Journal of King Saud University – Computer and Information Sciences xxx (xxxx) xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Using ECG signal as an entropy source for efficient generation of long random bit sequences

Md Saiful Islam

Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

ARTICLE INFO

Article history:
Received 3 July 2021
Revised 15 December 2021
Accepted 2 January 2022
Available online xxxx

Keywords:
True Random Number
Cryptography
Biometrics
Entropy source
ECG signal

ABSTRACT

Electrocardiogram (ECG) signal produced by the human heart has been investigated as a potential entropy source for cryptographic random bit generation for a long time. The throughput of existing methods remains as the bottleneck for its deployment in practical applications. To overcome this problem, we develop a Bernoulli entropy source by processing a single heartbeat ECG signal to obtain a long random bit sequence (RBS). The proposed method converts the signal into an IID (independent and identically distributed) source of entropy using efficient interpolation and optimization techniques. Several heartbeat signals, obtained from two different databases, were used to test the entropy source generating RBSs with one million bits. The entropy source was evaluated with the latest NIST recommendation for IID source validation and it passed all recommended tests and the average min-entropy obtained from several heartbeat signals of different individuals was close to the perfect entropy value of 1.0. It was also observed that the entropy increases monotonically with the increase of the length of keys. The proposed method can efficiently produce a long RBS for cryptographic applications, such as key generation for one-time pad and image encryption. The method could be further explored to generate a true random number with a personalized signature, which is crucial for information security in the future generation of computing.

1. Introduction

In the forthcoming era of computing, the use of true random numbers with a personalized signature is envisaged to be more crucial in cryptographic applications, such as one-time pad (OTP) (Argyris et al., 2016; Manucom et al., 2019), image encryption (Nguyen et al., 2020; Sivaraman et al., 2020), wireless body area network security (Camara et al., 2019; Karthikeyan and Manickam, 2019; Pirbhulal et al., 2018; Zheng et al., 2017), and protection of implantable medical devices (Chizari and Lupu, 2019; Zheng et al., 2015). A true random number generator harvests the numbers from an entropy source which is based on physical processes with inherent randomness. In fact, a correct entropy source is considered as the cornerstone of a true random number generator. Frequently used entropy sources include noise (e.g., electrical, thermal, environment noise), jitter (e.g., clock, phase), chaos, quantum effect (e.g., multiphoton emission, beam splitter port axis misalignment, non-perfect circular polarization), and bioelectrical signals (e.g., electrocardiogram, electroencephalogram, and electromyography) (Kaya, 2020a; Kaya, 2020b; Kaya et al., 2021; Stipčević and Koç, 2014; Wu et al., 2021; Yu et al., 2019).

A new trend of true random number generation from bioelectrical signals is emerging primarily in wireless body area networks (Arslan Tuncer and Kaya, 2018; Camara et al., 2019; Camara et al., 2018; Chen et al., 2012b; Pirbhulal et al., 2018; Zheng et al., 2017). Among the bioelectrical signals used as the entropy source, the electrocardiogram (ECG) signal is gaining attention because of its potential use in generating random numbers with personalized signatures for biometric authentication (González-Manzano et al., 2017; Karimian et al., 2019; Lyp et al., 2021) and cryptography (Chen et al., 2012a; Hamad et al., 2017; Islam, 2015).

Abbreviations: OTP, One-Time Pad; IID, Independent and Identically Distributed; RBS, Random Bit Sequence; ECG, Electrocardiogram; IPI, Inter-Pulse-Interval; HRV, Heart Rate Variability; TRNG, True Random Number Generation; DRNG, Deterministic Random Number Generation; PVS, Physiological Value-based Security.

E-mail address: saislam@ksu.edu.sa

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2022.01.001
1319-1578/

Please cite this article as: Md Saiful Islam, Using ECG signal as an entropy source for efficient generation of long random bit sequences, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2022.01.001

1.1. Related works

The ECG signal has already emerged as a biometric modality (AlDuwaile and Islam, 2021; Islam and Alajlan, 2016; Islam et al., 2012; Wu et al., 2021b) for its uniqueness, stability, universality, robustness, collectability, acceptability, and liveness properties, which are also desirable characteristics for a noise source for biometric cryptography (Chizari and Lupu, 2019; Ramli et al., 2013). Biometric cryptography has already been investigated for physiological value-based security (PVS) solutions (Venkatasubramanian and Gupta, 2010) that do not require a key exchange protocol. It could be viable because it is not as resource hungry as public-key cryptography and it proposes higher security than symmetric encryption (Chizari and Lupu, 2019). Hence, a random key generated from an ECG signal could introduce a new dimension in cryptography that is useful for many applications.

Most of the existing studies focused on the use of inter-pulse-interval (IPI) values of ECG signal for random bit sequence (RBS) generation. Although Ortiz-Martin et al. (2018) reported that IPI values of heartbeats do not make a good source of randomness, later in 2020 they found that a certain bit combination of eight-bit IPI values were feasible for RBS generation (Ortiz-Martin et al., 2020). They analyzed the randomness using the non-IID (independent and identically distributed) track of the NIST 800-90B recommendation (Turan et al., 2018) and found that RBS generated from several combinations of five bits could pass some of the tests. Different encoding and quantization of IPI values to obtain a string of 4 to 16 bits were also used in (Chen et al., 2012b; Chizari and Lupu, 2019; Pirbhulal et al., 2018). On the contrary, some researchers used other features extracted from a heartbeat signal to obtain a higher number of bits. For example, Zheng et al. (2017) used a binary representation of five-feature values to obtain a string of 128 bits and Camara et al. (2018) used quantization of wavelet coefficients to obtain 184 bits from single heartbeats. In all these studies, the required length of a RBS could be achieved by appending bit strings from consecutive heartbeats as required by a cryptographic protocol.

Although existing processes may be suitable for applications where the length of the RBS is relatively small, they are not feasible when the required sequence is much longer. This is because the time required to capture the ECG signal could be quite long, as shown in Table 1. For example, for encryption of a 128×128 Gy-scale image, existing IPI-based methods could take as long as 4.55 h to generate a key. Hence, the throughput of the RBS generation process may not be sufficient for many applications wherein a long RBS is required in a short period of time. Moreover, a bit sequence generated from IPI and other features may not be identically distributed and the produced key could have lower entropy. To the best of our knowledge, all existing methods generating RBS from ECG signals have been evaluated using the non-IID track.

1.2. Contributions

In this paper, we propose a method to use a single heartbeat ECG signal as a noise source and convert it into an entropy source to produce a long RBS with high throughput, such that the generated bit sequence follows a uniform distribution to maximize the entropy. We produce the whole sequence from the noise source, in contrary to the suggestion by Killmann and Schindler (2001), to use a true random number generation (TRNG) to generate a seed and then the deterministic random number generation (DRNG) to obtain an RBS. The main advantage of our method is that it is possible to check the biometric signature of the random sequence possessed by the heartbeat signal (AlDuwaile and Islam, 2020; Islam and Alajlan, 2015). We tested the entropy source to generate one million bits using several heartbeats from two different databases and evaluated it with the IID-track assumption of the latest NIST recommendation (Turan et al., 2018) and it passed all tests. The main contributions of this work are as follows:

i. Developing a Bernoulli entropy source: We have developed the entropy source as a Bernoulli process consisting of a set of independent binary random variables. We have processed the ECG signal obtained from a small segment of heartbeat signal using the interpolation technique. The bit string obtained from the interpolated samples are map with the entropy source to produce a RBS.
ii. Developing an IID source of entropy: We have developed an IID source of entropy by using an optimization technique to enhance the uniformity of distribution of the generated RBS. This is significant because uniform distribution increases the entropy of the source to enhance the security. To the best of our knowledge, no existing work on RBS generation using an ECG signal satisfies all tests for IID assumptions.
iii. An entropy source with high throughput: We use efficient cubic spline interpolation to transform a small segment of ECG signal into an entropy source to obtain a long RBS. The throughput depends primarily upon the time required for capturing the segment of the ECG signal and it could take less than one second for a complete heartbeat. Compared to existing methods this is a significant improvement because the throughput of existing methods is not suitable for many applications, like OTP and image encryption.

1.3. Outline

The remainder of this paper is organized as follows. In Section 2, the proposed method is presented. In Section 3, the datasets and experimental results are described. The discussion about the obtained results is presented in Section 4. Section 5 concludes the paper with possible future works.

