = G_2) = 0.500222224$

Consider $X_n = x$ as a random variable and X_{n+1} as the next random variable in a time series, then $X \leftarrow F(s)$ is defined as:

$$X_{n+1} = \begin{cases} X_n + 1 & s \in G_1 \\ X_n - 1 & s \in G_2 \end{cases} \qquad (12)$$

where $s \in S = \{0,1\}^3$, and S is the random variable of IPI from training Dataset 2. Then $E\,E(X_{n+1}) = G_1 * (x + 1) + G_2 * (x - 1)$. As $G_1, G_2 \approx 0.5$, then $E(X_{n+1}) = x$, which is the value for S_n. Thus, $E(X_{n+1}) = X_n$ and Eq. 12 is a Martingale Stochastic Process (Eq. 11).

The second phase is to use $X \leftarrow F(s)$ with two threshold values to produce the random bit. Consider $t_1 > 0$ and $t_2 < 0$ as two threshold points, then we have:

$$\forall n, X_n \leftarrow \mathscr{F}(s) \qquad (13)$$

$$X_n > t_1 \rightarrow X_n = 0, \mathscr{R}(s) = 1 \qquad (14)$$

$$X_n < t_2 \rightarrow X_n = 0, \mathscr{R}(s) = 0 \qquad (15)$$

where $R(s)$ is the output of random variable R from the proposed method MRE-IPI. Wider threshold levels will increase the number of bits we need from IPI to generate one MRE-IPI random bit. However, narrower threshold values may not provide a good randomness quality. Based on our experiments, the best values for the threshold levels are $t_1 = 3$ and $t_2 = -3$. The process starts with a $s = 0$, and continues through all the available bits from the first step one by one. Let b_i be the bit we read
at time i:

$$s_i = \begin{cases} s_{i-1} + 1 & \text{if } b = 1 \\ s_{i-1} - 1 & \text{if } b = 0 \end{cases} \qquad (16)$$

The next step is to monitor s_i to see when it crosses the threshold values as follows:

$$\mathscr{R}(s) = \begin{cases} 1 & \text{if } s > 3 \\ 0 & \text{if } s < -3 \end{cases} \qquad (17)$$

where $R(s)$ is the extraction function. Every time $R(s)$ generates one bit, we reset s to zero ($s = 0$).

6. Analysis and Results

To examine the randomness of the MRE-IPI algorithm we used two approaches. In a first step, we conducted an entropy analysis on the result of MRE-IPI to examine its *Robustness* and *Permanence*. We did not test the condition of *Uniqueness*, since in the previous section, we showed that Dataset 2 satisfies this condition. The second step of the analysis is to use random number test suites to check the quality of the random numbers obtained. To this end, we have used well known benchmarks such as the NIST STS and Dieharder randomness test suites.

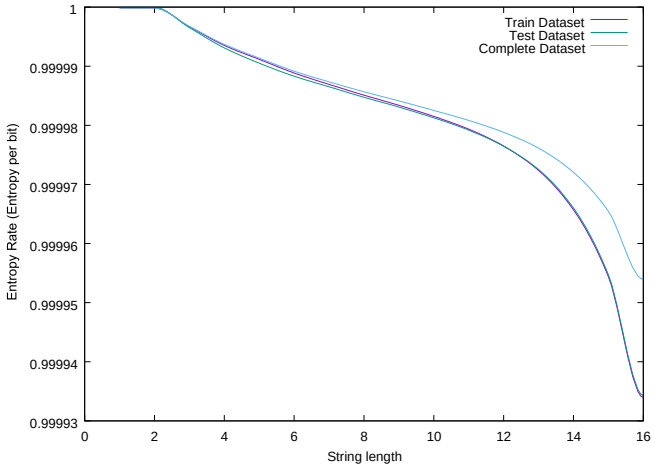


Fig. 10: Shannon Entropy of MRE-IPI datasets in various string lengths

A. Robustness

As mentioned before, we have used all the information secrecy measures to examine the *Robustness* of MREIPI. There are three sets to compare: the training dataset used for the conversion to a stochastic process, the test dataset which we did not use in the development of MRE-IPI and both of them together as one dataset. As shown in Fig. 10 the Shannon Entropy of MREIPI for up to string length of 16 is as high as 0.9999. Although, by increasing the size of the string to 16, the entropy rate drops from 1 to 0.99993, the difference is negligible. On the whole, MRE-IPI shows very high Shannon Entropy, and thus provides high quality randomness in *Perfect Secrecy* assumption.

Fig. 11 shows the Collision Entropy of MRE-IPI. The entropy rate even up to string lengths of 16 for training, testing and complete datasets is higher than 0.99986. Fig. 12 presents the Guessing Entropy analysis of MREIPI. As shown, for string lengths higher than 6, the Guess Entropy (subtracted from 0.5) is less than 0.01 and for string lengths of 16 for all datasets is less than $1e^{-03}$. Thus, MRE-IPI is able to provide *Robustness* in the *Conditional Secrecy* scenario. For Min-Entropy (fig. 13), the values for the training, test and complete datasets are almost equal. All the datasets, with the string length up to 16, have a MinEntropy rate higher than 0.930. This shows a great increase in Min-Entropy of IPI after using the MRE-IPI algorithm. Min-Entropy is a measure for *Unconditional Secrecy* and MRE-IPI shows *Robust* randomness in the worse case scenario (*Unconditional Secrecy*).

