مولد سلاسل عشوائية بالاعتماد على إشارة تخطيط القلب

م. كريستين زينيه* و د. م. محمد مازن المحايري**
و د. م. مفيد حداد***

الملخص

شبكة الجسم اللاسلكية (Wireless Body Area Network WBAN) هي عبارة عن مجموعة من الحساسات اللاسلكية المتصلة مع بعضها البعض، تقوم بنقل البيانات الحيوية المقاسة من جسم الإنسان، تستخدم بدرجة أساسية في أنظمة العناية بالصحة. في تلك الأنظمة يمكن أن يكون للهجمات الأمنية على البيانات الحيوية المتبادلة آثار سلبية قد تصل إلى تهديد حياة المريض. لذلك فإن الحفاظ على سرية وسلامة المعلومات الصحية في WBAN هو مطلب أساسي جداً. يعتبر توليد سلاسل البتات العشوائية (Random bit sequences RBSs) جانباً أساسياً في تحقيق حماية شبكات WBAN. ولكن بسبب محدودية موارد تلك الشبكات، يتعذر استخدام مولدات الأرقام شبه العشوائية التقليدية فهي تستهلك الكثير من الطاقة وقدرة المعالجة. اقترح بعض الباحثين الاعتماد على القيم الحيوية في توليد السلاسل العشوائية وبالتحديد على قيم إشارة التخطيط الكهربائي للقلب (Electrocardiogram ECG) مما يقلل من استهلاك الموارد. ولكن طرقهم تعاني من معدل إنتاج (throughput) منخفض لا يتناسب مع تطبيقات الرعاية الصحية التي تعمل في الزمن الحقيقي. استطعنا في هذا البحث تطوير مولد سلاسل عشوائية جديد بالاعتماد على إشارة ECG، يتمتع بمعدل إنتاج أفضل بعشرات أو مئات المرات من الطرق السابقة. كما أن المولد المطور يوفر استهلاك الموارد نظراً لاعتماده على عمليات حسابية بسيطة جداً. لتقييم المولد المقترح، تم إنشاء سلاسل عشوائية طول كل منها 128 بت اعتباراً من مجموعتي بيانات ECG، المجموعة الأولى هي بيانات أشخاص أصحاء، أما المجموعة الثانية فهي بيانات لأشخاص يعانون من عدم انتظام في نبضات القلب (Arrhythmia). تم قياس مدى العشوائية (Randomness) والتميز (Distinctiveness) في RBSs الناتجة من خلال تطبيق الاختبارات الإحصائية للمعهد الوطني للمعايير والتكنولوجيا (NIST) ومسافة هامينغ (Hamming Distance). وتم إثبات أن RBSs الناتجة صالحة للاستخدام في تطبيقات حماية المعلومات.

الكلمات المفتاحية: شبكة الجسم اللاسلكية (WBAN)، إشارة التخطيط الكهربائي للقلب (ECG)، مولد الأرقام العشوائية (RNG)، مولد الأرقام شبه العشوائية (PRNG)، سلاسل البتات العشوائية (RBS).

*طالبة دكتوراه هيئة فنية في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.
**أستاذ مساعد في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.
***مدرّس في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.

Random Bit Sequence Generator Based on ECG Signal

Eng. Christine Zenieh[*] Dr. Eng. Mohamed Mazen Al-Mahairi[**]
Dr. Eng. Moufid Haddad[***]

Abstract

A Wireless Body Area Network (WBAN) is a group of communicating wireless sensors that exchange biological values measured from a human body. This network is used essentially in health care systems. In such systems, security attacks on the exchanged biological data have negative effect and may threaten patient's life. Therefore, maintaining the confidentiality and integrity of health information in WBAN is a very essential requirement. The generation of random bit sequences (RBSs) is an essential aspect of protecting WBAN. However, due to the very limited resources of these networks, traditional pseudorandom number generators cannot be used as they consume a lot of energy and processing power. To reduce resource consumption in WBANs, some researchers suggested using biometrics in generating random bit sequences, specifically the electrocardiogram (ECG) signal. Nevertheless, their methods suffer from low throughput that is inconsistent with healthcare applications in real time. In this paper, we present a new random sequence generator based on ECG signal, which has a throughput tens or hundreds of times higher than previous methods. In addition, the developed generator reduces resources consumption due to its very simple processing operations. To evaluate the proposed generator, RBSs of 128 bits were generated from two ECG data sets, the first is for healthy people, and the second is for people who suffer from arrhythmia. Randomness and distinctiveness of generated RBSs are measured by using the National Institute of Standards and Technology (NIST) statistical tests and hamming distance. Thus, we have proved that the resulting RBSs are appropriate for information security applications.

Key words: Wireless Body Area Network (WBAN), Electrocardiogram (ECG), Random Number Generator (RNG), Pseudorandom Number Generator (PRNG), Random Bit Sequence (RBS)

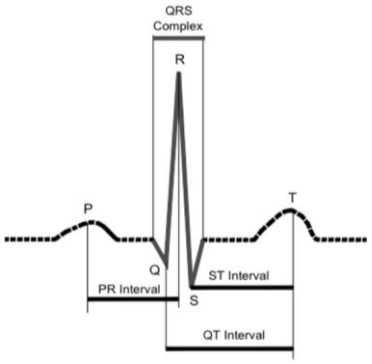
[*]PhD student, and member of technian assembly in computer and Automation Engineering, Department, Faculty of Mechanical and Electrical Engineering, Damascus University.
[**] Associate Professor , Computer and Automation Engineering, Department, Faculty of Mechanical and Electrical Engineering, Damascus University.
[***]Lecturer, , Computer and Automation Engineering, Department, Faculty of Mechanical and Electrical Engineering, Damascus University

المقدمة:

