



الجمهورية العربية السورية
جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تطوير خوارزميات لحماية المعلومات المحصّلة باستخدام شبكات الحساسات الطبية اللاسلكية في أنظمة التطبيب عن بعد

أطروحة مقدّمة لنيل درجة الدكتوراه في هندسة الحواسيب وشبكات

إعداد

م. كريستين يوسف زينية

إشراف

المشرف المشارك

د.م. مفيد حداد

المشرف الرئيس

د.م. محمد مازن المحاييري

2022

الجمهورية العربية السورية
جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تطوير خوارزميات لحماية المعلومات المحصلة باستخدام شبكات الحساسات

الطبية اللاسلكية في أنظمة التطبيب عن بعد

أطروحة مقدمة لنيل درجة الدكتوراه في هندسة الحواسيب والأتمتة

اختصاص هندسة الحواسيب وشبكاتها

إعداد الطالبة: م. كريستين يوسف زينية

لجنة الحكم:

د. محمد فراس الحناوي	الأستاذ في قسم الهندسة الطبية، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق	عضواً
د. محمد مازن المحاييري	الأستاذ المساعد في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق	عضواً مشرفاً
د. أميمة الحكواتي الدكاك	مدير بحوث، ورئيس قسم الاتصالات في المعهد العالي للعلوم التطبيقية والتكنولوجيا	عضواً
د. وسيم السمارة	الأستاذ المساعد في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق	عضواً
د. رافة خازم	المدرس في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق	عضواً

قرار مجلس البحث العلمي والدراسات العليا رقم /٢٤٤٤/ المتخذ

بالجلسة رقم /١٤/ تاريخ ٢٠٢٢/٤/١٨

اطلع مجلس البحث العلمي والدراسات العليا على قرار مجلس كلية الهندسة الميكانيكية والكهربائية

رقم /١٣٤٤/ تاريخ ٢٠٢٢/٤/٣

وبعد الرجوع إلى اللائحة التنفيذية لقانون تنظيم الجامعات الصادرة بالمرسوم /٢٥٠/ لعام ٢٠٠٦ .

قررو مجلس جامعة دمشق رقم /٢٤١٧/ص.م تاريخ ٢٠١٧/٧/٤ بشأن الموافقة على تسجيل رسالة الطالب

يستفيد الطالب من المرسوم رقم /٦٩/ تاريخ ٢٠١٩/٢/٢٣ ويمنح سنة إضافية اعتباراً من ٢٠٢١/٧/٤ لغاية

٢٠٢٢/٧/٤

يستفيد الطالب من المرسوم رقم /١٢٥/ تاريخ ٢٠٢٠/٥/٢٨ ويمنح سنة إضافية اعتباراً من ٢٠٢٢/٧/٤ لغاية

٢٠٢٣/٧/٤

وبتيجة المذاكرة قرر مجلس البحث العلمي والدراسات العليا :

الموافقة على تكليف لجنة الحكم على رسالة الدكتوراه في قسم هندسة الحواسيب والأتمتة التي أعدها الطالب

كويستين زينية بعنوان : ((تطوير خوارزميات لحماية المعلومات المحصلة باستخدام شبكات الحساسات الطبية

اللاسلكية في أنظمة التطبيق عن بعد)) بكلية الهندسة الميكانيكية والكهربائية من السادة الأساتذة :

د محمد فراس الحناوي الأستاذ في قسم الهندسة الطبية كلية الهندسة الميكانيكية والكهربائية

جامعة دمشق الاختصاص: تجهيزات طبية بصرية عضواً

د محمد مازن الحايري الأستاذ المساعد في قسم هندسة الحواسيب والأتمتة كلية الهندسة الميكانيكية والكهربائية

جامعة دمشق الاختصاص: هندسة تنظيم الحاسبات وبنيتها عضواً مشرفاً

د فريفة الحكواتي الدكاك مدير بحوث ورئيس قسم الاتصالات في المعهد عضواً

العالي للعلوم التطبيقية والتكنولوجيا

الاختصاص: نظم الكترونية

د وسيم السمارة الأستاذ المساعد في قسم هندسة الحواسيب والأتمتة كلية الهندسة الميكانيكية والكهربائية

جامعة دمشق الاختصاص: شبكات ووحدات الاتصال وتوزيع المعلومات عضواً

د رافة عازم المدرس في قسم هندسة الحواسيب والأتمتة كلية الهندسة الميكانيكية والكهربائية

جامعة دمشق الاختصاص: هندسة القيادة والقياس عن بعد (نظم تشغيل) عضواً

وذلك وفق ما هو وارد في قرار مجلس الكلية آنف الذكر،،

ملاحظة: يرجى إرسال نسخة عن الإعلان الخاص بتحديد موعد المناقشة فور صدوره إلى مكتب نائب رئيس

الجامعة لشؤون البحث العلمي والدراسات العليا.

الإهداء

إلى المحبة المطلقة . . .

ربي وإلهي

إلى اليد التي سندتني لأخطو خطواتي الأولى ودفعتني لأركض في درب النجاح، إلى من أمضى

حياته بالعمل والكد ليقدّم لي السعادة هدية . . .

أبي الحبيب

إلى الحب الصادق، سيدة المعلمات، إلى ملجئي الأمن، إلى من هي أقرب من ذاتي إلى . . .

أمي الحبيبة

إلى القلب الطيب والسند القوي، إلى من كان حاضراً في كل حين لمساعدتي في جميع مراحل حياتي . . .

أخي الغالي

إلى رمز الحنان، إلى من أشعر بوجودها قربي في كل لحظة رغم المسافات الفاصلة بيننا . . .

أختي الغالية

إلى من حملوا همومي وشاركوني أفراحي منذ نعومة أظفاري . . .

أقربائي

إلى من كانوا لي القدوة والمثل الأعلى، إلى من غرسوا في قلبي شغف العلم، إلى من قدموا لي الدعم

والنصح والتشجيع . . .

أساتذتي الكرام

إلى من قضيت معهم أجمل اللحظات وشاركوني أصعب الأوقات إلى من عرفت معهم معنى المحبة

الصادقة . . .

أصدقائي

إلى إخوتي الذين عشت معهم الفرح والمحبة والعطاء . . .

أصدقاء جان أتيد

إلى عائلتي الكبيرة . . .

الفوكولاري، عمل مريم

إلى كل من التقيت به خلال مسيرة حياتي وترك في أثر . . .

إليكم أهدي هذا العمل . . .