Fig. 14 shows the uniformity check of the distribution of MRE-IPI databases. This is the *Probabilistic Bound*; one of the information secrecy measures. For all datasets in MRE-IPI (training, test and complete), the values are less than 0.02 for all string lengths and thus, MRE-IPI shows an almost uniform distribution. In total, MRE-IPI shows that it has the *Robustness* condition of a strong randomness source.

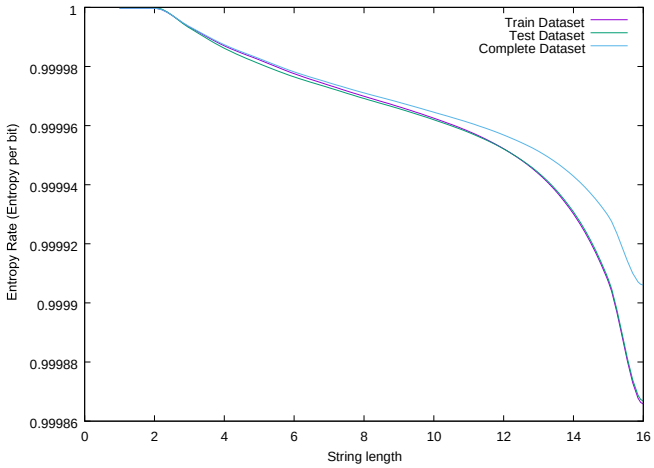


Fig. 11: Collision Entropy MRE-IPI datasets in various string lengths

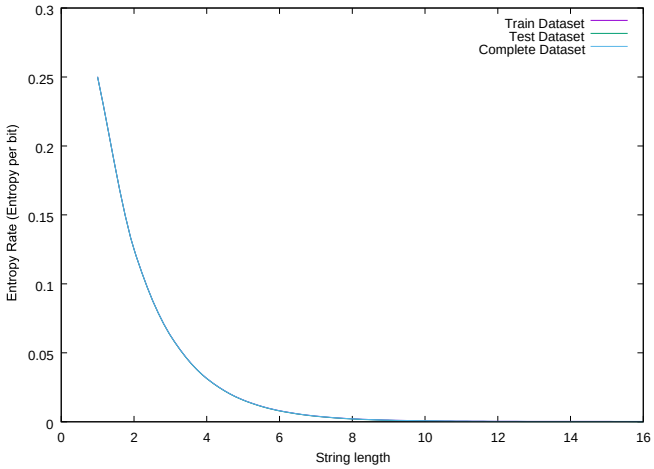


Fig. 12: Guessing Entropy of MRE-IPI datasets in various string lengths

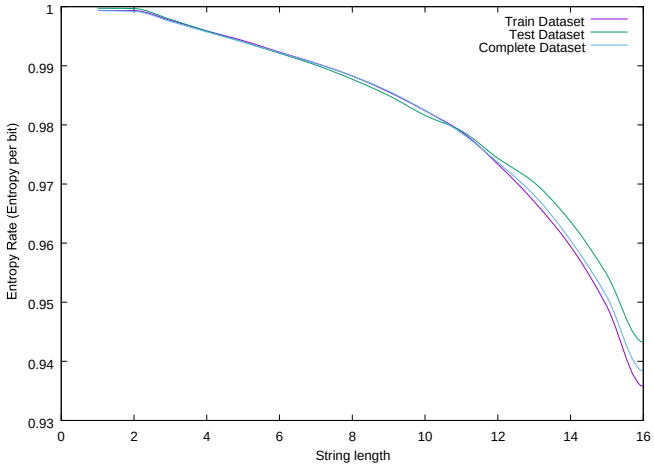


Fig. 13: Min-Entropy of MRE-IPI datasets in various string lengths

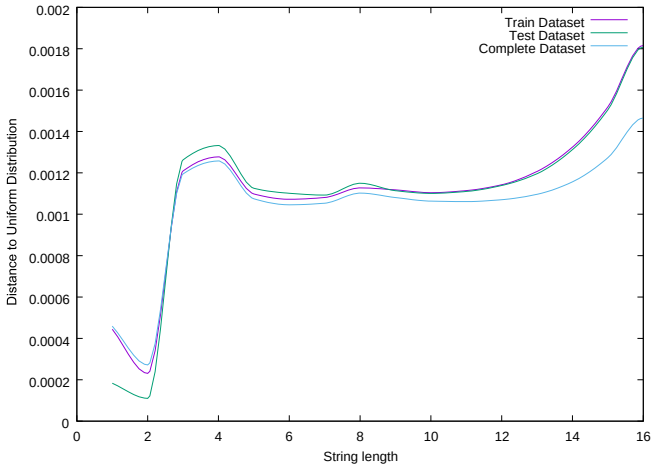


Fig. 14: Uniformity check for MRE-IPI datasets in various string length.

B. Permanence

The next step is to check the *Permanence* condition of MRE-IPI using the δ value of SV-source to see how much the MRE-IPI depends to its history. As shown in Fig. 15, MRE-IPI has a great reduction in dependency compared to the IPI value itself. Up to string lengths of 10, δ is less than 0.1, and δ increases for string length 16 to a max value of 0.4. This is a significant improvement compared to raw IPI values in which δ for string length 16 is almost 1. By having lower dependency to its history, MRE-IPI can provide *Permanence* condition to some extent. In this situation, MRE-IPI is not recommended to be used as a secret key, however, it could be used as a one-time-pad to exchange the session keys [56].