شبكة الجسم اللاسلكية WBAN هي عبارة عن مجموعة من الحساسات المختلفة المتصلة مع بعضها البعض والتي تقيس القيم الحيوية لجسم الإنسان بهدف مراقبة الحالة الصحية للمرضى عن بعد (Al-Janabi et *al.*, 2017, 114). يتم وضع تلك الحساسات إما على سطح جسم الإنسان أو حوله أو داخله. يمكن استخدامها لقياس تغيرات القيم الحيوية المختلفة للإنسان مثل مراقبة درجة حرارة الجسم، ضغط الدم، قياس معدل أكسجة الدم، التخطيط الكهربائي للقلب (ECG)، وغيرها (Masdari el *al.*, 2017, 1)، (Negra el *al.*, 2016, 1275). يتم استخدام البيانات المحصلة من تلك الحساسات في أنظمة العناية بالصحة، فعلى سبيل المثال، يتم تنبيه الأطباء المختصين عند وقوع حدث ما يهدد حياة المريض (Masdari el *al.*,2017,1). لضمان تقديم الرعاية الصحية بشكل سليم، وبهدف الحفاظ على خصوصية البيانات الصحية، لابد من حماية الاتصالات بين حساسات شبكة WBAN (Venkatasubramanian et *al.*, 2009, 60). حيث يمكن أن يتسبب التلاعب في البيانات بحوادث طبية خطيرة يمكن أن تصل إلى تهديد حياة المريض (Zhao et *al.*, 2015,1). تظهر في تطبيقات التشفير الحاجة إلى الأرقام العشوائية. على سبيل المثال، تستخدم أنظمة التشفير مفاتيح يجب إنشاؤها بحيث تكون عشوائية. كما أن العديد من بروتوكولات التشفير تتطلب مدخلات عشوائية أو شبه عشوائية في نقاط مختلفة (Rukhin et *al.*, 2001, Abstract-1). هناك نوعان أساسيان من المولدات المستخدمة لإنتاج الأرقام العشوائية وهي: مولدات الأرقام العشوائية (Random Number Generators RNGs) ومولدات الأرقام شبه العشوائية (Pseudo-Random Number Generators PRNGs).

تَستخدِم RNG مصدراً للإنتروبية، عادةً ما يكون مصادراً فيزيائياً، جنباً إلى جنب مع بعض عمليات المعالجة بهدف التغلب على أي ضعف في مصدر الانتروبية. يمكن استخدام مخرجات RNG بشكل مباشر كأرقام عشوائية أو يمكن استخدامها كمدخلات لـ PRNG. قد يستغرق إنتاج أرقام عشوائية عالية الجودة باستخدام RNG وقتاً طويلاً للغاية. لإنتاج كميات كبيرة من الأرقام العشوائية، قد تكون PRNG هي الأفضل (Rukhin et *al.*, 2001, 1-2). تستخدم PRNG مُدخلاً يسمى البذرة (seed) لتوليد أرقام شبه عشوائية. يجب أن يحصل PRNG على بذور عشوائية وغير متوقعة من مخرجات RNG لكي يضمن العشوائية الحقيقية للأرقام الناتجة عنه (Rukhin et *al.*, 2001, 1-2).

بشكل عام تُستخدم PRNG لتوليد RBSs لشبكات الحساسات اللاسلكية، ولكنها تتطلب اختيار البذور وحمايتها بعناية، بالإضافة إلى عمليات المعالجة المعقدة لضمان عشوائية السلاسل الناتجة، وهذا غالباً ما يستهلك الكثير من الموارد الحسابية. في هذا السياق، يمكن الاستفادة من حقيقة أن أجهزة الاستشعار في WBAN تقوم بتسجيل الإشارات الحيوية، وبالتالي يمكن استخراج العشوائية من تلك الإشارات. تم تطوير طرق توليد RBSs بالاعتماد على القيم الحيوية لتجنب استخدام PRNG في عقد الاستشعار وبالتالي توفر الطاقة وقدرة المعالجة (Pirbhulal et *al.*, 2018, 2).



الشكل (1): إشارة ECG (Camara et *al.*, 2018, 3) حيث P هي موجة إزالة استقطاب الأذينتين، QRS موجة إزالة استقطاب البطينين، T موجة إعادة استقطاب البطينين.

درس بعض الباحثين مؤخراً هذا الموضوع بالنسبة للإشارات العصبية. يتمثل القيد الرئيسي لهذه الدراسات في طول التسجيلات المستخدمة وحقيقة أن أجهزة التحسس لمخطط كهربية الدماغ (EEG) لها إمكانيات محدودة (Camara et *al.*, 2018, 3). ركزت العديد من الدراسات على إشارات القلب وبالتحديد إشارة ECG. هناك عدة نقاط مميزة في إشارة ECG يمكن الاستفادة منها في توليد القيم العشوائية وهي: الموجة P وهي تمثل إزالة الاستقطاب في الأذينتين. المركبة QRS وهي تمثل إزالة استقطاب البطينين. والموجة T وهي تمثل إعادة استقطاب البطينين. في الشكل (1)، تم رسم إشارة تخطيط القلب وتوضيح نقاط خصائصها.

في هذا المقال، نستعرض أبرز الأعمال السابقة في توليد السلاسل العشوائية بالاعتماد على إشارة ECG، وذلك في القسم الثاني. نورد في القسم الثالث شرحاً تفصيلياً للمخطط المقترح. أما القسم الرابع فيعرض نتائج تطبيق المخطط المقترح وميزاته مقارنةً بالدراسات السابقة. كما نجد في القسم الخامس الاستنتاجات والآفاق المستقبلية.

1. الدراسات السابقة:

اكتسب الفاصل الزمني بين دقات القلب المتتالية (الفاصل الزمني بين قمتي R لنبضتين متتاليتين والذي يشار إليه بـ Inter-Pulse-Interval IPI)، اهتمام العديد من الباحثين في مجال أمن المعلومات (Camara et *al.*, 2018, 3). كل قيمة IPI تنحرف عن الأخرى بشكل بسيط. لذلك، تستخلص معظم أساليب توليد السلاسل العشوائية فقط البتات الأربعة ذات الدلالة الأدنى من كل IPI، ثم يتم تجميعها لإنتاج 128 بت RBSs. يتمثل الجانب السلبي الرئيسي لتلك التقنيات التقليدية في أنها تستغرق وقتاً طويلاً إلى حد كبير حيث أن الحساسات يجب أن تكتشف ما لا يقل عن 33 نبضة قلب لتوليد 128 بت RBS. بالنسبة للبالغين، فإن معدل نبضات القلب الطبيعي هو 60–100 نبضة في الدقيقة، وبالتالي تتطلب تلك التقنيات وقت معالجة مرتفع يبلغ حوالي 25–30 ثانية (Pirbhulal et *al.*, 2018, 1).

قدم Xu وآخرون (2011, 5) طريقة يمكن أن تستخرج 16 بت من كل نبضة قلب؛ استخدموا الفترات RR، RQ، RS، RP، وRT لتوليد RBS. تتمثل محدودية بحثهم بأن استخدام خمس فترات مختلفة يتطلب مزيداً من عمليات المعالجة اللازمة للترميز. من أجل تحسين كفاءة الزمن، اقترح Pirbhulal وآخرون (2018, 3) جمع ثمانية قيم IPI متتالية لإنتاج RBS ذات طول 128 بت، بالإضافة إلى تطبيق تقنية تشفير الكتل الدورية (Cyclic block cipher) لتقليل أخطاء القياس وتوليد متتاليات ثنائية من نبضات القلب. إن هذه التقنية أسرع أربع مرات من الأساليب التقليدية القائمة على IPI ولكنها لا تزال تعاني من ضعف الكفاءة الزمنية.