شكر وتقدير

أود أن أتقدم بجزيل الشكر والتقدير للأستاذين الفاضلين:

د.م. محمد مازن المحاييري ود.م. مفيد حداد

وذلك لما قدماه من جهدٍ في إتمام هذا العمل، ولعدم توانيهما عن تقديم النصيحة والمشورة بكل صدق.

كما أود أن أتوجه بالشكر والامتنان لأعضاء لجنة الحكم:

د. محمد فراس الحناوي

د. أميمة الحكواتي الدكاك

د. وسيم السمارة

د. رافة خازم

على ملاحظاتهم القيمة وتقديرهم البناء الذي ساهم في رفع سوية هذا العمل.

فهرس المحتويات

6	فهرس المحتويات
10	قائمة الجداول
11	قائمة الأشكال والرسوم البيانية
12	قائمة الاختصارات والمصطلحات العلمية
18	الملخص
	التمهيد
20	أ- مقَمة
23	ب- الإشكالية البحثية
24	ت- هدف البحث
24	ث- مبررات البحث
25	ج- أهمية البحث
26	ح- لمحة حول الدراسات السابقة
26	خ- التساؤلات
27	د- الفرضيات
27	ذ- المسلمات
27	ر- حدود البحث
27	ز- مناهج البحث وأدواته
28	س- مكونات البحث
	الفصل الأول:
	الدراسة النظرية (القسم الأول)
	المفاهيم الأساسية حول شبكات الجسم اللاسلكية WBAN وحمايتها
30	1-1- تمهيد
30	2-1- شبكة الجسم اللاسلكية
30	1-2-1. عقد شبكة الجسم اللاسلكية
32	2-2-1. طوبولوجيا شبكة الجسم اللاسلكية
33	3-1- أنظمة العناية الصحية الإلكترونية المعتمدة على WBAN
33	1-3-1. طبقات نظام العناية الصحية الإلكتروني المعتمد على WBAN
34	2-3-1. مستويات الاتصال في نظام العناية الصحية الإلكتروني المعتمد على WBAN
37	4-1- حماية شبكات WBAN
37	1-4-1. أهمية حماية شبكات WBAN
37	2-4-1. التهديدات الأمنية لشبكة WBAN
39	3-4-1. متطلبات الأمان في شبكات WBAN
41	4-4-1. تحديات الأمان في شبكات WBAN
42	5-4-1. التقانات المستخدمة في WBAN وأساليب الحماية فيها

43	1. بلوتوث (Bluetooth) 5-4-1
44	2. بلوتوث منخفض الطاقة (Bluetooth Low Energy BLE) 5-4-1
45	3. معيار IEEE 802.15.4 وتقانة Zigbee 5-4-1
46	4. معيار IEEE 802.15.6 5-4-1
48	5-1 حماية شبكات WBAN بالاعتماد على القيم الحيوية
50	1-5-1 1. إشارة التخطيط الكهربائي للقلب
50	1-5-1 1. خصائص إشارة ECG
52	1-5-1 2. تحصيل إشارة ECG
55	6-1 خاتمة

الفصل الثاني:

الدراسة النظرية (القسم الثاني)

المفاهيم الأساسية حول التعمية وتبادل المفاتيح وتوليد السلاسل العشوائية

57	1-2 تمهيد
57	2-2 التعمية
57	1-2-2 التعمية المتناظرة
59	1-2-2 1. خوارزمية التعمية متناهية الصغر
61	2-2-2 التعمية غير المتناظرة
63	3-2 المصادقة
63	4-2 تبادل المفاتيح السرية
64	1-4-2 تبادل المفاتيح المصادق عليها
64	5-2 الأرقام العشوائية
65	1-5-2 تعريف العشوائية والسلسلة الثنائية العشوائية
65	2-5-2 أنواع مولّدات الأرقام العشوائية
65	2-5-2 1. مولّدات الأرقام العشوائية
66	2-5-2 2. مولّدات الأرقام شبه العشوائية
67	3-5-2 اختبارات العشوائية
70	3-5-2 1. مجموعة اختبارات NIST الإحصائية
73	3-5-2 2. برنامج اختبار سلاسل الأرقام شبه العشوائية ENT
74	3-5-2 3. مجموعة اختبار Diehard
74	6-2 خاتمة

الفصل الثالث:

الدراسة المرجعية

76	1-3 تمهيد
76	2-3 الدراسات السابقة حول توليد المفاتيح في WBAN بالاعتماد على القيم الحيوية
86	3-3 تحليل نتائج الدراسات السابقة في توليد المفاتيح الحيوية ومناقشتها
86	3-3-1 مقارنة بين مخططات تبادل المفاتيح المعتمدة على ECG الواردة في الدراسات السابقة
87	3-3-2 الشروط الواجب توافرها في خوارزمية تبادل المفاتيح المعتمدة على ECG

- 3-3-3. عدم الكفاية في الدراسات السابقة حول توليد المفاتيح وتبادلها بالاعتماد على ECG 88
- 3-4-4. الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على القيم الحيوية 90
- 3-5-5. تحليل الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على القيم الحيوية ومناقشتها 92
- 3-5-1. مقارنة بين الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على ECG 93
- 3-5-2. عدم الكفاية في الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على ECG 94
- 3-6-6. الدراسات السابقة حول تعمية البيانات في شبكات WBAN 94
- 3-7-7. تحليل الدراسات السابقة في تعمية البيانات في WBAN ومناقشتها 97
- 3-8-8. خاتمة 97

الفصل الرابع:

تطوير وتصميم نموذج لتوليد وتبادل المفاتيح السرية المصادق عليها بين حساسات WBAN بالاعتماد على إشارة ECG

- 4-1-1. تمهيد 100
- 4-2-2. البنية المعتمدة لشبكة نظام العناية الصحية الإلكترونية 100
- 4-3-3. أهداف تطوير نموذج جديد لتبادل المفاتيح السرية المصادق عليها في WBAN بالاعتماد على إشارة ECG 101
- 4-4-4. المبادئ والمفاهيم العامة لمخطط ECG-AKES 102
- 4-5-5. تطوير مخطط ECG-AKES وفق المبادئ والمفاهيم المقترحة 104
- 4-6-6. النتائج والمناقشة حول مخطط ECG-AKES المطور 126
- 4-6-1. نتائج التطبيق العملي لمخطط ECG-AKES وتحديد العتبات المثلى 126
- 4-6-2. أمان مخطط ECG-AKES 133
- 4-6-3. أداء مخطط ECG-AKES 135
- 4-6-4. ميزات مخطط ECG-AKES 136
- 4-7-7. خاتمة 138