C. Test Suites Analysis

To evaluate a random extraction algorithm, a number of statistical tests have been proposed. A combination of randomness test algorithms is called a randomness suite or a battery of tests. The most used batteries of tests in randomness assessment are: NIST STS [38] and Dieharder [44]. A randomness suite usually needs a large set of random numbers for its tests. For instance, in NIST STS Linear test, the length of a sequence of bits must be greater than 10^6 and at least 100 sequences are needed to get a reliable result. This is more than 3,000,000 of 32-bit integer

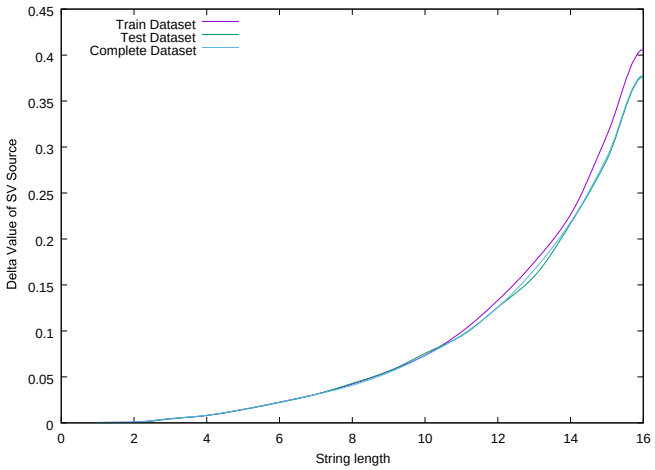
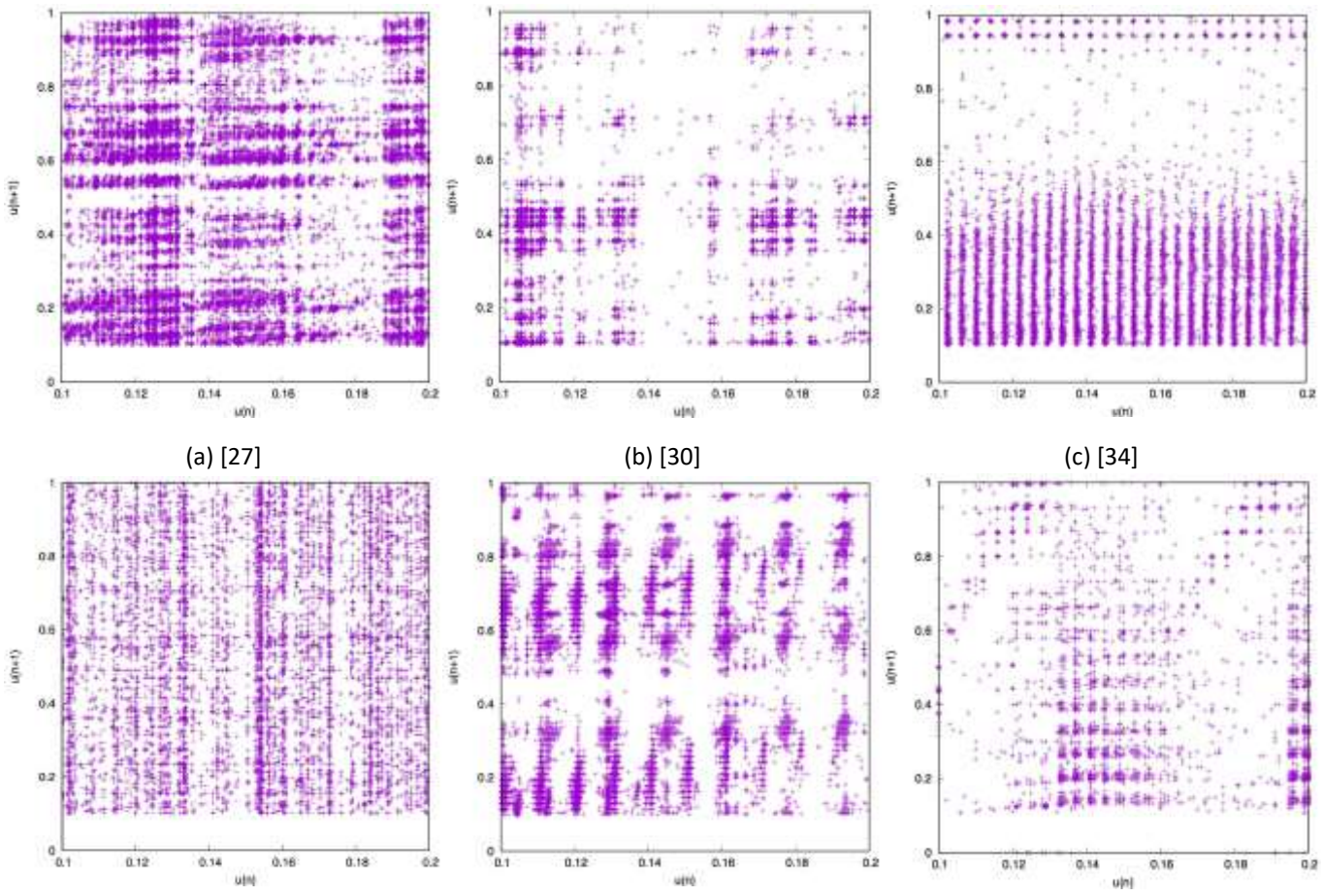


Fig. 15: δ value of SV-source for various string lengths of MRE-IPI

numbers. Using the collected IPI dataset, in this research, we evaluated MRE-IPI compared to the recent IPI randomness extraction algorithms by 2-dimensional scatter plot and two batteries of tests: NIST STS, and Dieharder.