Table 1
Time requirement for a key generation using existing IPI and feature-based methods.

Application	Required Key Length (minimum)	IPI (Chizari and Lupu, 2019)		Feature-based (Zheng et al., 2017)	
		Number of HBs Required[+]	Required Time[*]	Number of HB Required [++]	Required Time[*]
WBAN, IMD	128 bits	16 + 1	17 sec	1	1 sec
OTP (For a text with 1000 ASCII char)	8000 bits	1000 + 1	1001 sec (16.68 min)	63	63 sec
Image Encryption (128×128, gray scale)	131,072 bits	16,384 + 1	16,385 sec (**4.55 h**)	1024	1024 sec **(17.1 min)**

[*] Assuming 1 s for each heartbeat i.e. 60 heartbeats/minute.
[+] Assuming 8 bit/IPI is generated.
[++] Assuming 128 bit/ heartbeat.

2. Method

In this section, we describe we describe the development process of an entropy source by using a small segment of ECG signal as a noise source. At first, we discuss the randomness of ECG signals and their suitability as a noise source (Subsection 2.1). The entropy source is described as a Bernoulli random process and it is obtained by digitalization and resampling of the noise source and nonlinear mapping of quantized samples with discrete random variables. We did not use any optional conditioning component (Turan et al., 2018). In Subsection 2.5, we discuss the throughput and computational complexity of the proposed method.

2.1. ECG signal as a noise source

An ECG signal, which is a reflection of electrical activities of the heart, can be measured noninvasively on the surface of the body. The electrical signal produced by the heart is semi-periodic, and the duration required for a complete heartbeat is also random. This heart rate variability (HRV) is a natural process, and it is associated with different conditions such as respiration, blood pressure, physical activity, and mental stress (Sörnmo and Laguna, 2005). The dynamic nature of the heart makes it a potential noise source for true RBS generation. While there are large inter-individual differences among signals produced by hearts of different people, HRV introduces intra-individual variability of temporal and morphological properties of heartbeats as well (Islam and Alajlan, 2013b). Fig. 1 shows two heartbeats from the same individual showing the intra-individual differences in morphological (e.g. amplitudes of R-peaks) and temporal features (e.g. P-P durations). During a normal sinus rhythm, the signal of a complete heartbeat contains three main components: P-wave, QRS-complex, and T-wave. In general, a heartbeat starts with a P-wave corresponding to atrial contraction followed by a QRS-complex representing the contraction of the ventricles, and finally, it ends with a T-wave representing relaxation of the ventricles. It could be noted that the duration of a heartbeat for a healthy person varies from 0.6 to 1 s and the amplitude of the QRS-complex is much larger than those of the P-wave and the T-wave. We consider the use of a small segment of ECG signal which include the signal for one heartbeat (e.g., P-P segment) as a noise source. We process a ECG segment as a noise source and convert it into an entropy source that produces a RBS with the desired length required by an application.

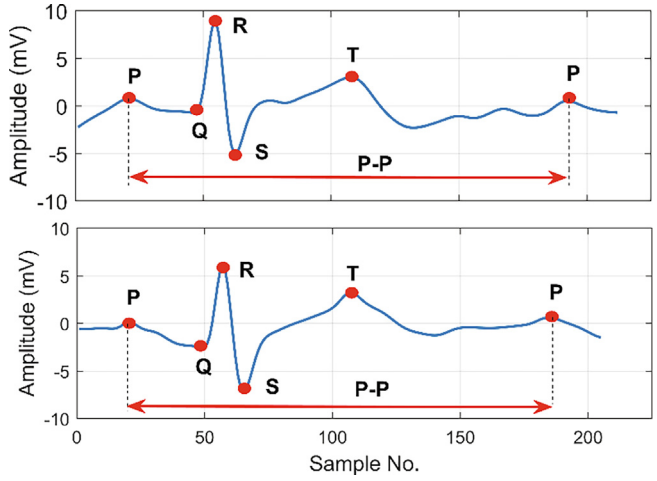

Fig. 1. Two segmented heartbeat signals from the same person showing all morphological elements and intra-individual variability.

2.2. Development of a Bernoulli process

We define the entropy source as a Bernoulli process with a set of n independent and identically distributed binary random variables $\{X_1, X_2, \ldots X_n\}$ producing a sequence of RBS with length n. The probability that the process generates a sequence X with j 1′s and $(n\text{-}j)$ 0′s can be described by the binomial distribution

$$P(X|j) = \binom{n}{j} P(X_i = 1)^j P(X_i = 0)^{n-j} \quad (1)$$

Uniform distribution of each of these random variables, i.e. $P(X_i = 1) = P(X_i = 0)$; $i = 1 \ldots n$, maximizes the entropy of the generated RBS. Hence, to obtain an IID entropy source producing a long RBS with maximum entropy, the following conditions are required to be fulfilled:

i) An arbitrarily large number of bits can be obtained from the noise source.
ii) When n is large, the expected numbers of 1′s and 0′s are equal i.e. $nP(X_i = 1) = nP(X_i = 0)$.
iii) Probability distributions of all random variables are independent i.e. $P(X_1, X_2, \ldots X_n) = P(X_1)\, P(X_2) \ldots P(X_n)$.

Since heartbeat signal $f(t)$; $0 \le t \le T$, where T is the duration of a heartbeat; is a continuous signal, it is always possible to obtain an arbitrarily large number of samples by applying sampling and interpolation techniques, and the desired length of the bit sequence is obtained by quantization of the samples. In order to obtain n bits from a continuous signal, we define a function $E : f \rightarrow \{X_1, X_2, \cdots, X_n\}$, which maps the noise source f onto the n binary random processes. Fig. 2 shows the steps of the proposed method to map the noise source onto an entropy source that produces the RBS with length n. The five steps of the development process as discussed below.

Step 1: Digitalization

For digital signal processing, a continuous ECG signal is generally sampled at a constant sampling rate s, which is not less than the Nyquist rate determined by the useful bandwidth of the signal. The digital representation of continuous signal $f(t)$, $0 \le t \le T$ for an ECG segment with duration T, produces r samples, where $r = T \times s$. The amplitude of each sample $a_i \in \mathrm{R}$, $i = 1 \ldots r$, is real and finite.

Step 2: Removal of R-Peak

The values of most of these r samples are suppressed by the large amplitude of the R-peak, which is the peak of the narrow but steep QRS complex. Hence, removing the top part of the narrow QRS-complex (i.e., the R-wave) could increase the uniformity of the distribution of the samples obtained from the remaining parts of the signal producing more uniformly distributed samples. Hence, we use a simple optimization technique to obtain the most uniform distribution possible (discussed in Subsection 2.3).

Step 3: Interpolation

Cubic spline interpolation technique is used in association with the optimization step to obtain the distribution of the interpolated samples as uniform as possible over the range of $0\text{–}2^m$ levels, where m is the number of quantized bits. In fact, the optimization process divides the signal f into two segments and each of them is interpolated separately, yielding a set of p interpolated samples in total as discussed in Subsection 2.3 in detail.

Step 4: Quantization

To obtain a sequence of n random binary values from the ECG segment represented by p interpolated samples, we use a quantization technique producing m-bits of each of them. The value of p and m depend on the number of bits (n) required for the application such that $n = p \times m$. At first, the amplitude of each sample $a_i \in \mathrm{R}$, $i = 1 \ldots p$, which is finite and real, is normalized to the range