الفصل الخامس:

تطوير وتصميم نموذج مولد سلاسل عشوائية عالي الإنتاجية مُعتمد على الإشارة الحيوية ECG

- 5-1-1. تمهيد 140
- 5-2-2. أهداف تطوير مولد السلاسل العشوائية المطلوب المُعتمد على إشارة ECG 140
- 5-3-3. المبادئ العامة لمولد السلاسل العشوائية المطور المُعتمد على إشارة ECG 141
- 5-4-4. مخطط مولد السلاسل العشوائية المطور المُعتمد على إشارة ECG 142
- 5-5-5. النتائج والمناقشة حول مولد السلاسل العشوائية المطور المُعتمد على إشارة ECG 146
- 5-5-1. أمان المولد المطور ضد فضح إشارة ECG 147
- 5-5-2. اختبار العشوائية والتميز 149
- 5-5-2. 1. اختبار العشوائية 150
- 5-5-2. 2. تحليل التميز 154
- 5-5-3. أداء مولد السلاسل العشوائية المطور ومعدل إنتاجه 158
- 5-6-6. خاتمة 158

الفصل السادس:

تحسين خوارزمية التعمية TEA بالاعتماد على إشارة ECG

- 6-1-1. تمهيد 161

161	2-6- أهداف تطوير خوارزمية تعمية مُعتمدة على إشارة ECG لتعمية بيانات WBAN
161	3-6- المبادئ العامة لخوارزمية TEA المُحسنة المعتمدة على ECG
162	4-6- مخطط خوارزمية TEA المحسنة
167	5-6- النتائج والمناقشة حول TEA المُحسنة
167	1-5-6- أمان خوارزمية TEA المُحسنة
169	2-5-6- أداء خوارزمية TEA المُحسنة
171	6-6- خاتمة

الفصل السابع: المساهمة العلمية والمناقشة

173	1-7- تمهيد
173	2-7- مقارنة بين مخطط ECG-AKES المطور والدراسات السابقة
177	3-7- مقارنة بين مخطط توليد السلاسل العشوائية المطور والدراسات السابقة
179	4-7- مقارنة بين خوارزمية TEA المُحسنة والدراسات السابقة
180	5-7- الحداثة والمساهمة التي توصل إليها البحث
183	6-7- مقارنة بين المخططات المطورة وأساليب الحماية في تقانات الاتصال في WBAN
184	7-7- خاتمة
185	الخاتمة
188	قائمة المراجع

قائمة الجداول

الجدول 1-1: التفانان المستخدمة في WBAN وخوارزميات الحماية المستخدمة فيها.	42
الجدول 1-2: القياسات الحيوية والخصائص الواجب توافرها لاستخدامها في حماية بيانات WBAN.	49
الجدول 1-2: الربط بين الحالة الحقيقية للعشوائية مع النتائج المستخلصة من الاختبار.	68
الجدول 1-3: مقارنة بين مخططات تبادل المفاتيح المعتمدة على ECG.	87
الجدول 2-3: المتطلبات الواجب تحقيقها في مخطط تبادل المفاتيح المعتمد على القيم الحيوية، ومدى مراعاة تلك المتطلبات في الدراسات السابقة.	89
الجدول 3-3: مقارنة بين مخططات توليد القيم العشوائية بالاعتماد على إشارة ECG.	93
الجدول 1-4: الرموز المستخدمة في مخطط تبادل المفاتيح المصادق عليها بالاعتماد على ECG (ECG-AKES) ودلائلها.	104
الجدول 1-5: قائمة بالرموز المستخدمة في مخطط مولد السلاسل العشوائية المطور المعتمد على إشارة ECG، ودلائلها.	142
الجدول 2-5: نتائج اختبارات NIST للسلاسل العشوائية ذات الأطوال المختلفة التي وُلدت من إشارة ECG المحصلة في ثانية واحدة من أشخاص أصحاء ومن مرضى عدم انتظام ضربات القلب.	152
الجدول 3-5: نتائج اختبارات NIST للسلاسل العشوائية ذات الأطوال المختلفة التي وُلدت من إشارة ECG المحصلة في ثانيتين من أشخاص أصحاء ومن مرضى عدم انتظام ضربات القلب.	153
الجدول 4-5: نتائج اختبارات NIST للسلاسل العشوائية ذات الأطوال المختلفة التي وُلدت من إشارة ECG المحصلة في أربع ثوانٍ من أشخاص أصحاء ومن مرضى عدم انتظام ضربات القلب.	153
الجدول 5-5: وسطي مسافة هامينغ HD بين السلاسل العشوائية المولدة باستخدام المولد المطور.	156
الجدول 1-6: قائمة بالرموز المستخدمة في خوارزمية TEA المحسنة، ودلائلها.	162
الجدول 1-7: مقارنة بين مخطط ECG-AKES المطور والدراسات السابقة.	176
الجدول 2-7: معدل إنتاج مولد السلاسل العشوائية المطور مقارنةً بمعدلات إنتاج المولدات المقترحة في الدراسات السابقة.	177
الجدول 3-7: مقارنة بين مولد السلاسل العشوائية المطور والدراسات السابقة.	179
الجدول 4-7: ملحق الجدول 2-3، المتطلبات الواجب تحقيقها في مخطط تبادل المفاتيح المعتمد على القيم الحيوية، ومدى تلبية تلك المتطلبات في مخطط ECG-AKES.	180