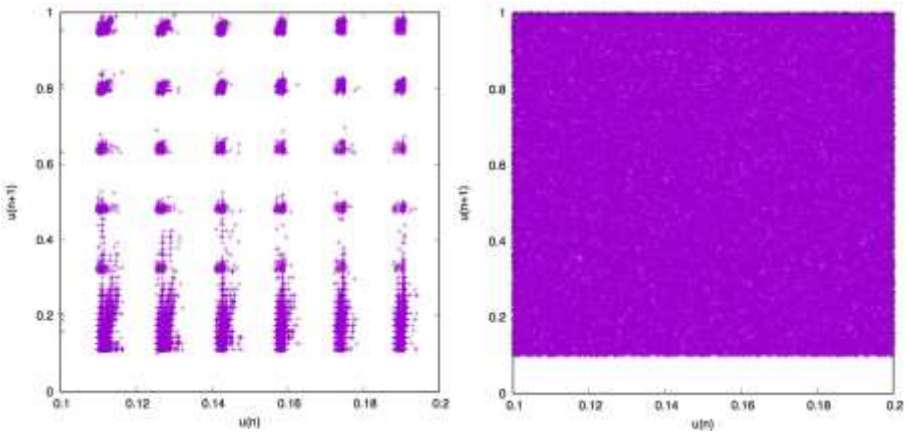
1) Two Dimensional Scatter Plot: The first step to examine the strength of randomness extractor algorithms is to produce a 2D scatter plot of *N* points obtained from them. The *N* points are generated in the t-dimensional unit hypercube $[0,1]^t$, either by taking vectors of *t* successive output values from the extractor algorithm, or by taking *t* non-successive values at pre-specified lags. The output of this 2D scatter plot should demonstrate a plane area without any specific pattern. To implement this, we have used the randomness statistical test suite TestU01 [43]. The output is presented in Fig. 16. As shown, all the current randomness extractor algorithms left a pattern in their figures. However, MRE-IPI produces an almost uniform distribution of numbers without any recognisable pattern.

2) NIST STS Test Suite: NIST STS is the first statistical suite for randomness tests several of them consisting in multiple sub-tests. In total, there are 190 tests and subtests for NIST STS. In order to test the IPI randomness extractor algorithms, two series of examinations have been conducted. In the first series, the binary dataset of random numbers is considered as the sequences with length 10,000 (10k) bits. In the second series of tests, 1,000,000 (1M) bits create a sequence to be tested in NIST STS.



(a) [27] (b) [30] (c) [34]

(d) [35] (e) [33] (f) [36]



(g) [23] (h) MRE-IPI

Fig. 16: Uniformity check from 2D scatter plot (TestU01) comparing our result (h) with algorithms proposed in selected works (a-g)

TABLE II: NIST STS Test Suite results for MRE-IPI and other IPI randomness extraction methods

Test Name	No. of tests	[27]		[30]		[57]		[35]		[33]		[36]		[23]		MRE-IPI	
		10k	1M	10k	1M	10k	1M	10k	1M	10k	1M	10k	1M	10k	1M	10k	1M
Frequency (Monobit)	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Block Frequency	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cumulative Sums	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Runs	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Longest Run	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Binary Matrix Rank	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Discrete Fourier Transform	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Non-overlapping Template Matching	150	5	0	65	0	0	0	19	0	68	0	105	0	109	0	143	131
Overlapping Template Matching	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Maurer's Universal	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Approximate Entropy	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Random Excursions	8	-	0	-	0	-	0	-	5	-	0	-	0	-	0	-	8
Random Excursions Variant	18	-	11	-	13	-	18	-	18	-	0	-	4	-	1	-	18
Serial	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2
Linear Complexity	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1
Total	190	5	12	65	13	0	19	19	23	68	0	105	4	109	1	152	164
Percentage	1.00	0.03	0.06	0.34	0.07	0.00	0.10	0.10	0.12	0.36	0.00	0.55	0.02	0.57	0.01	0.80	0.86

The reason for this is that, with NIST STS, the confidence in the results increases with longer sequences. Moreover, some tests cannot work with short bit sequences such as *Random Excursions Test* and *Random Excursions Variant Test*. However, if we increase the length of the sequences, the number of available sequences will be reduced which decreases the confidence in the results as well. Thus, in order to have a better picture of the quality of the results, we used both short (10k bits) and long (1M bits) sequences in our experiments.

We show in Table II the results of the NIST STS Test Suite on the studies reported in [27], [30], [57], [35], [33], [36], [23] compared with MRE-IPI. The algorithms proposed in [30] and [31] are very similar so we report them in a single column. [23], [37] and [22] also proposed very similar extraction algorithms and thus one column is used to present their results. As shown in the table, [36], [23] are the closest to MREIPI with 55% and 57% success rate in passing tests for sequence length 10k, while MRE-IPI has passed 80% of the NIST STS with the same sequence length. Moving to sequences with length 1M bits, the highest passing rate of 12% tests belongs to [35], while MRE-IPI has a pass rate of 86%. This clearly shows the robustness of the extraction method which with various length of sequences in testing, provides high quality results.

In addition to the success rate in passing the tests, checking the proportion of sequences passing a test is another measure to examine the quality of a randomness extractor. The confidence interval (*ci*) for the proportion of the binary sequences that passed the tests is calculated from Eq. 18, where $\hat{p}$ is 1 − α and *m* is the number of sequences.

$$ci = \hat{p} \pm 3\sqrt{\frac{\hat{3}(1-\hat{p})}{m}} \qquad (18)$$

The *alpha* value and the percentage of sequences that passed that confidence interval for MRE-IPI and other methods in literature are presented in Table III. Based on this table, with 95% confidence, more than 82% of sequences have passed the test for MRE-IPI, which is an improvement over the closest result, which belongs to [23] with 71.28% pass rate of sequences with 95% confidence. Figure 17 shows the scatter plot of p-values for NIST STS tests. Although these figures suggest only a slight improvement compared to other methods, we will show in the next section that our solution is a much stronger randomness generator in practice.