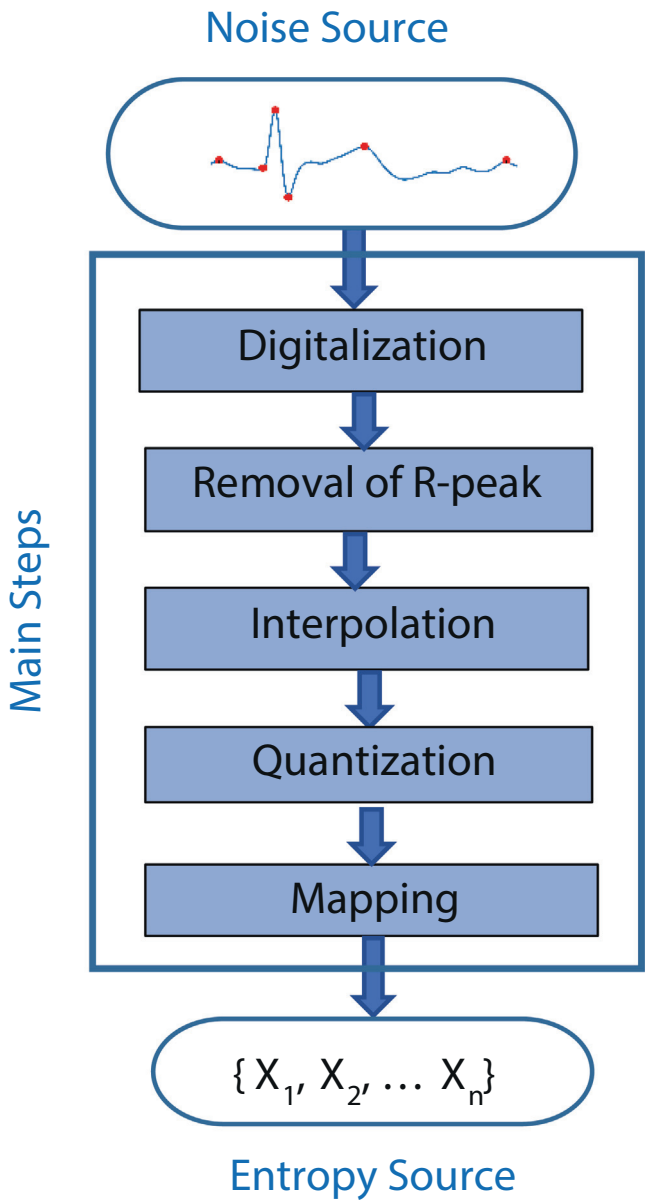

Fig. 2. Block diagram of the proposed entropy source development process from a segment of ECG signal.

[0–1] to obtain a normalized sample $\overline{a}_i$. Then for a m-bit quantization, each normalized sample is multiplied by 2^m as follows

$$\widehat{a}_i = \overline{a}_i \times 2^m \tag{2}$$

Step 5: Mapping

The binary representation of each quantized sample ($\widehat{a}_i$) yields a m-bit binary string. Hence, the concatenation of these strings produces a sequence of n random bits $\{b_1, b_2, \ldots, b_n\}$ where $b_i \in \{0, 1\}$. The Bernoulli process is obtained by mapping the n random values $\{b_1, b_2, \ldots, b_n\}$ to the n random variables $\{X_1, X_2, \ldots X_n\}$, by using a non-linear mapping process (discussed in Subsection 2.4) as follows:

$$M : b_i \rightarrow X_j; 1 \leq i, j \leq n \tag{3}$$

2.3. Interpolation and uniformity optimization

It is well known that a digital signal obtained by sampling at a rate higher than the Nyquist rate could be reconstructed by interpolation techniques. Cubic spline interpolation is a widely used method that requires only four parameters to define a continuous cubic polynomial function between a pair of samples (Revesz, 2014). We can interpolate an arbitrary number of samples in between them using the polynomial functions. In this way, we can obtain q samples equally divided among $r - 1$ intervals defined by r samples each of which could be quantized by Eq. (2) to obtain a n-bit RBS. However, the values of most of the q samples obtained by this process are suppressed by the large amplitude of the R-peak, which is the peak of the narrow but steep QRS complex. Hence, the distribution of the obtained samples, quantized into 2^m discrete levels, is mostly concentrated in a small region with a small standard deviation and the mean shifted towards zero rather than the middle of the range $0–2^m$, as shown in the left column of Fig. 3. The binary representation of these quantized samples produces more zeros than ones yielding non-uniform distribution for the binary random processes. Hence, removing the top part of the narrow QRS-complex (i.e., the R-wave) could increase the uniformity of the distribution of the samples obtained from the remaining parts of

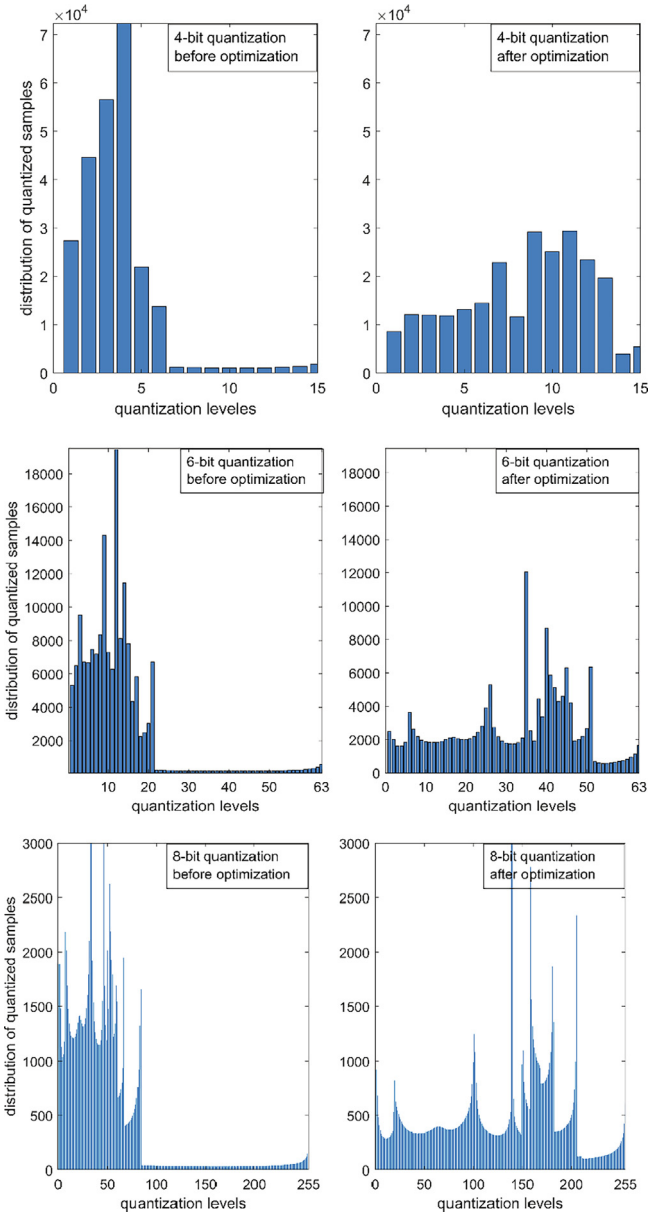

Fig. 3. Effect of the optimization process on the distribution of samples using 4-, 6-, and 8-bit quantization.

the signal producing more uniformly distributed samples. Hence, we use a simple optimization technique such that we can obtain the most uniform distribution possible of the obtained samples by removing only a small part of the R-wave.

To remove the top part of the R-wave, we first detect the R-peak using an efficient method described in (Islam and Alajlan, 2013a). Then, the S-peak is also detected by using the augmented-Hilbert transform described in (Islam and Alajlan, 2014). We use an iterative optimization process to select an optimal window w^* centered at the R-peak so that after removal of this part and then interpolation of the remaining parts of the signal produces q samples such that their distribution, over the range of quantization levels $0–2^m$, becomes as uniform as possible. To optimize the uniformity of the distribution of quantized samples $\hat{a}_i$, we minimize the variance (var) of the distribution $P(\hat{a}_i)$ for removing the top part of the QRS complex with different window sizes (w), as defined by the equation:

$$w^* = \arg\min_{w} var(P(\hat{a}_i)); 1 \le i \le q \tag{4}$$

We consider a widow (w) of the signal, centered at the R-peak, with increasing size until the radius of the window becomes equal to the length of the Q-S segment. Then we exclude the window, resample the remaining part of the signal, and compute the variance of the distribution $P(\hat{a}_i)$ of the obtained samples $\hat{a}_i$. We select the window w^* such that removal of it yields the minimum variance. Right side of Fig. 3 shows the effect of the optimization process on the distribution of samples obtained by 4-, 6-, and 8-bit quantization. The use of global optimization is feasible because the maximum possible window size is limited by the length of the QRS complex which is only a small part of the signal.