قائمة الأشكال والرسوم البيانية

- الشكل 1-1: طوبولوجيا WBAN. 32
- الشكل 2-1: طبقات نظام العناية الصحية الإلكتروني المعتمد على WBAN. 33
- الشكل 3-1: مستويات الاتصال في نظام العناية الصحية الإلكترونية المعتمد على WBAN. 35
- الشكل 4-1: إشارة ECG. 51
- الشكل 5-1: إشارة ECG مسجلة بشكل متزامن في ثلاثة أقطاب (حساسات) مختلفة موضوعة على الجسم نفسه. 51
- الشكل 6-1: نظام تحصيل إشارة ECG مكوّن من ثلاثة مسارٍ. 53
- الشكل 1-2: نموذج مبسط حول التعمية المتناظرة. 58
- الشكل 2-2: جولة واحدة من جولات خوارزمية التعمية TEA. 59
- الشكل 3-2: التعمية غير المتناظرة. 62
- الشكل 1-4: البنية المعتمدة لشبكة نظام العناية الصحية الإلكترونية. 100
- الشكل 2-4: مخطط تبادل المفاتيح المصادق عليها بالاعتماد على ECG (ECG-AKES). 108
- الشكل 3-4: إشارة ECG المحصلة في كل من الحساسين A و B بشكل متزامن خلال 1.4 ثانية بمعدل اعتيان يساوي 360 عينة في الثانية. 109
- الشكل 4-4: تحويل فوربييه السريع لـ 1024 عينة من إشارة ECG المُحصّلة بشكل متزامن في كل من الحساسين A و B. 110
- الشكل 5-4: تسلسل عمل الخطوتين الأولى والثانية من المرحلة الثالثة في ECG-AKES. 113
- الشكل 6-4: عناصر X_A في نهاية الخطوة الأولى من المرحلة الثالثة بحسب مثالنا. 113
- الشكل 7-4: توليد المفتاح k في الدورة الأولى لتنفيذ مخطط ECG-AKES. 115
- الشكل 8-4: مثال حول تشكيل المصفوفة r في الدورتين الأولى والثانية للتنفيذ. 117
- الشكل 9-4: مثال حول تشكيل المصفوفة r اعتباراً من KEY_{i-2} . 117
- الشكل 10-4: دورات تنفيذ ECG-AKES والعلاقة بينها. 119
- الشكل 11-4: تسلسل عمل الخطوة الأولى من المرحلة الرابعة في ECG-AKES. 120
- الشكل 12-4: تشكيل المجموعة S_B بعد عملية إعادة ترتيب X_A في المرحلة الرابعة بحسب مثالنا. 121
- الشكل 13-4: تسلسل عمل الخطوتين الثانية والثالثة من المرحلة الرابعة في ECG-AKES. 122
- الشكل 14-4: عناصر X_B في نهاية الخطوة الثانية من المرحلة الرابعة بحسب مثالنا. 123
- الشكل 15-4: تسلسل عمل المرحلة الخامسة في ECG-AKES. 124
- الشكل 16-4: تشكيل المجموعة S_A بعد عملية إعادة ترتيب X_B في المرحلة الخامسة بحسب مثالنا. 125
- الشكل 17-4: النسبة المئوية لعدد عناصر S المؤدّة في حساسين مختلفين. 129
- الشكل 18-4: معدل القبول الخاطئ FAR ومعدل الرفض الخاطئ FRR في مخطط ECG-AKES. 131
- الشكل 19-4: تسامح مخطط ECG-AKES مع ضعف التزامن بين حساسين موضوعين على الجسم نفسه. 132
- الشكل 1-5: مخطط مولّد السلاسل العشوائية المطوّر المعتمد على إشارة ECG. 143
- الشكل 2-5: رسم بياني توضيحي لإنترولوجيا السلاسل العشوائية الناتجة عن المولد المطور. 150
- الشكل 3-5: تدرّج مسافة هامينغ للسلاسل RS128 من أجل البيانات المحصّلة في ثانية واحدة. 155
- الشكل 4-5: الترابط بين RS32 المؤدّة من إشارة ECG لشخصين مختلفين. 157
- الشكل 1-6: تشكيل المصفوفة rx والتابع Prx اعتباراً من r خلال مرحلة التهيئة في خوارزمية TEA المحسّنة. 164
- الشكل 2-6: عملية التعمية وفق خوارزمية TEA المحسّنة. 165
- الشكل 3-6: مصفوفة التشابه بين عشرين مصفوفة Sx ناتجة عن إشارة ECG للشخص نفسه من أجل أزمنة بدء تحصيل مختلفة. 168
- الشكل 4-6: زمن تنفيذ عملية التعمية وعملية فك التعمية باستخدام خوارزمية TEA المحسّنة. 169
- الشكل 5-6: مقارنة بين زمن تنفيذ خوارزمية TEA المحسّنة وزمن تنفيذ AES. 170

قائمة الاختصارات والمصطلحات العلمية

Access Point (AP)	نقطة الوصول
Actuator	المشغل الميكانيكي
Ad-hoc networks	الشبكات النقلة المخصصة
Advanced Encryption Standard (AES)	معيار التعمية المتقدم
Advanced Encryption Standard in CCM mode (AES-CCM)	معيار التعمية المتقدم وفق نمط العداد مع رمز مصادقة الرسائل وفق نمط ربط الكتل المُعمَّاة
Advanced Encryption Standard in Counter Mode (AES-CTR)	معيار التعمية المتقدم وفق نمط العداد
Alternative hypothesis (H_a)	الفرضية البديلة
Approximate Entropy Test	اختبار الإنتروبية التقريبية
Array	مصفوفة
Arrhythmia	عدم انتظام ضربات القلب
Asymmetric Encryption	التعمية غير المتناظرة
Authenticated Key Exchange (AKE)	تبادل المفاتيح المصادق عليها
Authorization	التحويل، منح الصلاحية
Big O Notation	تدوين O الكُبرى
Binary Matrix Rank Test	اختبار رتبة المصفوفة الثنائية
Biometric key	المفتاح الحيوي (البيومترى)
Biometrics	القيم الحيوية
Block Cipher	التعمية الكتلية
Bluetooth Low Energy (BLE)	بلوتوث منخفض الطاقة
Body Surface Node	عقدة سطح الجسم
Brute force attack	هجوم القوى العمياء (البحث الشامل)
Camouflage Adversary Attack	هجوم تمويه الخصم
Cipher Block Chaining Message Authentication Code (CBC-MAC)	رمز مصادقة الرسائل وفق نمط ربط الكتل المُعمَّاة
Cipher-based Message Authentication Code (CMAC)	رمز مصادقة الرسائل المُعتمد على التعمية
Collision	التصادم
Coordination Network (CN)	شبكة التنسيق
Coordinator	المنسق