مما سبق يتبين أن تشكيل أرقام عشوائية استناداً إلى قيم IPI يوفر أداءً منخفضاً للغاية (Camara et *al.*, 2018, 3)، كما أنه، واستناداً إلى بعض الدراسات الحديثة، يمكن تحديد الفاصل الزمني بين نبضتي قلب باستخدام الكاميرات وتحليل لون البشرة مما يجعل تلك الطرق أقل أماناً.

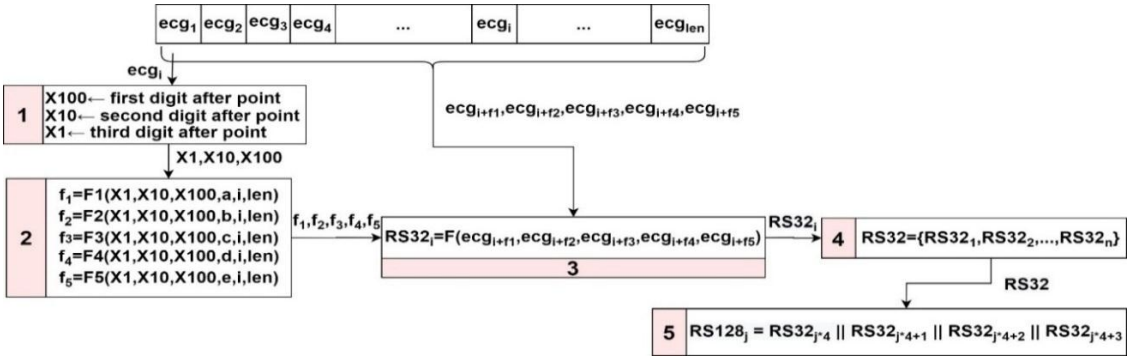
بناءً على ذلك، لم يستخدم Camara وآخرون (2018,4) قيم IPI في توليد RNG وإنما اعتمدوا على إشارة ECG بأكملها. في مخططهم المقترح، يتم بدايةً إزالة الضجيج من الإشارة المحصلة، ثم تقسيمها إلى نوافذ تحوي كل منها على ذروة R واحدة (نبضة قلب واحدة). بعدها يتم إجراء تحليل مويجي (wavelet decomposition) لكل نافذة. ثم يتم تخفيض أخذ العينات من الإشارة بمقدار النصف، وتكرار العملية لزيادة مستوى التحليل. هذه الطريقة هي أفضل من سابقاتها من حيث الإنتاجية ولكنها تحتاج لتنفيذ عمليات التحليل المويجي وبالتالي عمليات حسابية قد تؤدي إلى استهلاك طاقة الحساس.

2. مولد السلاسل العشوائية المقترح

نهدف في هذا البحث إلى تطوير مولد سلاسل عشوائية يعتمد على إشارة نبضات القلب لتوليد RBSs ذات طول 128 بت وهو الطول المناسب لمفاتيح التشفير في شبكات WBAN ولبعض القيم العشوائية الضرورية لتطبيق آليات حماية تبادل البيانات بين عقد تلك الشبكات. يعتمد المولد المطور على إشارة ECG كاملةً ليستغل جميع المعلومات الانتروبية الثرية الموجودة فيها. نسعى أن يحقق المولد المطور أعلى معدل إنتاج (توليد أكبر قدر ممكن من البتات العشوائية في الثانية) بحيث يتفوق على الدراسات السابقة، وأن يتميز ببساطة العمليات مما يقلل من استهلاك الطاقة المحدود للحساسات.

قبل البدء بشرح مخطط مولد السلاسل العشوائية المقترح، سنعتمد الافتراضين المعتمدين في كافة الدراسات السابقة وهما: أولاً، إشارة ECG سرية، أي لا يمكن لأحد التوصل إليها ما لم يكن لديه الصلاحيات اللازمة. ثانياً، إشارة ECG هي إشارة ثرية بالمعلومات الانتروبية، فهي متغيرة مع الزمن بشكل لا يمكن التنبؤ به بدقة، ولكن لا يمكن اعتبار انتروبيتها كافية لاستخدامها بشكل مباشر كسلاسل عشوائية لحماية المعلومات، فهي تحوي على بعض الخصائص الدورية ويمكن التنبؤ ببعض عيناتها.

بناءً على ما سبق، ومن أجل توليد كل تسلسل عشوائي مكون من 32 بت، قمنا بدايةً بتحصيل إشارة ECG لفترة زمنية محددة، ثم اخترنا إحدى عينات إشارة ECG المحصلة وطبقنا عليها بعض العمليات الحسابية. بعد ذلك، استخلصنا من القيم الناتجة أدلة 5 عينات ECG من الإشارة المحصلة نفسها لنستخدمها في تكوين السلسلة العشوائية. بشكل مختصر يمكن القول إنه في المولد المقترح كل سلسلة عشوائية طولها 32 بت يتم تكوينها اعتباراً من قيم 5 عينات ECG متباعدة (غير متتالية) بعد إخضاعها لبعض العمليات الحسابية. يتم اختيار تلك العينات الخمس بالاعتماد على قيمة إحدى عينات ECG المحصلة. بعد ذلك يتم تكوين سلاسل عشوائية ذات طول 128 بت بدمج 4 سلاسل عشوائية ذات طول 32 بت.



الشكل (2): مخطط مولد السلاسل العشوائية المقترح المعتمد على إشارة ECG.

حيث ecg هي إحدى عينات إشارة التخطيط الكهربائي للقلب، i رقم العينة، X100، X10، X1 قيمة أول وثاني وثالث رقم بعد الفاصلة على التوالي من عينة ecg، f_1,f_2,f_3,f_4,f_5 هو ناتج تطبيق التوابع F_1,F_2,F_3,F_4,F_5 من أجل قيم X100، X10، X1، a,b,c,d,e ثوابت سرية، len عدد عينات ecg المحصلة، $RS32_i$ السلسلة i من مجموعة السلاسل العشوائية الناتج RS32 ذات طول 32 بت، $RS128_j$ السلسلة j من السلاسل العشوائية الناتجة ذات طول 128 بت.