TABLE III: Percentage of sequences which passed the tests based on various α values

Extraction Methods	Seq size = 10,000		
	α =0.10	α =0.05	α =0.01
[27]	35.64	23.93	9.04
[30]	58.51	54.26	45.74
[34]	47.87	27.66	0.00
[35]	51.60	36.70	13.83
[33]	65.43	61.17	48.40
[36]	64.89	64.89	47.87
[23]	71.28	70.21	59.57
MRE-IPI	85.11	85.11	76.60
Extraction Methods	Seq size = 1,000,000		
	α =0.10	α =0.05	α =0.01
[27]	10.64	7.45	1.06
[30]	3.19	2.13	0.00
[34]	10.11	10.11	10.11
[35]	8.51	8.51	8.51
[33]	0.00	0.00	0.00
[36]	0.00	0.00	0.00
[23]	0.53	0.53	0.53
MRE-IPI	90.96	82.98	54.79

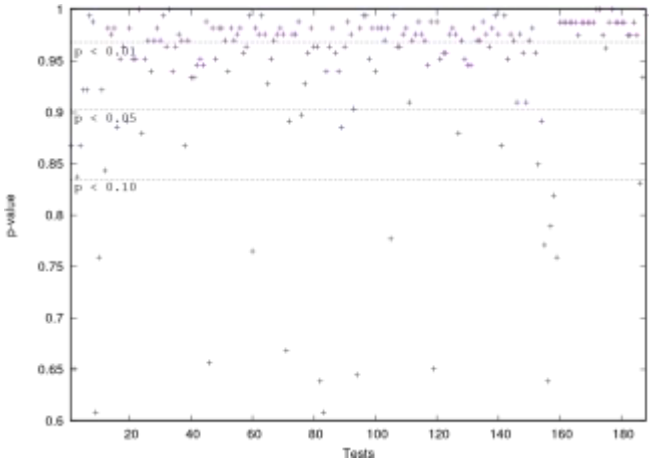


Fig. 17: Scatter plot of the p-values for NIST STS tests

D. Dieharder Test Suite

The final step to examine the quality of MRE-IPI is to use the Dieharder randomness test suite. Dieharder consists of 31 tests where some include several sub-tests. In total there are 114 tests and sub-tests. The output of Dieharder provides three ranks for each test including: PASSED, WEAK and FAILED. We have implemented the recent randomness extraction algorithms from IPI ([27], [30], [34], [35], [36], [33], [23]), and find that all of them have been FAILED in all the tests in the Dieharder test suite. So, to evaluate the quality of MRE-IPI, we selected four standard random number generators. The first one is Microsoft Excel, the second one is Niederreiter, Borosh random number generator [58], the third one is Robert R. (Bob) Coveyou random number generator [59] and finally the last one is the AES random number generator (e.g. [60]). For the last three random number generators, we used the Dieharder randomness test suite for both generation and test. As shown in Table IV, MRE-IPI completely outperforms the Excel and [58] random number generators. The quality of MRE-IPI is slightly better than [59], however, it is still far below AES. The reason for this could be the problem of *Permanence* condition in MRE-IPI. Although it is much better than IPI itself, its ”independency” from its history is not 100%. Thus, MRE-IPI fails in tests such as OPSO, OQSO, DNA and DAB DCT (Table IV). This shows that although MRE-IPI has high quality in *Robustness* and *Uniqueness*, it may still not be suitable to be used as a general cryptographic key. Because of the imperfect *Permanence* condition, our suggestion is to use additional tools such as hashing to convert MREIPI to a cryptographic key. This could be based on the idea of converting a known distribution histogram to a uniform histogram by reducing the number of bits in the original IPI. This is maybe the case and we will evaluate this in future work. However, we showed that the MREIPI is sufficiently good to be used in a cryptosystem. Nevertheless, due to the limited resources in IMDs, MRE-IPI can be used as a one-time pad for exchanging session key. For example, the gateway (outside the body) and IMD negotiated on a time and start to measure the IPI. Then, using MRE-IPI they create a one-time pad with the length same as the main key of the session. The gateway, produces the session key and encrypts it with a simple operation like XOR using the one-time pad and sends it to the IMD. Finally, IMD using its own one-time pad decrypts the received message and stores the session key for encryption and decryption of the next messages. In this scheme the usage of MRE-IPI is reduced to very few messages.

7. Conclusion

TABLE IV: Dieharder Test Suite results for proposed method and some conventional random number generators