Counter mode with CBC-MAC (CCM)	التعمية وفق نمط العداد مع رمز مصادقة الرسائل وفق نمط ربط الكُتل المُعمَّاة
Critical value	القيمة الحرجة
Cryptography	تعمية
Cumulative Sums Test	اختبار المجاميع التراكمية
Cyphertext	النص المُعمَّى
Data Access (DA)	النفوذ إلى البيانات
Data Authentication	مصادقة البيانات
Data Confidentiality	سرية البيانات
Data Encryption Standard (DES)	معيّار تعمية البيانات
Data Exposure	فضح البيانات
Data Freshness	حدّثة البيانات
Data Integrity	تكامل البيانات
Data origin authentication	مصادقة مصدر البيانات
Data tampering and modification	العبث بالبيانات وتعديلها
Decryption Algorithm	خوارزمية فك التعمية
Denial of Service Attack	هجوم منع الخدمة
Dependability	الجدارة
Differential cryptanalysis	تحليل التعمية التفاضلي
Digital Signature	التوقيع الرقمي
Discrete cosine transformation	تحويل التجيب المنقطع
Discrete Fourier Transform Test	اختبار تحويل فورييه المنقطع
Disjoint sub-matrices	المصفوفات الجزئية المنفصلة
Distinctiveness	التمييز
ECG-based Authenticated Key Exchange Scheme (ECG-AKES)	مخطط تبادل المفاتيح المصادق عليها بالاعتماد على التخطيط الكهربائي للقلب
Efficiency	فعالية
E-Healthcare System	أنظمة العناية الصحية الإلكترونية
Electrocardiogram (ECG)	التخطيط الكهربائي للقلب
Electroencephalogram (EEG)	التخطيط الكهربائي للدماغ

Elliptic Curve Cryptography (ECC)	تعمية المنحنى الاهليجي (القطعي)
Encryption	التعمية
Encryption Algorithm	خوارزمية التعمية
End Node	العقدة الطرفية
Extended Star Topology	الطوبولوجيا النجمية الموسعة
External Node	عقدة خارجية
False Acceptance Rate (FAR)	معدل القبول الخاطئ
False Rejection Rate (FRR)	معدل الرفض الخاطئ
Fast Furrier Transform (FFT)	تحويل فورييه السريع
Flexibility	المرونة
Flooding	إغراق، فيض
Frame	إطار
Frequency Test	اختبار التردد
Frequency Test within a Block	اختبار التردد ضمن الكتلة
Fuzzy Vault	القبو الغامض
Gateway	البوابة
General Packet Radio Service (GPRS)	خدمة الحزمة الراديوية العامة
Group Temporal Key (GTK)	مفتاح المجموعة المؤقت
Hamming Distance (HD)	مسافة هامينغ
Handshake	المصافحة
Hash function	تابع البصمة (التهشير)
Heart Rate Variability (HRV)	تغير معدل ضربات القلب
Hub	الموزع
Human Body Communication (HBC)	الاتصال ضمن نطاق جسم الإنسان
Implant Node	عقدة الزرع
Infrastructure based networks	الشبكات المعتمدة على البنية التحتية
Inter Pulse Interval (IPI)	الفاصل الزمني بين نبضتين متتاليتين
Jamming	التشويش
Key Exchange	تبادل المفاتيح
Latency	زمن الاستجابة

Level of significance	مستوى الدلالة (الأهمية)
Linear Complexity Test	اختبار التعقيد الخطي
Linear Feedback Shift Register (LFSR)	سجل إزاحة ذو تغذية خلفية خطية
Long-term Key (LTK)	مفتاح طويل الأمد
Low-Rate Wireless Personal Area Network (LR-WPAN)	شبكة المنطقة الشخصية اللاسلكية منخفضة معدل البيانات
Man-in-the-middle Attack	هجوم الرجل في الوسط
Master Key (MK)	مفتاح رئيس
Media Access Control layer (MAC)	طبقة التحكم بالوصول إلى الوسائط
Medical Implant Communication Service (MISC)	خدمة الاتصال للزرعات الطبية
Medical Server (MS)	المخدّم الطبي
Message Authentication Code (MAC)	رمز مصادقة الرسائل
Monitor and Eavesdropping	المراقبة والتنصت
Multicast	الاتصال متعدد الوجهات
Multipoint Fuzzy Key Management	الإدارة العائمة للمفتاح متعددة النقاط
Narrowband (NB)	النطاق الضيق (الحزمة الضيقة)
National Institute of Standards and Technology (NIST)	المعهد الوطني للمعايير والتكنولوجيا
Near Field Communication (NFC)	الاتصال في المجال القريب
Network Availability	متاحية الشبكة
Node Replication Attack	هجوم نسخ العقدة
Nominal Data Rate	معدل البيانات الاسمي
Non-overlapping Template Matching Test	اختبار مطابقة القوالب غير المتداخلة
Null hypothesis (H_0)	فرضية العدم
Overlapping Template Matching Test	اختبار مطابقة القوالب المتداخلة
Pairing devices	إقران الأجهزة
Pairwise Temporal Key (PTK)	المفتاح المؤقت المتبادل
Pattern	نمط
Peak	قمة
Peak Index	مؤشر القمة
Peer entity authentication	مصادقة الكيان النظير (النَد)

Permutation	تبديل المواضع
Permutation function	تابع تبديل المواضع
Personal Digital Assistant (PDA)	المساعد الرقمي الشخصي
Personal Server (PS)	المخدّم الشخصي
Physical Attacks	الهجمات الفيزيائية
Physiological-Signal-based Key Agreement (PSKA)	الاتفاق على المفتاح المُعتمد على الإشارة الحيوية
Plaintext	النص الصريح
Plug and play manner	طريقة التوصيل والتشغيل
Private key	المفتاح الخاص
Pseudo Random Number Generators (PRNG)	مولّد الأرقام شبه العشوائية
Pseudocode	شبه الرّماز
Public key	المفتاح العام
Public-key Encryption	التعمية بالمفتاح العام
Radio Frequency (RF)	التردد الراديوي
Random Binary Sequence (RBS)	السلسلة الثنائية العشوائية
Random Excursions Test	اختبار انحرافات العشوائية
Random Excursions Variant Test	اختبار متغير انحرافات العشوائية
Random Number Generator (RNG)	مولّد الأرقام العشوائية
Randomness Statistics	إحصاءات العشوائية
Real time	الزمن الحقيقي
Related-key attack	هجوم المفاتيح المرتبطة
Relay	المبدل
Runs Test	اختبار سلاسل البتات المتماثلة المتتالية
Sampling rate	معدل أخذ العينات
Secret Key	المفتاح السري
Secret Key Encryption	التعمية بالمفتاح السري
Secure Management	الإدارة الآمنة
Secure Simple Pairing (SSP)	الاقتران البسيط الآمن
Seed	البذرة
Sensors Network (SN)	شبكة الحساسات