في المخطط المقترح اعتمدنا على ظاهرة أن قيم عينات ECG عند اختيارها بشكل غير متتالي تظهر خصائص عشوائية أفضل منها عندما تكون متتالية. فعند قراءة العينات بشكل متتالي سيكون من الأسهل التنبؤ بقيمة العينة التالية. بالإضافة إلى ذلك، لم يتم استخدام قيم العينات كما هي وإنما تم إخضاعها لبعض العمليات الحسابية البسيطة ومنها الجمع والطرح والضرب وباقي القسمة وذلك من أجل إزالة الخصائص المميزة لها وزيادة عشوائيتها.

يبين الشكل (2) مخطط مولد السلاسل العشوائية المقترح المعتمد على إشارة ECG. لتشكيل n سلسلة عشوائية طول كل منها 32 بت، والتي يمكن تمثيلها بالمجموعة $RS32=\{RS32_1,RS32_2,...,RS32_n\}$، نقوم بدايةً بتحصيل إشارة ECG خلال فترة زمنية محددة والحصول على عينات الإشارة والتي عددها len عينة، وبالتالي تكوين مجموعة العينات المحصلة وهي $\{ecg_1,ecg_2,\ldots,ecg_{len}\}$. يتم تشكيل كل سلسلة عشوائية $RS32_i$ اعتماداً على قيم خمس عينات من ECG المحصلة، حيث i هو دليل السلسلة العشوائية المولدة تتراوح قيمه من 1 حتى n. يتم اختيار العينات الخمس بناءً على: قيمة i، قيمة العينة ecg_i، قيمة len، ومجموعة من القيم السرية المحددة مسبقاً وهي a,b,c,d,e. لتوليد السلاسل العشوائية $RS32_i$ واستنتاج السلاسل العشوائية $RS128_j$ المكونة من 128 بت اعتباراً من RS32، نقوم بالخطوات التالية:

1- يتم بدايةً قراءة قيمة العينة ecg_i من مجموعة العينات المحصلة. بعدها يتم حساب القيم X1، X10، X100، بحيث نجعل قيمة X100 تساوي قيمة أول رقم بعد الفاصلة في ecg_i و X10 ثاني رقم بعد الفاصلة و X1 ثالث رقم بعد الفاصلة، وذلك على اعتبار أن قيم العينات، ecg_i، تتراوح بين 1- و1. إذا كانت قيم العينات خارج المجال {1,1-} فيجب تقييسها لتصبح ضمنه.

2- حساب قيم f_1,f_2,f_3,f_4,f_5 بناءً على قيم X1، X10، X100 من الخطوة السابقة وعلى i و len (عدد عينات إشارة ECG المحصلة) وعلى القيم السرية a,b,c,d,e وذلك كما في المعادلات من (1) حتى (5):

$$f_1 = F1(X1, X10, X100, a, i, len)$$

$$= (i \times X100 + X10 \times a \times i + X1) mod(len - i) \quad (1)$$

$$f_2 = F2(X1, X10, X100, b, i, len)$$
$$= (i \times X10 + X1 \times b \times i + X100) mod(len - i) \quad (2)$$

$$f_3 = F3(X1, X10, X100, c, i, len)$$
$$= (i \times X10 + X100 \times c \times i + X1) mod(len - i) \quad (3)$$

$$f_4 = F4(X1, X10, X100, d, i, len)$$
$$= (i \times X1 \times X100 + X10 \times d \times i + X100) mod(len - i) \quad (4)$$

$$f_5 = F5(X1, X10, X100, e, i, len)$$
$$= (i \times X1 \times X10 + X10 \times X100 \times e \times i + X100)\ mod(len - i) \quad (5)$$

حيث a,b,c,d,e هي مجموعة ثوابت سرية وهي عبارة عن أعداد صحيحة موجبة. لا يوجد قيود على هذه القيم سوى أنها يجب ألا تحوي على تسلسل من الأصفار في خاناتها العشرية وخاصةً الدنيا كي لا يؤدي ذلك إلى خفض عشوائية السلاسل الناتجة.

3- حساب السلسلة العشوائية $RS32_i$ بالاعتماد على عينات إشارة ECG المحصلة ذات الأدلة $i+f_1$، $i+f_2$، $i+f_3$، $i+f_4$، $i+f_5$ كما في المعادلة (6):

$$RS32_i = (uint32)\left(\left(ecg_{i+f1} \times 10^9 + ecg_{i+f2} \times 10^8 + ecg_{i+f3} \times 10^6 + ecg_{i+f4} \times 10^5 + ecg_{i+f5} \times 10^3\right) \times (i) + i\right) \quad (6)$$

4- يتم تكرار العمليات السابقة اعتباراً من i=1 وحتى i=n، وبالتالي تشكيل n سلسلة RS32 طول كل منها 32 بت.

5- تشكيل سلاسل عشوائية طول كل منها 128 بت من خلال دمج كل 4 سلاسل عشوائية $RS32_i$ كما في المعادلة (7):

$$RS128_j \leftarrow RS32_{j\times4+1} || RS32_{j\times4+2} || RS32_{j\times4+3} || RS32_{j\times4+4} \quad (7)$$

حيث j يمكن أن تأخذ القيم من 1 حتى n/4.

تعتمد قيمة n على عدد السلاسل العشوائية التي نريد توليدها. ولكن كحد أقصى يمكننا توليد len/2 سلسلة عشوائية ذات طول 32 بت. فلو أردنا، على سبيل المثال، تشكيل تسلسل عشوائي واحد فقط طوله 128 بت بالتالي يمكن جعل n=4. يتم اختيار قيمة n بحيث تكون أصغر أو تساوي len/2 لأن قيم f، التي تحدد العينات المساهمة في تكوين RS32، يتم حسابها بالاعتماد على باقي القسمة على len-i. فعندما تصبح قيمة i قريبة من n وإذا كانت n=len يكون ناتج باقي القسمة على len-i ذو مجال قيم محدود جداً يجعل اختيار عينات ecg المشاركة في تكوين RS32 محدوداً أيضاً. قد يضعف ذلك من عشوائية السلاسل الناتجة أو قد يسهل على المهاجم مهمة تحديد قيم ecg من RS32.

إن العمليات الحسابية باستخدام قيمة i كالجمع والطرح والضرب وباقي القسمة هي عمليات تم تطبيقها من أجل الحصول على العشوائية المطلوبة. أما استخدام القيم السرية a,b,c,d,e فهو بهدف حماية إشارة ECG من الفضح. فكما ذُكر في الدراسات السابقة، في مولدات السلاسل العشوائية المعتدة على الإشارات الحيوية، يجب ألا يتمكن المهاجم من التوصل إلى قيم الإشارة الحيوية بمعرفة التسلسل العشوائي الناتج عنها. هذا الشرط محقق في المخطط المقترح حيث لا يمكن تحديد قيم عينات ECG اعتباراً من RS32 وسيتم إثبات ذلك في القسم التالي من هذا المقال.