Fig. 4(a) shows a segment of an ECG signal before normalization and the window of the signal that was selected by the optimization process. Fig. 4(b) shows the segment after resampling and normalization without removal of the window. Fig. 4(c) shows the segment with removal of the window but without resampling and normalization. Next, the segment is divided into two sub-segments f_{pq} (P-Q segment) and f_{st} (S-T segment) with r_1 and r_2 samples respectively, where $r_1 + r_2 < r$. The divided sub-segments f_{pq} and f_{st} are discrete representations of useful parts of noise source f. As the original function was sampled at a rate higher than the Nyquist rate, we can obtain an arbitrarily large number of samples by a resampling process known as piecewise uniform resampling [30, 34]. The resampling process yields p_{pq} and p_{st} samples from f_{pq} and f_{st} respectively, such that $p = p_{pq} + p_{st}$. The amplitude of a sample $a_i \in R$; $i = 1 \ldots p$; is finite and real and it is normalized ($\bar{a}_i$) to the range [0–1], as shown in Fig. 4(d). The quantization of these p samples, as defined by Eq. (2), yields a n-bit binary sequence $\{b_1, b_2, \ldots, b_n\}$.

2.4. Mapping

We used a non-linear mapping process to associate the digitalized and quantized samples with the random variables. The mapping process does not change the number of bits and their distribution, and the entropy of the generated sequence does not change as well. The importance of the mapping process is that it will reduce the chance of obtaining long repeated subsequences due to the interpolation and quantization processes as the probability of getting consecutive samples with the same value will increase with an increasing value of n. Since we use only deterministic operations, the process is invertible and the sequence could be completely recovered to verify the signature. The algorithm is given below:

Algorithm Mapping ($\{b_1, b_2, \ldots, b_n\}$, c)

Input: binary sequence $\{b_1, b_2, \ldots, b_n\}$, c is a constant
Output: Random process $\{X_1, X_2, \ldots X_n\}$
for $j \leftarrow 1$ to c do
begin

1. The n-bit sequence is divided into two equal subsequences and swap the sequence as follows:

$$b_{i|i=1,\ \ldots,\ k} = \begin{cases} b_{i+k/2} & if\ i \leqslant k/2 \\ b_{i-k/2} & if\ i > k/2 \\ b_i & if\ i = k/2 \times 2. \end{cases} \tag{5}$$

2. These two subsequences are merged by taking the alternative samples from each subsequence as follows:

$$b_{i|i=1,\ \ldots,\ k} = \begin{cases} b_{i/2+1} & if\ i\ is\ odd \\ b_{(i+k)/2} & if\ i\ is\ even. \end{cases} \tag{6}$$

3. The n bit sequence (or the maximum part possible) is reshaped into a square matrix. The matrix is transposed and then the i-th row is swapped with the $(i + j)$-th row
4. The resulting matrix is again reshaped to convert it into a sequence of n bits $\{b'_1, b'_2, \ldots, b'_n\}$.
5. $b_i = b'_i$; $0 \le i \le n$

end

6. $X_i = b_i; 1 \le i \le n$.

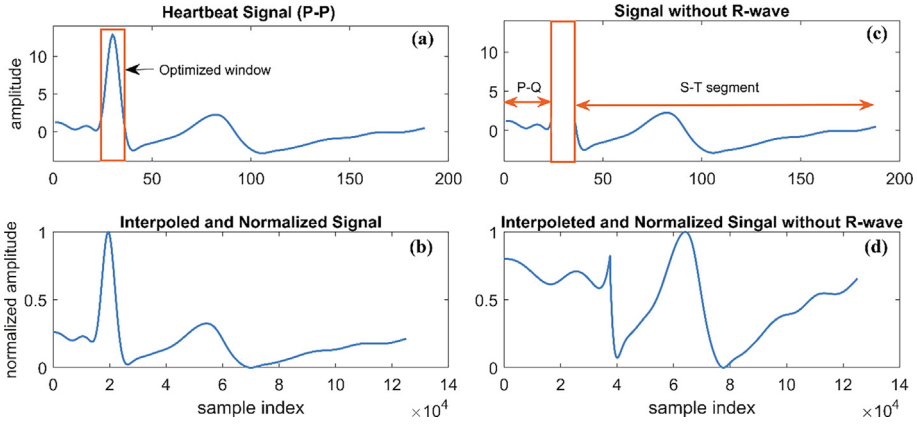

Fig. 4. (a) P-P segmented heartbeat signal (noise source) with selected window w^*, (b) interpolated samples without removal of the window, (c) the signal after removal of the window, (d) interpolated and normalized samples after removal the window.

2.5. Throughput and computational complexity

The throughput can be defined as the number of bits produced by the RBS generator in a unit time. Due to the physiological constraint, the capturing time of a P-P segment could be up to one second for a healthy individual, although the average duration is smaller than that. Hence, the throughput for a heartbeat signal based RBS generation system depends on two factors: i) duration of the heartbeat and ii) computational complexity. In this work, we need a single heartbeat signal as the noise source and the capturing time is minimal compared to existing methods. In fact, by our method we can increase the value of n arbitrarily using the same segment of ECG signal. Hence, the computational complexity of the proposed method is the important factor for efficient RBS generation with high throughput.

In the interpolation and uniformity optimization process, we first detect the R peak using an $O(r)$ algorithm where r is the number of samples in the signal, which is limited by the sampling rate. Then the iterative optimization process interpolates the signal at each iteration. Due to the use of the global optimization process, the number of iterations (p) is small and limited by the length of the QS segment, which is a small fraction of r. By using cubic spline functions, we can obtain q samples in $O(p \times q)$ times. Since p is a small fraction of r and $O(r)$ is negligible, the total time required by the process is $O(q)$, which is linear to the number of samples q.

Each of the six steps of the mapping algorithm is a linear-time operation for one iteration. By applying these operations only for a constant number of iterations, the shuffling process remains a linear-time operation. Although n is big, for a particular application it is bounded and the total computational cost of the proposed method becomes linear. Hence, real-time response is possible using a machine with ordinary computing power even for a long RBS.

3. Experiments and results

Recently, NIST updated its guidelines for the evaluation of an entropy source for cryptographic bit generation using physical processes. According to this recommendation, known as NIST 800-90B (Turan et al., 2018), the testing of an entropy source can be carried out in two different tracks: IID track and non-IID track. The IID track is used for an entropy source that generates independent and identically distributed samples, whereas the non-IID track is used for entropy sources that do not generate IID samples. As discussed in Section 2, the proposed Bernoulli entropy source consists of n independent and identically distributed random variables to produce a sequence of n bits of IID samples and we evaluate the entropy source as the IID-track.

In cryptography, the unpredictability of secret keys is essential. The probability of guessing a secret correctly in the first trial is related to the entropy of the secret generated from the noise source and the unpredictability increases with the increase of entropy. NIST recommends using a very conservative measure known as min-*entropy*. The min-entropy of an independent discrete random variable X_i, which takes values from the set {0, 1} with probability $P(X_i = 0) = p_0$ and $P(X_i = 1) = p_1$ is defined as

$$H = -log_2(min(p_0, p_1)) \tag{7}$$

In Subsection 3.1, we summarize the validation process for the IID-track. We used two different databases for the validation. In Subsection 3.2, we describe the databases and the experimental protocols. Subsections 3.3 and 3.4 independently give the validation results of these two databases. Finally, Subsection 3.5 shows the entropy for heartbeat signals from different ECG records and for different throughputs.

3.1. Entropy source validation for the IID-Track

As recommended by NIST 800-90B, a sequence of at least one-million bits is required to be collected from the entropy source for the validation process. In this work, the sequence generated by n binary random variables is tested using statistical tests for verification of the IID assumption, and it is accepted as a RBS if it passes all tests. Three different sets of statistical tests are carried out on the generated bit sequence: i) permutation tests, ii) chi-square statistical tests, and iii) restart tests. Each of these tests, discussed in the following three subsections, takes a sequence as input and tests the hypothesis that the bits are IID. If the hypothesis is rejected by any of the tests, the sequence is considered to be non-IID.