Serial Test	الاختبار التسلسلي
Short-term Key (STK)	مفتاح قصير الأمد
Similarity Matrix	مصفوفة التشابه
Single-point Fuzzy Key Management	الإدارة العائمة للمفتاح أحادية النقطة
Sink node	عقدة المجرى (المصرف)
Star topology	الطوبولوجيا النجمية
Stream Cipher	التعمية الدفقية
Substitution	الاستبدال
Sybil Attack	هجوم سيبيل
Symmetric Encryption	التعمية المتناظرة
Synchronization	التزامن
Telemedicine System	نظام التطبيب عن بُعد
Temporal variance	التباين الزمني
Test for the Longest Run of Ones in a Block	اختبار أطول سلسلة واحدات متتالية ضمن الكتلة
Throughput	الإنتاجية
Throughput rate	معدل الإنتاج
Time complexity	التعقيد الزمني
Tiny Encryption Algorithm (TEA)	خوارزمية التعمية متناهية الصغر
Traffic Analysis Attack	هجوم تحليل حركة المرور
Trust center	مركز ثقة
Ultra-Wideband (UWB)	النطاق العريض للغاية (الحزمة الواسعة جداً)
Unauthorized Access	الوصول غير المرخص
Unicast	الاتصال أحادي الوجهة
Universal Statistical Test	اختبار الإحصاء العام
Unlicensed Industrial, Scientific, and Medical radio band (ISM)	حزمة الترددات الراديوية من دون ترخيص للتطبيقات الصناعية والعلمية والطبية
Wavelet Distribution	التحليل المويجي
Wireless Body Area Network (WBAN)	شبكة الجسم اللاسلكية
Wireless Medical Telemetry Services (WMTS)	خدمات القياس الطبي اللاسلكي عن بعد
Wireless Sensors Network (WSN)	شبكة الحساسات اللاسلكية

الملخص

أنظمة التطبيب عن بُعد (Telemedicine Systems)، أو ما يطلق عليها أيضاً أنظمة العناية الصحية الإلكترونية (E-healthcare Systems)، هي أنظمة تُراقب الحالة الصحية للمريض في أي زمان وأي مكان من دون تقييد حركته، ونشاطاته اليومية. لتحقيق ذلك، تُستخدم شبكات الجسم اللاسلكية (Wireless Body Area Networks WBANs)، وهي مجموعة من الحساسات الطبية المتصلة مع بعضها لاسلكياً، مصممة لتحصيل القياسات الحيوية المختلفة لجسم الإنسان وتبادلها. يُعدُّ الحفاظ على أمان المعلومات الصحية في هذه الأنظمة أمراً بالغ الأهمية، نظراً لما للهجمات الأمنية من تأثيرات سلبية تعرض حياة المريض للخطر. ولكن محدودية موارد حساسات WBAN لا تسمح بتطبيق آليات الحماية التقليدية؛ إذ إنها تستهلك كثيراً من الطاقة والموارد. بغية تقليل استهلاك الموارد، طور الباحثون خوارزميات التعمية، وآليات المصادقة، والموسطات اللازمة لها بالاعتماد على القيم الحيوية والتي من أبرزها إشارة التخطيط الكهربائي للقلب (Electrocardiogram ECG). ولكن تعاني مناهجهم من بعض المشاكل. فبالنسبة لتوليد مفاتيح التعمية بالاعتماد على ECG، تعاني الطرائق المطورة من التأخير الزمني، والتزامن (synchronization) الصارم المطلوب، أو من معدل قبول خاطئ (False Acceptance Rate FAR) أكبر من الصفر، وغير ذلك. كذلك الأمر بالنسبة لتوليد السلاسل العشوائية بالاعتماد على ECG، والتي تُستخدم لأغراض حماية المعلومات، فهي تعاني من الإنتاجية (Throughput) المنخفضة غير المناسبة لمتطلبات الرعاية الصحية في الزمن الحقيقي. في هذه الأطروحة نُطوّر مخططات جديدة لحماية شبكة WBAN، بالاستفادة من إشارة ECG. يمكن تلخيص الحداثة والمساهمة في هذا البحث في ثلاث مساهمات رئيسية. أولاً: تطوير وتصميم نموذج جديد

لتوليد وتبادل المفاتيح السرية المصادق عليها بين حساسات WBAN؛ وذلك بالاعتماد على الخصائص الزمنية والترددية لإشارة ECG، بحيث يتغلب على نقاط الضعف في الدراسات السابقة. كما يتميز ببساطة العمليات، وتوليد مفاتيح متغيرة مع الزمن، والتسامح مع عدم الدقة في التزامن بين الحساسات، و FAR يساوي الصفر. ثانياً: تطوير وتصميم نموذج مولد سلاسل عشوائية عالي الإنتاجية مُعتمد على إشارة ECG، يتميز ببساطة العمليات؛ وذلك انطلاقاً من الحاجة إلى توليد سلاسل عشوائية في مخطط تبادل المفاتيح المطور. ثالثاً: تحسين خوارزمية التعمية متناهية الصغر (Tiny Encryption Algorithm TEA) بالاعتماد على إشارة ECG، بطريقة ترفع من أدائها، وتجعلها آمنة ضد الهجمات التي تتعرض لها TEA التقليدية؛ وذلك بهدف استخدامها في تعمية البيانات المتبادلة في WBAN. تُستخدم TEA المحسنة القيم السرية والمفاتيح الناتجة عن مخطط تبادل المفاتيح المطور. قمنا ببناء النماذج المطورة واختبرناها عملياً ودرسنا أمان كلٍ منها وأدائه. أثبتنا أن السلاسل العشوائية الناتجة أياً كان طولها بين 128 bit و 2048 bit، مناسبة لتطبيقات حماية المعلومات، وأن معدل إنتاج (Throughput rate) تلك السلاسل أكبر بعشرات أو مئات المرات من مقابله في الدراسات السابقة. وقمنا أيضاً بالتحقق من صحة نموذج تبادل المفاتيح، وإثبات أمانه، ودراسة أدائه، ومقارنته مع النماذج المقترحة في الدراسات السابقة. كما أثبتنا أن TEA المحسنة هي أسرع بحوالي ست عشر مرة من معيار التعمية المتقدم (Advanced Encryption Standard AES) المستخدم في معيار IEEE 802.15.6 الخاص بشبكات WBAN.

الكلمات الرئيسية: شبكة الجسم اللاسلكية (WBAN)، إشارة التخطيط الكهربائي للقلب (ECG)، المفتاح الحيوي، مخطط تبادل المفاتيح السرية، السلاسل الثنائية العشوائية (RBSS)، خوارزمية التعمية متناهية الصغر (TEA).