3. النتائج العملية

A. أمان المخطط المقترح

فيما يلي نبرهن عدم قدرة المهاجم على التوصل إلى إشارة ECG اعتباراً من السلاسل العشوائية الناتجة وعدم قدرته على التوصل إلى قيم a,b,c,d,e السرية.

إذا افترضنا أن المهاجم استطاع معرفة دليل السلسلة i بالنسبة لسلسلة معينة $RS32_i$، وأن طول كل من a,b,c,d,e يساوي 10 بت (قد تكون أطول من ذلك)، بالتالي سيحتاج معرفة f_1,f_2,f_3,f_4,f_5 وما يقابلها من أدلة العينات الخمس لإشارة ECG التي تم تشكيل $RS32_i$ اعتباراً منها إلى $(2^3)^3 \times (2^{10})^5 = 2^{59}$ تجربة. تمثل $(2^3)^3$ بشكل تقريبي عدد التجارب اللازمة للحصول على X1، X10، X100، لأن كل منها هو عبارة عن رقم عشري يأخذ إحدى

القيم من 0 حتى 9. وتمثل $5^{(2^{10})}$ عدد التجارب اللازمة للحصول على قيم a,b,c,d,e. إذا أراد المهاجم تحديد f_1,f_2,f_3,f_4,f_5 لكافة السلاسل العشوائية الناتجة، $RS32_i$، والتوصل إلى قيمة len عينة من ecg "في أسوأ الأحوال" فهو بحاجة إلى $n^{(2^{59})}$ تجربة. على سبيل المثال، إذا أراد المهاجم تحديد f_1,f_2,f_3,f_4,f_5 لكافة السلاسل العشوائية الناتجة عن العينات المحصلة خلال ثانية من الوقت وكان معدل اعتيان الإشارة يساوي 360 عينة في الثانية وكانت n=len/2، بالتالي سيحتاج المهاجم إلى $(2^{59})^{360/2} = 2^{10620}$ تجربة. نستخدم العبارة "في أسوأ الأحوال" لأنه قد يتكرر اكتشاف قيمة نفس العينة ecg_i من قبل المهاجم عدة مرات وقد يكون هناك بعض العينات التي لم يتم استخدامها في تكوين RS32، بالتالي تكون معرفة كافة قيم ecg هي السيناريو الأسوأ فهو الأقل احتمالاً. في حال كان المهاجم لا يستطيع تحديد i بالنسبة لـ $RS32_i$، أي لا يستطيع معرفة العينة التي تم تحديد f_1,f_2,f_3,f_4,f_5 منها، وبالتالي العينات المكونة لـ $RS32_i$، يصبح التوصل إلى قيم ecg أكثر صعوبة. لو افترضنا العكس، أي أن المهاجم استطاع بطريقة ما التوصل إلى قيم f_1,f_2,f_3,f_4,f_5 فهو لن يستطع التوصل إلى ecg_i لأن a,b,c,d,e هي قيم سرية. إن عملية باقي القسمة في علاقات حساب f تجعل الحصول على قيمة ecg_i عملية معقدة جداً. لو استطاع المهاجم بطريقةٍ ما التوصل إلى إشارة ECG وإلى قيم $RS32_i$ الناتجة عنها، فهو بحاجة إلى $5^{(2^{10})}$ تجربة لتحديد قيم a,b,c,d,e وبالتالي الحصول على إشارة ECG من السلاسل العشوائية التي سيتم توليدها لاحقاً.

يمكن ملاحظة أنه كلما كانت len أكبر و n أصغر، كلما استطعنا حماية إشارة ECG من الفصح اعتباراً من السلسلة العشوائية الناتجة. كما تجدر الإشارة إلى أن وجود القيم السرية a,b,c,d,e لا يجعل من المولد المقترح مولد أرقام شبه عشوائية لأن تلك القيم ثابتة مع الزمن ولا يمكن اعتبارها بمثابة نواة لتوليد السلسلة العشوائية، كما أن السلسلة العشوائية الناتجة لا تعتمد على هذه القيم فحسب وإنما تعتمد بشكل أساسي على قيم إشارة ECG المتغيرة بشكل دائم مع الزمن.

B. اختبار العشوائية والتفرد

من أجل تقييم جودة RBSs يجب التحقق من عاملين أساسيين هما العشوائية والتفرد (Distinctiveness). لا يكفي أن تكون RBS المعتمدة على نبضات القلب عشوائية بما يكفي لتعمل كمفاتيح تشفير وإنما يجب أيضاً أن تمتلك خصائص مميزة لضمان قيام الأفراد المختلفين بإنشاء RBS فريدة، وهذا ما نطلق عليه التفرد. وكذلك يجب ألا يتمكن الخصوم من الحصول على البيانات السرية لشخص ما من خلال الحصول على إشارة تخطيط القلب لشخص آخر (Pirbhulal et *al.*, 2018, 7).

لتحليل عشوائية وتفرد السلاسل العشوائية الناتجة عن المولد المقترح، تم توليد تلك السلاسل اعتباراً من بيانات (إشارة ECG) محصلة من 36 شخص. تقسم تلك البيانات إلى مجموعتين، المجموعة الأولى مكونة من بيانات 18 شخص بحالة صحية جيدة، تم الحصول عليها من قاعدة البيانات MIT-BIH Normal Sinus Rhythm Database، معدل الاعتيان فيها يساوي 128 عينة في الثانية. والمجموعة الثانية مكونة من بيانات 18 شخص يعانون من عدم انتظام في نبضات القلب، تم الحصول عليها من قاعدة البيانات MIT-BIH Arrhythmia Database، معدل الاعتيان فيها يساوي 360 عينة في الثانية. تم إجراء التجارب من أجل سلاسل عشوائية بطول 128 بت، أي من أجل RS128، ومن أجل len مقابلة لزمن تحصيل إشارة قدره ثانية واحدة. تم اختيار ثانية واحدة حيث من الأفضل أن تحوي العينات التي سينتج عنها

RBSs على نبضة قلب واحدة على الأقل، مما يؤمن عشوائية أكبر.

يجدر بنا هنا أن ننوه إلى أن زمن تحصيل الإشارة لا علاقة له بطول السلسلة الناتجة. فكما وضحنا سابقاً، وعلى سبيل المثال، إذا قما بتحصيل الإشارة لمدة ثانية واحدة وكان معدل الاعتيان يساوي 360 عينة في الثانية، فيمكننا كحد أقصى الحصول على RS32 180=2/(360×1)، يمكن تجميع كل 4 منها معاً للحصول على 45 سلسلة عشوائية طول كل منها 128 بت.