Table 2
Permutation tests for the PTB database.

i	Name of test	Quantization Levels					
		4-bit		6-bit		8-bit	
		$C_{i,0}$	$C_{i,1}$	$C_{i,0}$	$C_{i,1}$	$C_{i,0}$	$C_{i,1}$
1	Excursion Test Statistic	304	0	3503	0	8985	0
2	Number of Directional Runs	9032	18	3058	28	5650	35
3	Length of Directional Runs	6914	2033	7179	1912	252	3033
4	Number of Increases and Decreases	2439	25	7149	30	595	14
5	Number of Runs Based on the Median	2308	5	8336	6	7578	5
6	Length of Runs Based on Median	585	1142	6509	1299	5249	1754
7	Average Collision Test Statistic	1759	1	171	2	1873	4
8	Maximum Collision Test Statistic	2410	1150	7767	552	1172	815
9	Periodicity Test Statistic (log = 1)	1538	19	5096	30	1412	13
10	Periodicity Test Statistic (log = 2)	9428	5	7998	19	2118	25
11	Periodicity Test Statistic (log = 8)	1294	15	6285	23	3898	27
12	Periodicity Test Statistic (log = 16)	1336	21	7919	19	9122	10
13	Periodicity Test Statistic (log = 32)	3969	19	6444	14	1794	27
14	Covariance Test Statistic (log = 1)	6427	3	3191	8	4298	5
15	Covariance Test Statistic (log = 2)	8805	3	2440	10	8259	0
16	Covariance Test Statistic (log = 8)	9788	1	6578	5	9820	0
17	Covariance Test Statistic (log = 16)	465	5	652	3	8312	4
18	Covariance Test Statistic (log = 32)	9553	4	4677	4	6156	7
19	Compression Test Statistic	8681	18	1515	18	2166	44
	Permutation Tests Assessment	Passed		Passed		Passed	

Table 3
Chi-square statistical tests for the PTB database.

i	Name of test	Quantization Levels					
		4-bit		6-bit		8-bit	
		test statistic (T)	*critical value (C_v)*	*test statistic (T)*	*critical value (C_v)*	*test statistic (T)*	*critical value (C_v)*
1	Independence Test	961.5	1167.4	1926.9	2249.4	2057.3	2249.4
2	Goodness-of-fit Test	4.4	27.9	11.8	27.9	9.2	27.9
3	Length of the Longest Repeated Substring Test (the threshold for P is 0.001)	P = 0.81		P = 0.89		P = 0.322	
	Chi-square Tests Assessment	Passed		Passed		Passed	

3.1.1. Permutation tests

The permutation tests consist of a set of eleven statistical hypothesis tests as listed in Tables 2 and 6. Given an input bit sequence, ten-thousand (10,000) permutations are generated for each of the tests and the test statistic of the original sequence is compared to that of each permutation. Two counters initialized with zeros, $C_{i,0}$ and $C_{i,1}$ (where i is the index of a test), are used to find the ranking of the original test statistics among the permuted test statistics. The values of $C_{i,0}$ and $C_{i,1}$ are increased when the statistical value of a permutation for the i-th test is greater than and equal to the value of the original sequence respectively. If the samples are IID, their test statistics should be similar and type-I error probability should not exceed 0.001. Hence, extreme values for the counters suggest that the bits are not IID and the following condition should be satisfied to pass each of the tests:

$$C_{i,0} + C_{i,1} > 5 and C_{i,0} < 9995 \tag{8}$$

3.1.2. Chi-square tests

The chi-square tests consist of three statistical tests such as the independence test, goodness-of-fit test, and length-of-the-longest-repeated-substring test, as listed in Tables 3 and 7. The independence test checks dependencies between successive bits in a sequence by comparing the frequencies of m-bit tuples to their expected values. The test passes, if the chi-square test statistic (T) is smaller than the critical value (C_v) with 2 m–2 degrees of freedom when the type-I error is chosen as 0.001. The goodness-of-fit test attempts to check whether the distribution of the ones remains the same throughout the entire bit sequence. Here, the test statistic (T) is a chi-square random variable with nine degrees of freedom. Similar to the independence test, the test passes if T is smaller than the critical value (C_v) at type-I error 0.001, i.e.

$$T < C_v \tag{9}$$

The length-of-the-longest-repeated-substring test checks if the length of the longest repeated substring is significantly longer than the expected value which invalidates the IID assumption. Suppose w is the length of a longest repeated substring in the given bit sequence with length n, X_i is a binomially distributed random variable with parameter $j = \binom{n-w-1}{2}$, and a probability of success $p_s = (p^2 + (1 - p)^2)^w$, where p is the probability of the number of 1′s in the sequence. Then, the test passes if

$$P(X_i \geq 1) = 1 - (1 - p_s)^j \geq 0.001. \tag{10}$$

3.1.3. Entropy estimation and restart tests

If the bit sequence passes all permutation and Chi-square tests, the initial entropy is estimated using the min-entropy estimation determined using the most-common-value estimate (Turan et al., 2018). This method first finds the proportion P = max (p, 1 − p), where p is the probability of 1's in the given sequence. The upper bound of the confidence interval is used to estimate the min-entropy per sample of the source:

$$p_u = min\left(1, \hat{p} + 2.576\sqrt{\frac{\hat{p}(1-\hat{p})}{L-1}}\right) \tag{11}$$

where 2.576 corresponds to the $Z_{(1-0.005)}$ value.

Then the initial estimation of min-entropy (H_I) is

$$H_I = -log_2(p_u) \tag{12}$$

The estimated entropy of a source might provide an overestimate if the noise source generates correlated sequences after restarts. The restart tests re-evaluate the entropy estimation using different outputs from many restarts of the noise source. This ensures that bits in a restart sequence are drawn from the same distribution but are independent and uncorrelated. This will prevent an attacker (with access to output sequences of multiple noise sources) from predicting the next output sequence. For the restart tests, we use 1000 different heartbeats, and from each of them, 1000 bits are collected. This data is stored in a 1000 × 1000 restart matrix M, where samples from a heartbeat are stored in a row. Then two tests are carried out: i) sanity check, and ii) validation test.

The sanity-check tests the frequency of the most common value X_{max} in the rows and the columns of the matrix M. If this frequency is significantly greater than the expected value $P(X > X_{max})$, given the initial entropy estimate H_I, the restart test fails and the sequence is considered non-IID. Setting the probability of type-I error at 0.01 and with the error α for each of the binomial experiments, the test passes if

$$P(X > X_{max}) = \sum_{j=X_{max}}^{1000} \binom{1000}{j} p^j (1-p)^{1000-j} \geq \alpha \tag{13}$$

If the random bit sequence passes the sanity check, the validation test is carried out. Two datasets are constructed: i) the row dataset is constructed by concatenating the rows, and ii) the column dataset is constructed by concatenating the columns of M. Then, the entropy is estimated for the row (H_r) and column (H_c)

Table 4
Initial estimation of entropy for the PTB database.

Record #	Quantization Levels		
	4-bit	6-bit	8-bit
Record 1	0.8664	0.8159	0.8778
Record 2	0.9085	0.9209	0.8659
Record 3	0.8436	0.9204	0.9171
Average H_I	0.8728	0.8857	0.8869

datasets. The validation test passes if the minimum of H_r and H_c is more than half of H_I. The final entropy assessment (H) of the source becomes the minimum of the row, the column, and the initial estimates, i.e.,

$$H = min(H_r, H_c, H_I) \tag{14}$$

3.2. Databases and experimental protocol

We have used two databases for the evaluation of our method. The first one is known as PTB (Physikalisch–Technische–Bundesanstalt) which is publicly available in Physionet (Goldberger et al., 2000). This dataset contains 60 s ECG records collected with a sampling frequency of 1000 Hz from 290 individuals with ages ranging from 17 to 87 years. We also used an in-house database of ECG signals captured from fingers (Islam et al., 2017). This dataset contains 656 ECG records from 164 individuals collected in two different sessions. We used a commercially available finger-based ECG device to capture each record of the ECG signal for fifteen seconds from the thumbs of a subject at a sampling frequency of 250 Hz.

We independently tested and evaluated the proposed method using both databases. First, we inspected all the records and excluded those heartbeats which had been significantly altered by noise during capturing time. For testing and initial entropy estimation, we used the first five records from each database. For evaluation of IID assumption, one heartbeat (P-P segment) was selected randomly from one of these ECG records and one million bits were generated from it by the method discussed in Section 2. The number of extracted samples for the heartbeat depends on the quantization levels. For 4-, 6-, or 8-bit quantization, 250 000, 166 667, and 125 000 samples were collected, respectively. Each of these samples was quantized accordingly and then shuffled to obtain the random sequence. Then, permutation and Chi-square tests were carried out.

For initial entropy estimation, we used three heartbeats randomly selected from the first five records and compute the min-entropy, and the average of these estimations was used as an initial estimation H_I. Then for the restart test, we used 1000 heartbeat signals collected from different ECG records and 1000 bits were collected from each of them. We applied increasing numbers of iterations for the shuffling operations on the bits collected from each heartbeat and the sanity check and validation test were carried out. Finally, the initial entropy estimation was updated to obtain the final entropy. In Subsection 3.3, and 3.4, we present the experimental results for all these tests using PTB and FEGG databases respectively.