التمهيد

أ- مقدّمة

أدى التطور التقني وخاصةً في مجال الاتصالات اللاسلكية إلى تغييرات كبيرة في حياتنا عامةً وفي طرق العناية بالصحة خاصةً. وبفضل التطور الكبير في تقانات الاتصال في الزمن الحقيقي (Real time) أصبح نقل المعلومات الحيوية أمراً ممكناً [1]. ففي الآونة الأخيرة تزايد الاهتمام في الوقاية من الأمراض، والاكتشاف المبكر للأزمات الصحية، وتقديم العناية المُثلّى للمرضى الذين يعانون من الأمراض المزمنة؛ مما أدى إلى تكثيف محاولات بناء أنظمة الرعاية الصحية الإلكترونية. وكان لتطور شبكات الحساسات اللاسلكية (Wireless sensor network) (WSN) الدور الأساسي في تصميم أنظمة التطبيب عن بُعد التي تُراقب الحالة الصحية للمريض في أي مكانٍ كان من دون تقييد حركته ونشاطاته اليومية [2].

لهذه الأنظمة أهمية كبيرة في رفع وسطي عمر الإنسان وحمايته من أخطار الموت. فهي تساعد على الكشف المبكر عن الأزمات الصحية كالأزمات القلبية، وتفيد في الكشف المبكر عن الأمراض قبل أن تصبح حرجة، وتساعد على السيطرة على النوبات، ومن ثم التخفيف من آثارها، وتؤمّن الاتصال المستمر بالمريض وإرسال معلوماته لحظياً أثناء نقله إلى المستشفى في سيارة الإسعاف [2]، [3]. بناءً على كل ما سبق، فإن استعمال هذه الأنظمة يرفع مستوى حياة الإنسان.

تُعدّ شبكة الجسم اللاسلكية WBAN جزءاً أساسياً من نظام الرعاية الصحية الإلكتروني، وهي شبكة مصمّمة بهدف جمع البيانات الصحية للأشخاص. تتألف من مجموعة من الحساسات اللاسلكية المختلفة المتصلة بعضها مع بعض، والتي يمكن وضعها على جسم الإنسان أو حوله أو داخله لقياس القيم الحيوية المختلفة، مثل: درجة حرارة الجسم، وضغط الدم، ومعدل الأكسجة، وغيرها [4]، [5]، [6]. يمكن استعمال شبكات WBAN في تطبيقات طبية متعددة. على سبيل المثال، في أنظمة الرعاية الصحية الإلكترونية، يمكن استعمال البيانات التي تُجمع من خلال حساسات WBAN لتنبيه الأطباء عند وقوع حدث ما يهدد الحياة [7]، [8]، [9].

وبما أن المعلومات الطبية هي معلومات حساسة وحرجة، يُعدُّ الحفاظ على أمانها في أثناء نقلها، وعند تخزينها، وضمان حمايتها من أخطار المتطفلين مطلباً أساسياً [10]، [11]، [12]. بناءً عليه، تُعدُّ حماية الاتصالات بين حساسات WBAN أمراً ضرورياً؛ للحفاظ على خصوصية البيانات الصحية، وضمان تقديم الرعاية الصحية بشكل سليم [13]، [14]. ومن الواضح أن التلاعب بالبيانات الحيوية يمكن أن يتسبب في وقوع حوادث طبية خطيرة؛ بل وقد يهدد حياة المريض [14].

تتصف WBAN بالمحدودية البالغة في موارد الحساسات، مثل: الذاكرة، وقدرة وحدة المعالجة المركزية، وموارد الطاقة؛ مما يجعل تطبيق مخططات أمن المعلومات في تلك الحساسات أكثر صعوبة من تطبيقها في الشبكات التقليدية الأخرى، والتي يمكن أن تستعمل آليات حماية عالية التكلفة [7]، [14]، [15]. هناك العديد من المتطلبات يجب تحقيقها من أجل حماية شبكات WBAN، ومنها: الحفاظ على سرية البيانات وسلامتها، والمصادقة، وضمان حداثة المعلومات، وغيرها [4]، [16]. لتحقيق سرية البيانات يجب أن تُعمَى قبل تبادلها بين الحساسات. هناك نوعان أساسيان من التعمية، وهما: التعمية المتناظرة، والتعمية غير المتناظرة. تتصف خوارزميات التعمية المتناظرة ببساطة العمليات، ولكنها تعاني من الحاجة إلى تبادل المفتاح السري بشكل آمن [17]. أما خوارزميات التعمية غير المتناظرة فهي لا تحتاج إلى تبادل المفاتيح بشكل سري وآمن، ولكنها تعاني من التعقيد الحسابي واستهلاكها للموارد [17]. فضلاً عن ذلك، تتميز خوارزميات التعمية المتناظرة بأداء أعلى من أداء خوارزميات التعمية غير المتناظرة؛ مما يجعلها أكثر ملاءمة لاستعمالها في تطبيقات الرعاية الصحية التي تعمل في الزمن الحقيقي، ومن ثمَّ يمكننا استنتاج أن خوارزميات التعمية المتناظرة هي الأنسب لاعتمادها في WBAN. ولكن ينتج عن اعتمادها الحاجة إلى حلِّ مشكلة أساسية ألا وهي صعوبة إنشاء المفاتيح السرية المشتركة بين عقد الحساسات وإدارتها [14]. يُعدُّ التوزيع المسبق للمفاتيح؛ أي قبل نشر الشبكة في الجسم، هو الحل الأبسط لإدارة المفاتيح السرية المتناظرة [5]، [18]. ولكن هذه الطريقة تعاني من مشكلتين أساسيتين، وهما: أولاً، الاحتفاظ بالمفاتيح قيد الاستعمال نفسها لفترات زمنية طويلة، والذي يجعلها عرضةً للفضح. ثانياً، عدم قابلية إضافة عُقد جديدة من دون إعادة تهيئة الشبكة كاملةً [19]. وللاستغناء عن التوزيع المسبق للمفاتيح، لا بدَّ من استعمال

مخططات تبادل المفاتيح الشائعة، ولكنها تعتمد على أنظمة التعمية غير المتناظرة ومن ثم هي مكلفة للغاية في سياق شبكة WBAN [20]، [21].