I. اختبار العشوائية

قمنا باختبار وتقييم العشوائية من خلال تحليل الانتروبية (Entropy Analysis) وإجراء مجموعة من الاختبارات الإحصائية للمعهد الوطني للمعايير والتكنولوجيا (NIST).

❖ **اختبار العشوائية من خلال تحليل الانتروبية**

يمكن تعريف الانتروبية على أنها عدم القدرة على التنبؤ بتسلسل البتات العشوائية الذي تم توليده. يمكن قياسه بتطبيق معادلة Shannon Entropy على النحو التالي:

$$H(X) = -\sum_{j=1}^{n} P(x_j) \times \log_2 P(x_j) \quad (8)$$

حيث X هو مصدر معلومات لـ n حدث مستقل و $x_1, x_2, \dots, x_n$ و $p(x_j)$ هو احتمال وقوع الحدث j.

يمكن أن يكون للإنتروبية قيمة قصوى تساوي 1 إذا كانت ذات توزع موحد، حيث أن السلاسل المختبرة مكونة من تتالي لقيمتين هما 0 و1 (Pirbhulal et *al.*, 2018, 6). لاختبار عشوائية السلاسل الناتجة تم قياس وتحليل انتروبيتها. تم حساب الانتروبية من أجل مجموعتي البيانات (بيانات الأشخاص الأصحاء وبيانات المرضى). الانتروبية الناتجة عن السلاسل العشوائية المولدة من مجموعة بيانات الأشخاص الأصحاء (18 شخص) تساوي 0.993072، حيث تم حساب متوسط الانتروبية لـ 54 سلسلة (3 سلاسل لكل شخص). أما الانتروبية الناتجة عن السلاسل العشوائية المولدة من مجموعة بيانات الأشخاص المرضى (18 شخص) تساوي 0.993831، حيث تم حساب متوسط الانتروبية لـ 54 سلسلة أيضاً (3 سلاسل لكل شخص). كما هو واضح فإن وسطي الإنتروبية أعلى من 0.99 بالتالي قريب جداً من 1. كما نلاحظ أن الانتروبية بالنسبة للسلاسل العشوائية الناتجة عن الأشخاص المرضى هي أفضل بقليل من تلك الناتجة عن الأشخاص الأصحاء. يمكن تبرير ذلك بأن عشوائية بيانات الأشخاص المرضى بعدم انتظام نبضات القلب أكبر من مقابلتها لدى الأصحاء.

❖ **اختبار العشوائية من خلال إجراء اختبارات NIST**

لتقييم عشوائية تسلسل ما ومقارنته بتسلسل عشوائي حقيقي يمكن تطبيق اختبارات إحصائية مختلفة. من أشهر تلك الاختبارات NIST Statistical Test Suite (NIST) (Rukhin,2001)، ENT (Walker)، وDieharder (Brown). NIST هي مجموعة اختبارات إحصائية مكون من 15 اختباراً، تحدد مدى عشوائية مولدات الأرقام العشوائية والأرقام الناتجة عنها. تم اختيار مجموعة الاختبار NIST دوناً عن غيرها لتقييم المولد المقترح لأنها تعنى باختبار عشوائية السلاسل التي تُستخدم لأغراض التشفير وحماية المعلومات. بالنسبة للعديد من الاختبارات في مجموعة الاختبار NIST، تم افتراض أن طول التسلسل العشوائي كبير (من مرتبة 10^3 إلى 10^7)، ولكن معظم تلك الاختبارات قابل للتطبيق على سلاسل قصيرة. في دراستنا، حيث نسعى لتوليد سلاسل عشوائية قصيرة طولها 128 بت، اكتفينا بإجراء عشرة من تلك الاختبارات والتي يمكن استخدامها لفحص عشوائية السلاسل القصيرة.

الجدول (1): نتائج اختبارات NIST على سلاسل عشوائية مولدة من بيانات أشخاص أصحاء وبيانات مرضى عدم انتظام نبضات القلب

NIST Test	Normal	Arrhythmia
Frequency test	0.495594 (107/108)	0.479416 (107/108)
Block Frequency test	0.482623 (106/108)	0.460845 (107/108)
Runs test	0.493043 (108/108)	0.506384 (106/108)
Longest Run test	0.524182 (108/108)	0.487409 (108/108)
FFT test	0.471779 (106/108)	0.418977 (105/108)
Non-overlapping (148/148)	0.880578 (108/108)	0.881454 (108/108)
Linear Complexity test	0.563778 (104/108)	0.573706 (105/108)
Serial test (2/2)	0.533063 (107/108)	0.527817 (107/108)
Approximate Entropy test	0.48837 (105/108)	0.492551 (106/108)
Cumulative Sums test (2/2)	0.505728 (107/108)	0.518168 (107/108)

يمكن تقييم عشوائية السلاسل المختبرة بناءً على قيمة α التي يطلق عليها مستوى أهمية الاختبار (level of significance). ينتج عن كل اختبار قيمة P. نفترض أن السلسلة عشوائية إذا كانت قيمة P الناتجة أكبر من قيمة α والتي تساوي 0.01 (Rukhin, 2001). أما إذا كانت P الناتجة أصغر من α فنعتبر السلسلة غير عشوائية. تم إجراء العديد من اختبارات NIST على RBSs المختلفة الناتجة للتحقق من عشوائيتها والتحقق فيما إذا كان بالإمكان استخدامها لغرض حماية المعلومات. يبين الجدول (1) نتيجة الاختبارات على السلاسل العشوائية الناتجة عن المولد المقترح باستخدام البيانات المحصلة من 18 شخص من مجموعة الأشخاص الأصحاء والبيانات المحصلة من 18 شخص من مجموعة الأشخاص المرضى خلال ثانية واحدة. تم اختبار 108 سلسلة عشوائية لكل مجموعة، بحيث تم اختيار السلاسل بشكل عشوائي (6 سلاسل لكل شخص).