3.3. Results of validation on the PTB database

This section presents the results of entropy source validation for the IID-track using the PTB database. Table 2 shows test statistics ($C_{i,0}$ and $C_{i,1}$) for eleven permutation tests for three different levels of quantization. All tests passed by satisfying the criteria given in Eq. (8). It could be noted that for both of the periodicity test statistic and covariance test statistic, five different logs were used. Table 3 shows the results of three chi-square statistical tests for different levels of quantization and all tests passed by satisfying the criteria discussed in Subsection 3.1.2. Initial estimation of entropy for three different heartbeats, individually obtained from three different ECG records, and the average entropy are shown in Table 4. Results of restart tests and updated entropy estimation are shown in Table 5. It could be noted that sanity check and validation tests passed the criteria discussed in Subsection 3.1.3.

3.4. Results of validation on the FECG database

This section presents the results of entropy source validation for the IID-track using the FECG database. Table 6 shows test statistics ($C_{i,0}$ and $C_{i,1}$) for eleven permutation tests, for three different levels of quantization, and all tests passed by satisfying the criteria given in Eq. (8). Like before, for both of the periodicity test statistic and covariance test statistic, five different logs were used. Table 7 shows the results of three chi-square statistical tests for different levels of quantization and all tests passed by satisfying the criteria discussed in Subsection 3.1.2. Initial estimation of entropy for three different heartbeats individually obtained from three different ECG records and the average entropy are shown in Table 8. Results of restart tests and updated entropy estimation are shown in Table 9. It could be noted that sanity check and validation tests passed the criteria discussed in Subsection 3.1.3.

3.5. Entropy and throughput

We computed entropy for three different heartbeats (HB-1, HB-2, HB-3), selected randomly, from each of the first five records of both databases. We extracted one-million bits using 8-bit quantization to compute the entropy. Then, we computed the average entropy for each record as shown in Table 10.

We also tested the throughput for three different heartbeats randomly selected from each of the first five records of ECG signal from both databases. From the same heartbeat, we extracted bit sequences for different lengths ranging from 1to10 million bits/-heartbeat. Then, for a particular length, we computed the average entropy of RBSs for three heartbeats for each quantization levels as shown in Table 11. Since the computing time is not significant, we assumed that throughput is equal to the length of a RBS by considering the total capturing and processing time for a single heartbeat ECG signal as one second.

4. Discussion

We tested a single heartbeat ECG signal as an IID source of entropy for RBS generation individually using different resampling rates and quantization levels for two different databases. It could be noted from Subsections 3.3 and 3.4 that bit sequences generated from both databases passed all permutation, chi-square, and restart tests with a good margin between the test results and critical values. For example, the value of $\boldsymbol{C_{i,0}}$ and $\boldsymbol{C_{i,1}}$ was 8985 and 0 respectively, for the excursion test statistic (Table 2) while the threshold for $\boldsymbol{C_{i,0}} + \boldsymbol{C_{i,1}}$ was 5 (lower bound) and for $\boldsymbol{C_{i,0}}$ was 9995 (upper bound), as given in Equation (8). We tested several heartbeats from different records of both databases and found equivalent results. As an initial estimation, we reported the average entropy obtained from three heartbeats randomly selected from each of the first five records, and the restart test is based on this average entropy.

The proposed optimization technique, discussed in Subsection 2.1, played a crucial role in improving the entropy by making the distribution of random variables more uniform. To observe the effect of the optimization process on the distribution of bits produced by the Bernoulli process, we have computed the distribution of 0′s and 1′s in the RBS generated from three different heartbeats before and after optimization as shown in Fig. 5. It could be noted that due to optimization the distribution becomes almost uniform on the average (50.56% 0's and 49.44% 1's).

The large throughput of the proposed method makes it promising for practical applications. We increased the throughput by

Table 5
Restart tests and updated estimation for the PTB database.

i	Name of test	Quantization Levels		
		4-bit	6-bit	8-bit
1	Sanity Check (α = 0.0000104)	P($X \geq$ Xmax) = 0.053	P($X \geq$ Xmax) = 0.0201	P($X \geq$ Xmax) = 0.0360
2	Validation Testing	H_r = 0.9472 H_c = 0.9472	H_r = 0.9503 H_c = 0.9503	H_r = 0.9379 H_c = 0.9379
	Assessment	Passed	Passed	Passed
	Updated Estimation of Entropy (H)	0.8728	0.8857	0.8399

Table 6
Permutation tests for the FECG database.

i	Name of test	Quantization Levels					
		4-bit		6-bit		8-bit	
		$C_{i,0}$	$C_{i,1}$	$C_{i,0}$	$C_{i,1}$	$C_{i,0}$	$C_{i,1}$
1	Excursion Test Statistic	2633	0	1922	0	1603	0
2	Number of Directional Runs	5540	22	8936	8	41	2
3	Length of Directional Runs	0	304	3483	3912	9146	583
4	Number of Increases and Decreases	6497	39	4471	37	8666	19
5	Number of Runs Based on the Median	468	1	2557	9	994	1
6	Length of Runs Based on Median	8392	745	9322	323	2415	2323
7	Average Collision Test Statistic	4474	9	1086	2	6493	0
8	Maximum Collision Test Statistic	1032	765	2257	1048	9488	141
9	Periodicity Test Statistic (log = 1)	8694	17	3591	29	4862	34
10	Periodicity Test Statistic (log = 2)	9307	7	7609	22	5841	25
11	Periodicity Test Statistic (log = 8)	6363	26	3450	27	4051	29
12	Periodicity Test Statistic (log = 16)	8068	13	2357	23	6385	33
13	Periodicity Test Statistic (log = 32)	7457	20	8111	23	8613	15
14	Covariance Test Statistic (log = 1)	3657	5	9214	4	7197	3
15	Covariance Test Statistic (log = 2)	7066	5	9803	0	299	0
16	Covariance Test Statistic (log = 8)	661	2	2729	7	2309	4
17	Covariance Test Statistic (log = 16)	2990	4	1249	3	3897	7
18	Covariance Test Statistic (log = 32)	6665	5	8949	1	7562	3
19	Compression Test Statistic	9344	15	3701	82	6274	61
	Permutation Tests Assessment	Passed		Passed		Passed	

Table 7
Chi-square statistical tests for the FECG database.

i	Name of test	Quantization Levels					
		4-bit		6-bit		8-bit	
		test statistic (T)	*critical value* (C_v)	*test statistic* (T)	*critical value* (C_v)	*test statistic* (T)	*critical value* (C_v)
1	Independence Test	1950.3	2249.4	1967.8	2249.4	2057.8	2249.4
2	Goodness-of-fit Test	11.4	27.9	9.2	27.9	5.1	27.9
3	Length of the Longest Repeated Substring Test (the threshold for P is 0.001)	P = 0.859		P = 0.986		P = 0.397	
	Chi-square Tests Assessment	Passed		Passed		Passed	

Table 8
Initial estimation of entropy for the FECG database.

Record #	Quantization Levels		
	4-bit	6-bit	8-bit
Record 1	0.9345	0.9061	0.9241
Record 2	0.8882	0.9632	0.9525
Record 3	0.9652	0.9236	0.9430
Average H_I	0.9293	0.9400	0.9399

increasing the resampling rate and the number of quantization levels. Due to the use of efficient cubic polynomial interpolation technique, this increase of throughput does not significantly increase the computation time but the entropy improves monotonically. Fig. 6 shows the increase of entropy for different lengths of RBS ranging from 1 to 10 million bits. This slow but monotonic increase implies that the Bernoulli process converges to the perfect source of entropy while the length of the bit sequence increases, which is a significant implication about the proposed entropy source.

We have compared the performance of the proposed method with those of state-of-the-art methods, as given in Table 12. Although several studies were evaluated by recommendations of NIST 800-90B, none of the existing works was evaluated using the IID track. The throughput of the proposed method has increased significantly due to the use of the heartbeat-resampling process making the method suitable for applications that require a long RBS. In fact, most of the existing methods fail to generate such a sequence due to their dependency on long ECG signal requiring a long time to be captured.