Test Name	Excel	[58]	[59]	AES	MRE-IPI
Birthdays	0	1	1	1	1
OPERM5	0	1	1	1	1
32x32 Binary Rank	0	0	0	1	1
6x8 Binary Rank	0	0	0	1	0
Bitstream	0	0	0	1	0
OPSO	0	0	0	1	0
OQSO	0	0	0	1	0
DNA	0	0	0	1	0
Count the 1s (stream)	0	0	0	1	0
Count the 1s (byte)	0	0	0	1	1
Parking Lot	0	1	1	1	1
Minimum Distance (2d Circle)	0	1	1	0	1
3d Sphere (Minimum Distance)	0	1	1	1	1
Squeeze	0	1	1	1	0
Sums	0	1	1	1	1
Runs	0	0	1	1	1
Craps	0	0	1	1	1
Marsaglia and Tsang GCD	0	0	0	1	1
STS Monobit	0	0	1	1	1
STS Runs	0	0	0	1	1
STS Serial (Generalized)	0	0	0	1	0
RGB Bit Distribution	0	0	0	1	0
RGB Generalized Minimum Distance	0	0	1	1	0
RGB Permutations	0	1	1	0	1
RGB Lagged Sum	0	0	0	1	0
RGB Kolmogorov-Smirnov	0	0	1	1	0
Byte Distribution	0	0	0	1	0
DAB DCT	0	0	0	1	0
DAB Fill Tree	0	1	0	1	0
DAB Fill Tree 2	0	0	0	1	0
DAB Monobit 2	0	0	0	1	0
Total	0	9	13	29	14
Percentage	0.00	0.29	0.42	0.94	0.45

Although previous work has advocated the use of the physiological values in securing Body Sensor Networks and access to IMDs, the methods proposed for randomness extraction led to weak security and were not thoroughly evaluated. In this paper, using a significant dataset comprising almost 900,000,000 IPI values, we measured the three conditions of a strong random source: *Uniqueness*, *Robustness* and *Permanence*. We have shown that IPI values satisfy the condition of *Uniqueness* when up to four least significant bits are being used as the source of randomness. IPI is a *Robust* random source in the *Perfect Secrecy* or
Secrecy scenarios. However, it is not able to provide the *Robustness* in the worst case *Unconditional Secrecy* scenario. Moreover, we have shown that IPI does not have the condition of *Permanence* as it is highly dependent on its history. Thus, we do not recommend extraction of random numbers from the raw IPI values. However, rather than using the value of IPI, we propose using its trend. By converting the IPI trend to a Martingale Stochastic Process, we developed a random number extraction method named MRE-IPI. Despite the shortcomings of raw IPI values, MRE-IPI provides *Robustness* in all information secrecy measures, even in *Unconditional Secrecy*. When it only uses the first two least significant bits of IPI, it also satisfies the condition of *Uniqueness*. MRE-IPI has much lower dependency to its history compared to IPI and thus has a better *Permanence* condition. However, it is still not completely independent from its history as the IPI itself is not a strong randomness source with high independence from its history.

Using randomness test suites such as NIST STS and Dieharder, we have shown that MRE-IPI has an almost perfect score in the NIST STS suite and can pass Dieharder with a quality about half that of the AES random number generator. Other proposed IPI randomness extraction algorithms failed to pass the tests. We conclude that, as MRE-IPI has the properties of *Robustness*, *Uniqueness* and to some level the property of *Permanence*, and as it is measurable in every person (*Universality*) everywhere and any time (*Liveness*), it can be considered as an almost strong random extractor. Although, due to its dependency on its history it was not able to pass several tests of the Die Harder suite, MRE-IPI was able to produce a quality about half as good as AES. Additionally, it has low computational requirements suitable for resource constrained IMDs. We there propose using MRE-IPI as a one-time pad in IMDs to receive the secure session key from the reader. This reduces the usage of MRE-IPI during a secure communication and thus the probability of breaking it.

We also advocate the evaluation steps used in this paper as a general evaluation method for Physiological Value Security. The dataset we have used is available at
[61].

8. Acknowledgement

This work was funded by the UK EPSRC under grant EP/N023242/1 as part of the PETRAS Research Hub Cyersecurity of the IoT.

REFERENCES

[1] P. Buchta, M. Tajstra, A. Kurek, M. Skrzypek, M. Swietlinska, E. Gadula-Gacek, M. Wasiak, L. Pyka, and M. Gkasior, "The impact of remote monitoring of implanted cardioverterdefibrillator (ICD) and cardiac resynchronisation therapy device (CRT-D) patients on healthcare costs in the Silesian population: three-year follow-up ," *Kardiologia Polska*, vol. 75, no. 6, pp. 573–580, Jun. 2017.

[2] J. Walk, J. Weber, C. Soell, R. Weigel, G. Fischer, and T. Ussmueller, "Remote Powered Medical Implants for Telemonitoring," *Proceedings of the IEEE*, vol. 102, no. 11, pp. 1811–1832.

[3] L. Guedon-Moreau, D. Lacroix, N. Sadoul, J. Clementy, C. Kouakam, J. S. Hermida, E. Aliot, S. Kacet, and on behalf of the ECOST trial Investigators, "Costs of remote monitoring vs. ambulatory follow-ups of implanted cardioverter defibrillators in the randomized ECOST study," *Europace*, vol. 16, no. 8, pp.
1181–1188, Jul. 2014.

[4] The UK's largest database for microchipped pets.

[5] J. Hamill. An inventor has fitted himself with a implant which replaces car keys and he says the future is HERE.

[6] X. Liu, A. Ogirala, L. Berger, and M. Mickle, "Design and implementation of a volume conduction based RFID system for smart implants," in *2011 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2011, pp. 2893–2896.

[7] L. Pycroft, S. G. Boccard, S. L. F. Owen, J. F. Stein, J. J. Fitzgerald, A. L. Green, and T. Z. Aziz, "Brainjacking: Implant Security Issues in Invasive Neuromodulation," *World Neurosurgery*, vol. 92, no. C, pp. 454–462, Aug. 2016.

[8] Finkle, Jim. (2016, Oct.) J&J warns diabetic patients: Insulin pump vulnerable to hacking. [Online]. Available: http://www.reuters.com/article/us-johnson-johnson-cyberinsulin-pumps-e-idUSKCN12411L

[9] A. Hern. (2017, Aug.) Hacking risk leads to recall of 500,000 pacemakers due to patient death fears.