تشير القيم في الجدول (1) إلى وسطي قيم P للاختبارات المجراة. وتشير القيمة بين قوسين إلى عدد الاختبارات الناجحة من أصل 108 اختبار. نجاح كل اختبار يعني أن قيمة P الناتجة أكبر من 0.01. تعطي المعادلة (9) الحد الأدنى لعدد الاختبارات التي يجب اجتيازها لكل من اختبارات NIST حتى نحكم بنجاحه (Camara et *al.*, 2019, 8).

$$mpr = (1-\alpha) - 3 \times \text{sqrt}(\frac{\alpha \times (1-\alpha)}{k}) \qquad (9)$$

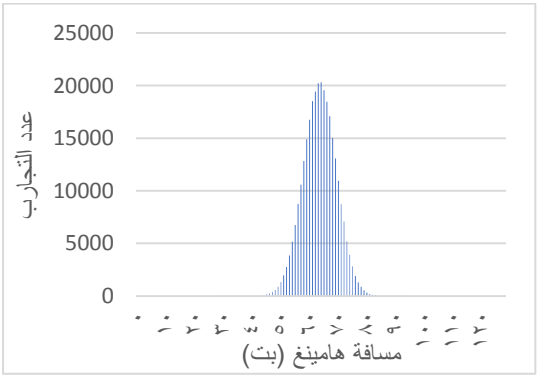
حيث α هي مستوى الأهمية و k عدد السلاسل المختبرة. في حالتنا، $\alpha = 0.01$ و $K = 108$، بالتالي يكون معدل الأدنى للنجاح هو 96%. أي يجب أن ينجح 103 اختبار أو أكثر اعتباراً من 108 اختبار.

يوضح الجدول (1) أن RBSs المولدة اجتازت الاختبارات العشرة، لأن القيمة P كانت أعلى من 0.01 في عدد من الاختبارات أكبر 103 من أجل كل اختبار. بالتالي، يمكن اعتبار RBSs المولدة من خلال بيانات أشخاص أصحاء وبيانات أشخاص مرضى بالطريقة المقترحة هي عبارة عن سلاسل عشوائية.

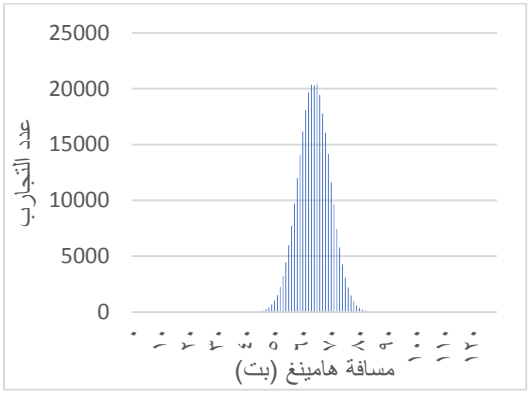
II. اختبار التفرد (التميز)

يستخدم اختبار التميز لتقييم فيما إذا كانت RBSs الناتجة اعتباراً من أجسام مختلفة، متميزة بشكلٍ كافٍ. يتم تطبيق مسافة هامينغ (Hamming Distance HD) لقياس الاختلاف بين اثنتين من RBS من نفس الطول والمولدة اعتباراً من جسمين مختلفين. بالنسبة للتسلسلات الثنائية العشوائية الحقيقية يجب أن يكون لمسافة هامينغ توزع طبيعي وبالتالي متوسط HD (average HD-distribution) يجب أن يكون مساوياً تقريباً لـ 50٪ من طول السلسلة العشوائية (Pirbhulal et *al.*, 2018, 7).

لتقييم التميز في السلاسل العشوائية الناتجة عن المولد المقترح، تم توليد ملف يحوي 1920 سلسلة عشوائية من أجل كل شخص. وتم حساب مسافة هامينغ بين السلاسل المكونة اعتباراً من بيانات كل شخص مع مقابلتها لكل شخص آخر ضمن نفس المجموعة (أصحاء، مرضى) من أجل نفس زمن تحصيل البيانات وهو ثانية واحدة.



الشكل (3) توزع مسافة هامينغ لـ RBSs الناتجة عن بيانات أشخاص أصحاء مختلفين



الشكل (4) توزع مسافة هامينغ لـ RBSs الناتجة عن بيانات مرضى مختلفين.

يوضح الشكل (3) التوزع الطبيعي لـ HDs من أجل بيانات الأشخاص الأصحاء. متوسط HDs الناتج يساوي 63.518 وهو قريب جداً من 50% من طول السلاسل العشوائية. ويوضح الشكل (4) التوزع الطبيعي لـ HDs من أجل بيانات الأشخاص المرضى. متوسط HDs الناتج يساوي 63.942، وهو أيضاً قريب من 50% من طول السلسلة.

بناءً على النتائج السابقة، RBSs الناتجة عن بيانات كل شخص تكون فريدة ويمكن استخدامها لتطبيقات الأمان في شبكات WBAN. تتحقق هذه الخاصية من أن المهاجمين لن يستطيعوا فرض تهديدات أمنية على شبكات WBAN من خلال استخدام بيانات ECG لأشخاص آخرين. كما نلاحظ أن النتائج كانت جيدة بالنسبة لبيانات الأشخاص الأصحاء والأشخاص المرضى.

C. دراسة الأداء

باستخدام المخطط المقترح، وكما ذكرنا سابقاً، يمكننا توليد عدد من RS32 يساوي نصف عدد العينات المحصل كحد أقصى. فإذا كان معدل الاعتيان يساوي 128 عينة في الثانية، نستطيع توليد 64 سلسلة RS32 في الثانية أي ما يعادل 2048 بت في الثانية. أما إذا كان معدل الاعتيان 360 عينة في الثانية فيمكننا في كل ثانية تشكيل 180 سلسلة RS32 أي ما يعادل 5760 بت. بذلك نكون قد تفوقنا تفوقاً كبيراً على معدل توليد RBSs (معدل الإنتاجية throughput) في الدراسات السابقة.

الجدول (2): معدل إنتاج المخطط المقترح مقارنةً بالدراسات السابقة، حيث PPM تمثل عدد نبضات القلب في الدقيقة.

IPI-based approaches	2 bit/second (60 PPMs)
	3.3 bit/second (100 PPMs)
(Pirbhulal et al., 2018)	8 bit/second (60 PPMs)
	13.33 bit/second (100 PPMs)
(Camara et al., 2018)	184 bit/second (60 PPMs)
	306 bit/second (100 PPMs)
Our approach	2048 bit/second (128 sample/ second)
	5760 bit/second (360 sample/ second)

يبين الجدول (2) معدل إنتاج المخطط المقترح مقارنةً بمعدل إنتاج الطرق المقترحة في الدراسات السابقة وبالتحديد في (Pirbhulal et *al.*, 2018) و(Camara et *al.*, 2018). نلاحظ التفوق الكبير لمولد الأرقام العشوائية المقترح في هذه الدراسة على باقي مولدات الأرقام العشوائية المعتمدة على إشارة ECG. كما نلاحظ ارتباط الإنتاجية

بمعدل الإعتيان على خلاف الطرق السابقة التي تعتمد فيها الإنتاجية على معدل نبضات القلب في الدقيقة (PPMs). ولكن حتى بالنسبة لمعدل اعتيان منخفض (وهو 128 عينة / الثانية) يبقى المولد المقترح ذو إنتاجية أعلى من المولدات المقترحة في الدراسات السابقة.