Table 9
Restart tests and updated estimation for the FECG database.

i	Name of test	Quantization Levels		
		4-bit	6-bit	8-bit
1	Sanity Check (α = 0.0000104)	$P(X \geq X_{max}) = 0.02$	$P(X \geq X_{max}) = 0.00057$	$P(X \geq X_{max}) = 0.0176$
2	Validation Testing	H_r = 0.9537 H_c = 0.9537	H_r = 0.9625 H_c = 0.9625	H_r = 0.9777 H_c = 0.9777
	Assessment	Passed	Passed	Passed
	Updated Estimation of Entropy (H)	0.9293	0.9400	0.9399

Table 10
Entropy for different ECG records.

	Entropy for the PTB database				Entropy for the FECG database			
ECG Record	HB-1	HB-2	HB-3	Average	HB-1	HB-2	HB-3	Average
1	0.9148	0.8596	0.8676	0.8807	0.9955	0.9543	0.9247	0.9582
2	0.8962	0.9423	0.9559	0.9315	0.9859	0.9755	0.9287	0.9634
3	0.8834	0.9877	0.9619	0.9443	0.9484	0.9501	0.9006	0.9330
4	0.9957	0.9612	0.9657	0.9742	0.9766	0.9715	0.9918	0.9800
5	0.8769	0.8879	0.9907	0.9185	0.9099	0.9339	0.9542	0.9327
	Average			0.9298	Average			0.9535

Table 11
Average entropy for different throughputs.

Length of the RBS (Million bits /HB)	Average entropy for the PTB database			Average entropy for the FECG database		
	4-bit	6-bit	8-bit	4-bit	6-bit	8-bit
1	0.8758	0.9072	0.9179	0.9545	0.9632	0.9705
2	0.8768	0.9083	0.9189	0.9556	0.9643	0.9716
4	0.8775	0.9090	0.9196	0.9563	0.9650	0.9723
8	0.8780	0.9095	0.9201	0.9568	0.9656	0.9729
10	0.8782	0.9096	0.9203	0.9570	0.9657	0.9730

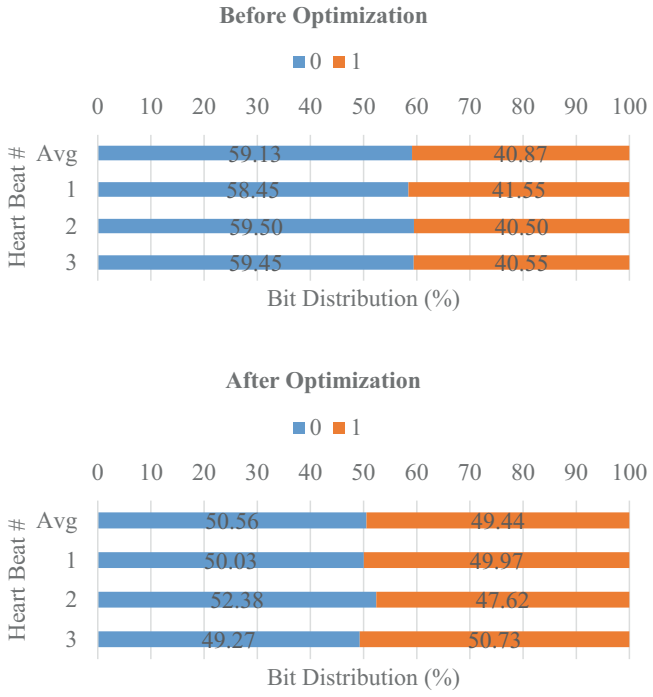

Fig. 5. Distribution of 0′s and 1′s before and after optimization.

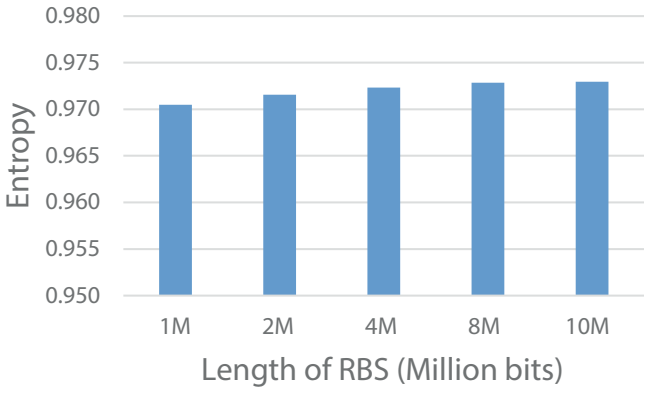

Fig. 6. Effect of length of RBS on entropy.

5. Conclusion

A single heartbeat ECG signal has been found to be feasible to yield an IID source of entropy that can be used to generate a long RBS satisfying the requirement for most cryptographic applications. The proposed method is also computationally efficient, which makes a small segment of ECG signal feasible for the generation of long RBS for practical applications. The average min-entropy of RBSs with a length of one million or more bits, obtained from several heartbeat signals from different individuals, were

Table 12
Comparison with the state-of-the-art methods.

Ref.	Important concept of the Method	Evaluation Process of the Entropy Source	Throughput (bits per heartbeat)	Applicability
(Ortiz-Martin et al., 2020)	Concatenation of five bits from 8-bit IPI value	NIST 800-90B (Non-IID track)	5	WBAN: Yes IMD: Yes OTP: No ImgEncrp: No
(Chizari and Lupu, 2019)	8-bit representation of IPI value	NIST SP 800–22, Dieharder (Brown et al., 2013)	8	WBAN: Yes IMD: Yes OTP: No ImgEncrp: No
(Pirbhulal et al., 2018)	16-bit representation of IPI value	NIST SP 800–22 (Rev 1a)	16	WBAN: Yes IMD: Yes OTP: No ImgEncrp: No
(Camara et al., 2018)	Quantization of wavelet coefficients of a heartbeat signal	NIST SP 800–22 (Rev 1a), Dieharder, ENT (Walker, 2008)	184	WBAN: Yes IMD: Yes OTP: Maybe ImgEncrp: No
(Zheng et al., 2017)	Binary representation of five feature values obtained from a heartbeat	NIST SP 800–22 (Rev 1a)	<128 (adaptive)	WBAN: Yes IMD: Yes OTP: Maybe ImgEncrp: No
(Chen et al., 2012b)	IPI value encoded into 4-bit	NIST SP 800–22 (Rev 1a)	4	WBAN: Yes IMD: Yes OTP: No ImgEncrp: No
Proposed	Resampling of ECG signal	NIST 800-90B, (IID track)	≥1,0000,000	WBAN: Yes IMD: Yes OTP: Yes ImgEncrp: Yes

close to perfect entropy of 1.0. More interestingly, the entropy increases monotonically with the increase of the length of a key. The developed entropy source has passed all tests recommended by NIST for IID source validation. The randomness of the generated RBSs for cryptographic applications requiring personalized signatures will be investigated and evaluated further in our future work using other tests such as TESTU01 (L'Ecuyer and Simard, 2007) and SP 800-90C (Barker and Kelsey, 2016).

Declaration of interests

None.

References

AlDuwaile, D.A., Islam, M.S., 2021. Using convolutional neural network and a single heartbeat for ECG biometric recognition. Entropy 23 (6), 733.

AlDuwaile, D.A., Islam, M.S., 2020. Single heartbeat ECG biometric recognition using convolutional neural network. In: 2020 International Conference on Advanced Science and Engineering (ICOASE), pp. 145–150. https://doi.org/10.1109/ICOASE51841.2020.9436592.

Argyris, A., Pikasis, E., Syvridis, D., 2016. Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators. J. Lightwave Technol. 34 (22), 5325–5331.

Arslan Tuncer, S., Kaya, T., 2018. True Random Number generation from bioelectrical and physical signals. Comput. Math. Methods Med. 2018, 1–11.

Barker, E., Kelsey, J. 2016. Recommendation for Random Bit Generator (RBG) Constructions, NIST Special Publication 800-90C.

Brown, R.G., Eddelbuettel, D., Bauer, D., 2013. Dieharder: A random number test suite Open Source software library (https://webhome.phy.duke.edu/∼rgb/General/dieharder.php).

Camara, C., Martín, H., Peris-Lopez, P., Aldalaien, M., 2019. Design and analysis of a true random number generator based on GSR signals for body sensor networks. Sensors (Basel) 19 (9), 2033.

Camara, C., Peris-Lopez, P., Martín, H., Aldalaien, M.A., 2018. ECG-RNG: A Random number generator based on ECG signals and suitable for securing wireless sensor networks. Sensors (Basel) 18 (9), 2747.