[10] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *JOURNAL OF BIOMEDICAL INFORMATICS*, vol. 55, no. C, pp. 272–289, Jun. 2015.

[11] M. R. Kanjee and H. Liu, "Authentication and key relay in medical cyber-physical systems," *Security and Communication Networks*, vol. 9, no. 9, pp. 874–885, May 2014.

[12] W. P. Adams Jr. and D. Mckee, "Matching the Implant to the Breast," *Plastic and Reconstructive Surgery*, vol. 138, no. 5, pp. 987–994, Nov. 2016.

[13] A. Y.-J. Wu, H.-L. Huang, J.-T. Hsu, and W. Chee, "Biomechanical effects of the implant material and implant–abutment interface in immediately loaded small-diameter implants," *Clinical Oral Investigations*, vol. 18, no. 4, pp. 1335–1341, Sep. 2013.

[14] Z. Chen, M.-K. Law, P.-I. Mak, and R. P. Martins, "A SingleChip Solar Energy Harvesting IC Using Integrated Photodiodes for Biomedical Implant Applications," *Ieee Transactions on Biomedical Circuits and Systems*, vol. 11, no. 1, pp. 44–53.

[15] S. L. Cotton, R. D'Errico, and C. Oestges, "A review of radio channel models for body centric communications," *Radio Science*, vol. 49, no. 6, pp. 371–388, Jun. 2014.

[16] B. B. Rios. (2017, May) Understanding Pacemaker Systems
Cybersecurity.

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

[18] K. K. Venkatasubramanian and S. K. S. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *Acm Transactions on Sensor Networks*, vol. 6, no. 4, pp. 1–36, Jul. 2010.

[19] G. Bajwa and R. Dantu, "Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms," *Computers & Security*, vol. 62, pp. 95–113, Sep. 2016.

[20] A. Ali and F. A. Khan, "An Improved EKG-Based Key Agreement Scheme for Body Area Networks." *ISA*, vol. 76 CCIS, no. Chapter 29, pp. 298–308, 2010.

[21] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proceedings - IEEE Military Communications Conference MILCOM*, Arizona State University, Tempe, United States. IEEE, Dec. 2008, pp. 1–7.

[22] G. Zheng, G. Fang, M. A. Orgun, R. Shankaran, and
E. Dutkiewicz, "Securing wireless medical implants using an ECG-based secret data sharing scheme." *ISCIT*, 2014.

[23] S. Peter, B. P. Reddy, F. Momtaz, and T. Givargis, "Design of secure ECG-based biometric authentication in body area sensor networks," *Sensors (Switzerland)*, vol. 16, no. 4, p. 570, Apr. 2016.

[24] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in Wireless Body Area Network (WBAN)," in *International Conference on Advanced Communication Technology, ICACT*. Universiti Teknikal Malaysia Melaka, Ayer Keroh, Malaysia, Apr. 2013, pp. 998–1001.

[25] S. Wolf, "Unconditional Security in Cryptography," in *Information Security Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, Mar. 2003, pp. 217–250.

[26] W. Wang, K. Hua, M. Hempel, D. Peng, H. Sharif, and H.-H. Chen, "A Stochastic Biometric Authentication Scheme Using Uniformed GMM in Wireless Body Area Sensor Networks," in *st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, South Dakota State University, Brookings, United States. IEEE, 2010, pp. 1620–1624. [27] T. Hong, S.-D. Bao, Y.-T. Zhang, Y. Li, and P. Yang, "An improved scheme of IPI-based entity identifier generation for securing body sensor networks," in *2011 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2011, pp. 1519–1522.

[28] S. N. Ramli, R. Ahmad, and M. F. Abdollah, "Electrocardiogram (ECG) signals as biometrics in securing wireless body area network," in *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*, Universiti Teknikal Malaysia Melaka, Ayer Keroh, Malaysia. IEEE, Jan. 2013, pp. 536–541.

[29] K. Kalaivani, V. Anjalipriya, R. Sivakumar, and R. Srimeena, "An efficient Bio-key Management scheme for telemedicine applications," in *Proceedings - 2015 IEEE International Conference on Technological Innovations in ICT for Agriculture and Rural Development, TIAR 2015*, SRM Group Of Educational Institutions, Chennai, India. IEEE, Dec. 2015, pp. 122–126.

[30] S.-D. Bao, "A matching performance study on IPI-based entity identifiers for body sensor network security," in *2012 5th International Conference on Biomedical Engineering and Informatics, BMEI 2012*, Ningbo University of Technology, Ningbo, China. IEEE, Dec. 2012, pp. 808–811.

[31] F. Miao, S.-D. Bao, and Y. Li, "Physiological Signal Based Biometrics for Securing Body Sensor Network," in *New Trends and Developments in Biometrics*. InTech, Nov. 2012.

[32] S.-D. Bao, F. Miao, and Y. Li, "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security," *IET Information Security*, vol. 7, no. 2, pp. 87–96, Jun. 2013.

[33] D. K. Altop, A. Levi, and V. Tuzcu, "Towards using physiological signals as cryptographic keys in Body Area Networks," in *Proceedings of the 2015 9th International Conference on Pervasive Computing Technologies for Healthcare, PervasiveHealth 2015*, Sabancl University, Tuzla, Turkey. ICST, Dec. 2015, pp. 92–99.

[34] K. Cho and D. H. Lee, "Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Korea University, Seoul, South Korea. Berlin, Heidelberg: Springer Berlin Heidelberg, Mar. 2012, pp. 203–218.