نلاحظ أننا استطعنا التوصل إلى مولد سلاسل عشوائية يقوم بتوليد عدد كبير من السلاسل بفترة زمنية محدودة على عكس باقي المولدات. فمولدات السلاسل العشوائية غالباً ما يجعلها اعتمادها على الظواهر الطبيعية ذات أداء بطيء، فهي عادةً ما تقوم بتوليد سلاسل عشوائية قصيرة خلال زمن طويل نسبياً. أما مولدات الأرقام شبه العشوائية فيتم استخدامها عند الحاجة لتوليد سلاسل عشوائية كثيرة خلال زمن قصير. في المولد المطور استطعنا تجاوز إحدى أهم سلبيات مولدات الأرقام العشوائية والحصول بالمقابل على إحدى أهم ميزات مولدات الأرقام شبه العشوائية، ألا وهي توليد عدد كبير من السلاسل العشوائية خلال فترة زمنية قصيرة.

بما يتعلق باستهلاك موارد المعالجة والطاقة فيجدر بنا الإشارة إلى أن المولد المقترح هو أقل استهلاكاً لموارد المعالجة والطاقة وذلك لأن العمليات التي يحتاجها في توليد السلاسل العشوائية بسيطة للغاية. رغم بساطة تلك العمليات إلا أننا استطعنا أن نثبت أن المولد المقترح يولد سلاسل تتمتع بالخصائص العشوائية المطلوبة لاستخدامها في حماية المعلومات.

4. الاستنتاجات والآفاق المستقبلية

يتميز مولد السلاسل العشوائية المقترح في دراستنا بعدم اعتماده على قيم IPI، وإنما تُستخدم إشارة ECG بأكملها لاستخراج العشوائية. وهو ليس الوحيد الذي يعتمد على إشارة ECG كاملةً، ولكن ما يميزه عن غيره هو معدل الإنتاج الذي استطعنا الوصول إليه، حيث يتجاوز معدل إنتاج المولد المقترح أسلافه بعشرات أو مئات المرات. بالإضافة إلى ذلك، لا يحتاج المولد المقترح إلى عمليات تشفير أو تحليل طيفي أو توابع هاش أو غيرها من العمليات التي قد تستهلك طاقة الحساسات، فهو يتميز ببساطة العمليات.

تم إجراء كافة التجارب على مجموعتين من البيانات وهي بيانات أشخاص أصحاء وبيانات أشخاص مرضى بعدم انتظام ضربات القلب. كان بإمكاننا الاكتفاء باختبار المولد المقترح باستخدام بيانات أشخاص أصحاء وهو أسوأ السيناريوهات، لأن المرض نفسه من شأنه أن يدخل المزيد من الانتروبية في إشارة تخطيط القلب. ومع ذلك اختبرنا بيانات المرضى للتحقق بشكل عملي من عشوائية السلاسل الناتجة عنها.

جانب آخر مهم في المولد المقترح، وهو عدم قدرة الخصم على التنبؤ بالقيم العشوائية المولدة من بيانات شخص باستخدام بيانات شخص آخر. تشير التجارب التي أجريت بوضوح إلى عدم وجود فرصة للمهاجم في النجاح بالقيام بذلك. علاوة على ذلك، وعلى عكس الطرق القائمة على IPI، يمنع استخدام إشارة ECG بأكملها الهجمات التي يتم فيها التنصت على إشارة نبضات القلب من مسافة بعيدة كمراقبة تغير لون البشرة. كما تم إثبات أن التوصل إلى إشارة ECG من قبل المهاجم بالاعتماد على السلاسل العشوائية الناتجة هي عملية غير مجدية.

أما بما يتعلق بالآفاق المستقبلية فنسعى إلى دراسة أقصى طول للسلاسل المولدة يمكن التوصل إليه بما يضمن العشوائية المطلوبة. كما نسعى إلى تطوير المولد المقترح لاستخدامه كآلية مصادقة أو كطريقة لتبادل المفاتيح من خلال توليد سلاسل عشوائية متطابقة في حساسين مختلفين موضوعين على نفس الجسم بشكل متزامن.

المراجع:

[1] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). **Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications.** Egyptian Informatics Journal, 18(2), 113-122.

[2] Masdari, M., Ahmadzadeh, S., & Bidaki, M. (2017). **Key management in wireless Body Area Network: Challenges and issues.** Journal of Network and Computer Applications, 91, 36-51.

[3] Negra, R., Jemili, I., & Belghith, A. (2016). **Wireless body area networks: Applications and technologies.** Procedia Computer Science, 83, 1274-1281.

[4] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. S. (2009). PSKA: **Usable and secure key agreement scheme for body area networks.** IEEE Transactions on Information Technology in Biomedicine, 14(1), 60-68.

[5] Zhao, H., Chen, C., Hu, J., & Qin, J. (2015). **Securing body sensor networks with biometric methods: A new key negotiation method and a key sampling method for linear interpolation encryption.** International Journal of Distributed Sensor Networks, 11(8), 764919.

[6] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). **A statistical test suite for random and pseudorandom number generators for cryptographic applications**. Booz-allen and hamilton inc mclean va.

[7] 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 Transactions on Biomedical Engineering, 65(12), 2751-2759.

[8] 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, 18(9), 2747.

[9] Xu, F., Qin, Z., Tan, C. C., Wang, B., & Li, Q. (2011, April). **IMDGuard: Securing implantable medical devices with the external wearable guardian**. In 2011 Proceedings IEEE INFOCOM (pp. 1862-1870). IEEE.

[10] Walker, John. **ENT – A Pseudorandom Number Sequence Test.** Fourmilab. 15/Jan/2021.https://www.fourmilab.ch/random/

[11] Brown, Robert G. **Dieharder: A Random Number Test Suite.** Duke Trinity College of Arts and Sciences. 15/Jan/2021.
https://webhome.phy.duke.edu/~rgb/General/dieharder.php#:~:text=Dieharder%20is%20a%20random%20number,random%20process%2C%20it%20might%20be

[12] 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**

[13] **sensor networks.** Sensors, 19(9), 2033.

Received	**2021/6/20**	**إيداع البحث**
.Accepted for Publ	**2021/11/7**	**قبول البحث للنشر**