Chen, C.-K., Lin, C.-L., Chiang, C.-T., Lin, S.-L., 2012a. Personalized information encryption using ECG signals with chaotic functions. Inf. Sci. 193, 125–140.

Chen, X., Zhang, Y., Zhang, G., Zhang, Y., 2012b. Evaluation of ECG random number generator for wireless body sensor networks security. In: 2012 5th International Conference on BioMedical Engineering and Informatics, pp. 1308–1311.

Chizari, H., Lupu, E.C., 2019. Extracting Randomness From The Trend of IPI for Cryptographic Operators in Implantable Medical Devices. IEEE Transactions on Dependable and Secure Computing, 1-1.

Goldberger, A.L., Amaral, L.A.N., Glass, L., Hausdorff, J.M., Ivanov, P.C., Mark, R.G., Mietus, J.E., Moody, G.B., Peng, C.-K., Stanley, H.E., 2000. PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals. Signals 101 (23). https://doi.org/10.1161/01.CIR.101.23.e215.

González-Manzano, L., de Fuentes, J.M., Peris-Lopez, P., Camara, C., 2017. Encryption by Heart (EbH)—Using ECG for time-invariant symmetric key generation. Future Generation Comput. Syst. 77, 136–148.

Hamad, N., Rahman, M., Islam, S., 2017. Novel remote authentication protocol using heart-signals with chaos cryptography. In: 2017 International Conference on Informatics, Health & Technology (ICIHT), pp. 1–7.

Islam, M.S., 2015. Heartbeat biometrics for remote authentication using sensor embedded computing devices. Int. J. Distrib. Sens. Netw. 11 (6), 549134. https://doi.org/10.1155/2015/549134.

Islam, M.S., Alajlan, N., 2013a. An Efficient QRS Detection Method for ECG Signal Captured from Fingers, IEEE International Conference on Multimedia and Expo Workshops (ICMEW). San Jose, California, USA.

Islam, M.S., Alajlan, N., 2013b. A morphology alignment method for resampled heartbeat signals. Biomed. Signal Process. Control 8 (3), 315–324.

Islam, M.S., Alajlan, N., 2014. Augmented-hilbert transform for detecting peaks of a finger-ECG signal. In: Biomedical Engineering and Sciences (IECBES), 2014 IEEE Conference on, pp. 864–867.

Islam, M.S., Alajlan, N., 2015. Model-based alignment of heartbeat morphology for enhancing human recognition capability. Comput. J. 58 (10), 2622–2635. https://doi.org/10.1093/comjnl/bxu150.

Islam, M.S., Alajlan, N., 2016. Biometric template extraction from a heartbeat signal captured from fingers. Multimed Tools Appl 76 (10), 12709–12733. https://doi.org/10.1007/s11042-11016-13694-11046.

Islam, M.S., Alajlan, N., Bazi, Y., Hichri, H.S., 2012. HBS: a novel biometric feature based on heartbeat morphology. IEEE Trans. Inf Technol. Biomed. 16 (3), 445–453.

Islam, S., Ammour, N., Alajlan, N., Abdullah-Al-Wadud, M., 2017. Selection of heart-biometric templates for fusion. IEEE Access 5, 1753–1761.

Karimian, N., Tehranipoor, M., Woodard, D., Forte, D., 2019. Unlock Your Heart: Next Generation Biometric in Resource-Constrained Healthcare Systems and IoT. IEEE Access 7, 49135–49149.

Karthikeyan, M.V., Manickam, J.M.L., 2019. ECG-Signal Based Secret Key Generation (ESKG) Scheme for WBAN and Hardware Implementation. Wireless Pers. Commun. 106 (4), 2037–2052.

Kaya, T., 2020a. A true random number generator based on a Chua and RO-PUF: design, implementation and statistical analysis. Analog Integr Circ Sig Process 102 (2), 415–426. https://doi.org/10.1007/s10470-019-01474-2.

Kaya, T., 2020b. Memristor and Trivium-based true random number generator. Physica A 542, 124071.

Kaya, T., Tuncer, T., Avaroğlu, E., 2021. True bit generation by using two different noise sources. J. Circ., Syst. Comput. 30 (14). https://doi.org/10.1142/S0218126621502613.

Killmann, W., Schindler, W., 2001. A proposal for : Functionality classes and evaluation methodology for true (physical) random number generators. Version 3, 1.

L'Ecuyer, P., Simard, R., 2007. TestU01: A C library for empirical testing of random number generators. ACM Trans. Math. Software 33 (4), 1–40.

Lyp, T., Karimian, N., Tehranipoor, F., 2021. LISH: A New Random Number Generator using ECG Noises, IEEE International Conference on Consumer Electronics (ICCE). Las Vegas, NV, USA.

Manucom, E.M.M., Gerardo, B.D., Medina, R.P., 2019. Analysis of key randomness in improved one-time pad cryptography. In: 2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID), pp. 11–16.

Nguyen, N., Pham-Nguyen, L., Nguyen, M.B., Kaddoum, G., 2020. A low power circuit design for chaos-key based data encryption. IEEE Access 8, 104432–104444.

Ortiz-Martin, L., Picazo-Sanchez, P., Peris-Lopez, P., 2020. Are the Interpulse Intervals of an ECG signal a good source of entropy? An in-depth entropy analysis based on NIST 800–90B recommendation. Fut. Gen. Comput. Syst. 105, 346–360.

Ortiz-Martin, L., Picazo-Sanchez, P., Peris-Lopez, P., Tapiador, J., 2018. Heartbeats do not make good pseudo-random number generators: an analysis of the randomness of inter-pulse intervals. Entropy 20 (2), 94.

Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S.C., Zhang, Y.-T., 2018. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. IEEE Trans. Biomed. Eng. 65 (12), 2751–2759.

Ramli, S.N., Ahmad, R., Abdollah, M.F., Dutkiewicz, E., 2013. A biometric-based security for data authentication in Wireless Body Area Network (WBAN). In: 2013 15th International Conference on Advanced Communications Technology (ICACT), pp. 998–1001.

Revesz, P., 2014. Cubic spline interpolation by solving a recurrence equation instead of a tridiagonal matrix. CSE Conference and Workshop.

Sivaraman, R., Rajagopalan, S., Amirtharajan, R., 2020. FPGA based generic RO TRNG architecture for image confusion. Multimed. Tools Appl. 79 (19), 13841–13868.

Sörnmo, L., Laguna, P., 2005. Bioelectrical Signal Processing in Cardiac and Neurological Applications. Academic Press.

Stipčević, M., Koç, Ç.K., 2014. True Random Number Generators, Open Problems in Mathematics and Computational Science. Springer International Publishing.

Turan, M.S., Barker, E., Kelsey, J., McKay, K.A., Baish, M.L., Boyle, M., 2018. Recommendation for the Entropy Sources Used for Random Bit Generation, NIST Special Publication 800-90B.

Venkatasubramanian, K.K., Gupta, S.K.S., 2010. Physiological value-based efficient usable security solutions for Body Sensor Networks. ACM Trans. Sens. Netw. 6 (4), 1–36.

Walker, J., 2008. ENT: A Pseudorandom Number Sequence Test Program, http://www.fourmilab.ch/random.

Wu, H., Yin, Z., Xie, J., Ding, P., Liu, P., Song, H., Chen, X., Xu, S., Liu, W., Zhang, Y., 2021a. Design and implementation of true random number generators based on semiconductor superlattice chaos. Microelectron. J. 114, 105119. https://doi.org/10.1016/j.mejo.2021.105119.

Wu, S.-C., Hung, P.-L., Swindlehurst, A.L., 2021b. ECG Biometric Recognition: Unlinkability, Irreversibility and Security. IEEE Internet Things J. 8 (1), 487–500.

Yu, F., Li, L., Tang, Q., Cai, S., Song, Y., Xu, Q., 2019. A Survey on True Random Number Generators Based on Chaos. Discr. Dyn. Nat. Soc. 2019, 1–10.

Zheng, G., Fang, G., Shankaran, R., Orgun, M.A., 2015. Encryption for implantable medical devices using modified one-time pads. IEEE Access 3, 825–836.

Zheng, G., Fang, G., Shankaran, R., Orgun, M.A., Zhou, J., Qiao, L.i., Saleem, K., 2017. Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. IEEE J. Biomed. Health. Inf. 21 (3), 655–663.