[35] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen,
"OPFKA - Secure and Efficient Ordered-Physiological-Feature-
Based Key Agreement for Wireless Body Area Networks," in *Proceedings - IEEE INFOCOM*, George Washington University, Washington, United States. IEEE, 2013, pp. 2274–2282.

[36] N. Jammali and L. C. Fourati, "PFKA: A physiological feature based key agreement for wireless body area network," in *2015 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, 2015, pp. 1–8.

[37] G. Zheng, G. Fang, M. A. Orgun, and R. Shankaran, "A Comparison of Key Distribution Schemes Using Fuzzy Commitment and Fuzzy Vault Within Wireless Body Area Networks," in *IEEE th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications PIMRC*, Macquarie University, North Ryde, Australia. IEEE, 2015, pp. 2120–2125.

[38] A. Rukhin, J. Sota, J. Nechvatal, M. Smid, E. Barker, S. Leigh,
M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Computer Security Division., Gaithersburg, MD, Gaithersburg, MD, Tech. Rep., 2000.

[39] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. De Zeeuw, "Adaptive Entity-Identifier Generation for IMD Emergency Access," in *First Workshop on Cryptography and Security in Computing Systems*, Erasmus University Medical Center, Rotterdam, Netherlands. New York, New York, USA: ACM Press, 2014, pp. 41–44.

[40] S. A. Israel, J. M. Irvine, A. Cheng, M. D. Wiederhold, and B. K. Wiederhold, "ECG to identify individuals," *Pattern Recognition*, vol. 38, no. 1, pp. 133–142, Jan. 2005.

[41] B. Espinoza and G. Smith, "Min-entropy as a resource," *Information and Computation*, vol. 226, pp. 57–75, May 2013.

[42] A. L. Goldberger, L. A. N. Amaral, L. Glass, J. M. Hausdorff, P. C. Ivanov, R. G. Mark, J. E. Mietus, G. B. Moody, C. K.
Peng, and H. E. Stanley, "PhysioBank, PhysioToolkit, and
PhysioNet : Components of a New Research Resource for Complex Physiologic Signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, Jun. 2000.

[43] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," *ACM Transactions on Mathematical Software (TOMS)*, vol. 33, no. 4, pp. 22–es, Aug. 2007.

[44] R. G. Brown, D. Eddelbuettel, and D. Bauer, *Dieharder: A random number test suite*. Open Source software library, 2013.

[45] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 2013.

[46] Y. Yao and Z. Li, "Security of weak secrets based cryptographic primitives via the Renyi entropy," *IET Information Security*, vol. 10, no. 6, pp. 442–450, Nov. 2016.

[47] C. Cachin, "Entropy measures and unconditional security in cryptography." Ph.D. dissertation, SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH, 1997.

[48] J. L. Massey, "Guessing and entropy," in *1994 IEEE International Symposium on Information Theory*. IEEE, p. 204.

[49] M. Santha and U. V. Vazirani, "Generating quasi-random sequences from semi-random sources," *Journal of Computer and System Sciences*, vol. 33, no. 1, pp. 75–87, Jan. 1986.

[50] A. G. Konheim, *Cryptography, a Primer*, 1st ed. New York, NY, USA: John Wiley and Sons, Inc., 1981.

[51] R. Downey, E. Griffiths, and G. Laforte, "On Schnorr and computable randomness, martingales, and machines," *MLQ*, vol. 50, no. 6, pp. 613–627, Oct. 2004.

[52] S. Beigi, O. Etesami, and A. Gohari, "Deterministic Randomness Extraction from Generalized and Distributed SanthaVazirani Sources," *Electronic Colloquium on Computational Complexity*, vol. 179, pp. 1–32, Dec. 2014.

[53] J. Rute, "Computable randomness and betting for computable probability spaces," *Mathematical Logic Quarterly*, vol. 62, no. 4-5, pp. 335–366, Sep. 2016.

[54] B. Kjos-Hanssen, P. K. L. Nguyen, and J. Rute, “Algorithmic randomness for Doob’s martingale convergence theorem in continuous time,” *Logical Methods in Computer Science*, vol. 10, no. 4, pp. 1–35, 2014.

[55] A. John Ayodele, “Empirical Test of the Martingale Property in Stock Market: Evidence from Nigeria,” *Journal of Finance and Accounting*, vol. 5, no. 4, p. 147, 2017.

[56] K. K. Venkatasubramanian and S. K. S. Gupta, “Physiological value-based efficient usable security solutions for body sensor networks,” *Acm Transactions on Sensor Networks*, vol. 6, no. 4, pp. 1–36, Jul. 2010.

[57] S. Choto and N. Premasathian, “A Dynamic Fuzzy Commitment Scheme Using Multiple Commitments,” in *International Symposium on Communications and Information Technologies*
ISCIT, King Mongkut’s Institute of Technology Ladkrabang, Ladkrabang Bangkok, Thailand. IEEE, 2012, pp. 308–312.

[58] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*. Society for Industrial and Applied Mathematics, May 2012.

[59] R. R. Coveyou, “Random number generation is too important to be left to chance,” *Applied Probability and Monte Carlo Methods and modern aspects of dynamics. Studies in applied mathematics*, vol. 3, pp. 70–111, 1969.

[60] J. E. Gentle, W. K. Hardle, and Y. Mori, Eds.,¨ *Handbook of Computational Statistics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[61] H. Chizari and E. Lupu, “Ipi values of heart beats,” Mar. 2018. [Online]. Available: https://doi.org/10.5281/zenodo.1188936