تستخدم العديد من مخططات إدارة المفاتيح الإشارات الحيوية في إتمام عملية توليد المفاتيح وتبادلها [18]، [19]، [22]، [23]. تأتي فكرة استخدام خصائص الإشارات الحيوية من ملاحظة أن جسم الإنسان ديناميكي ومعقد، وأن حالته الفيزيولوجية تكون فريدة في لحظة معينة [13]، ومن ثم، فإن القيم الحيوية لها خصائص عشوائية يمكن الاستفادة منها في توليد المفاتيح وتبادلها [24]، [25]، [26]، [27]. لذلك يُعدُّ توليد المفاتيح وتبادلها؛ بالاعتماد على القيم الحيوية أفضل من توليدها باستخدام مولدات الأرقام شبه العشوائية، ثم تبادلها باستخدام المخططات التقليدية لتبادل المفاتيح والتي تتطلب حسابات ثقيلة [19]. تعطي بعض الإشارات الحيوية قيماً متقاربة لدى قياسها بشكل متزامن في حساسات مختلفة تنتمي للجسم نفسه. يمكن الاستفادة من هذه القيم المتقاربة في توليد المفاتيح المتناظرة في تلك الحساسات. يوفر هذا الأسلوب إمكانية العمل وفق طريقة التوصيل والتشغيل (Plug and play manner)؛ أي إضافة أجهزة الحساسات، وإزالتها، وتعديلها في WBAN من دون الحاجة إلى إعادة تهيئة جميع الحساسات [13]. من الواضح أن توليد المفاتيح المعتمد على القياسات الحيوية يزيد من فعالية (efficiency) شبكات WBAN [28].

تُعدُّ إشارة ECG واحدة من أبرز الإشارات المرشحة لاستخدامها في بناء مخططات فاعلة وآمنة لإدارة المفاتيح الحيوية في WBAN [5]، [20]، [22]. وهي تُمثِّل التسجيل البياني للتيارات الكهربائية التي تولِّدها عضلة القلب. تتصف هذه الإشارة بالتباين الزمني؛ مما يجعلها مناسبة لحماية الاتصالات عبر WBAN [29]. فضلاً عن ذلك، ينتج عن إشارة ECG خصائص متماثلة لدى قياسها في الحساسات المختلفة بشكل متزامن [20].

في تطبيقات حماية الشبكات، يتطلب عددٌ من بروتوكولات التعمية، ومخططات تبادل المفاتيح مدخلات عشوائية في نقاط مختلفة [30]. هناك نوعان أساسيان من المولدات التي تُستعمل لإنشاء الأرقام العشوائية، وهي: مولدات الأرقام العشوائية (Random number generators RNG) ومولدات الأرقام شبه العشوائية (Pseudo-random number generators PRNG). يستغرق إنتاج الأرقام العشوائية عالية الجودة زمناً طويلاً. ولإنتاج عدد

كبير من الأرقام العشوائية، قد يكون مولّد الأرقام شبه العشوائية هو الأفضل [30]. لذلك نَسْتَعْمِلُ شبكات WBAN مولّدات الأرقام شبه العشوائية [24]، [31]. ولكن، تتطلب تلك المولّدات حسابات ثقيلة للحصول على العشوائية، ويجب اختيار بذورها بعناية وحمايتها؛ مما يؤدي بدوره إلى استهلاك الموارد [24].

في هذا السياق، يمكن استخراج السلاسل العشوائية من القيم الحيوية المقاسة في WBAN. طوّرت بعض مولّدات الأرقام العشوائية القائمة على القياسات الحيوية، لتجنب استعمال مولّدات الأرقام شبه العشوائية في حساسات WBAN؛ مما يؤدي إلى توفير الطاقة وقدرة المعالجة [25]، [26]، [32]. ركّز بعض الباحثين على إشارة ECG، فهي تملك العديد من الخصائص التي تجعل استخدامها لتوليد القيم العشوائية ممكناً [29]، [33]، [34].

مما سبق، نلاحظ أن أفضل سيناريو يمكن اعتماده لحماية شبكات WBAN هو تطبيق خوارزميات التعمية المتناظرة التي تستخدم المفاتيح الحيوية. ولكن لا يزال التوصل إلى مخطط توليد مفاتيح سرية وتبادلها بالاعتماد على القيم الحيوية مجالاً مفتوحاً للبحث ذا أهمية بالغة؛ نظراً لما تعاني منه المخططات المطورة في الدراسات السابقة من نقاط ضعف. كما أن مولّدات الأرقام العشوائية المطورة حتى يومنا هذا؛ وبالتحديد تلك المعتمدة على القيم الحيوية مثل ECG، والتي تحتاج إليها مخططات حماية WBAN، لاتزال تعاني من معدل إنتاج منخفض غير ملائم لمتطلبات تطبيقات الزمن الحقيقي. وإن السعي نحو خوارزمية تعمية آمنة، وعالية الأداء، وذات استهلاك منخفض للطاقة بحيث تراعي محدودية موارد WBAN لا يزال يشكل بحثاً مفتوحاً للدراسة.

ب - الإشكالية البحثية

في أنظمة التطبيب عن بُعد، تُعدّ حماية البيانات الطبية المتبادلة مطلباً أساسياً غاية في الأهمية [10]، [11]، [12]. تقتضي حماية بيانات تلك الأنظمة حماية البيانات المتبادلة بين حساسات WBAN [13]، [14]. ولكن تعاني حساسات WBAN من المحدودية الكبيرة في الطاقة وقدرة المعالجة [7]، [14]، [15]. وكما هو معروف تتصف خوارزميات الحماية التقليدية بالتعقيد الحسابي؛ مما يتطلب استهلاكاً كبيراً للموارد. ومن ثمّ لا يمكن تطبيقها في حساسات WBAN، فقد تكون بعض الحساسات مزروعة داخل الجسم، ويتعذر الوصول إليها بسهولة من أجل

تبدیل وحدة الطاقة الخاصة بها [28]، [35]. كما أن تطبيقات الرعاية الصحية يجب أن تعمل في الزمن الحقيقي، وخاصةً في حالات الإسعاف، مما يقتضي تنفيذ خوارزميات تتناسب مع هذا المطلب [2].

بالتالي، يواجه نظام التطبيب عن بعد تحديات عدة، ومنها، إيجاد طرق تضمن حماية المعلومات الطبية الحرجة في أثناء تبادلها بين حساسات WBAN، تتمتع بأداء عالٍ بحيث تكون مناسبة للعمل في الزمن الحقيقي، وذات عمليات بسيطة توفر من استهلاك طاقة الحساس.

ت - هدف البحث

يهدف هذا البحث إلى التوصل إلى طرائق لدعم حماية المعلومات الطبية في نظام التطبيب عن بُعد؛ مما يسمح باستمرار نقل بيانات المريض بشكل آمن في أي مكان، وفي أي وقت؛ وخاصةً في حالات الإسعاف. وبالتالي سنسعى في هذا البحث إلى تطوير خوارزميات لحماية شبكة WBAN التي تُعدّ الجزء الرئيس لنظام التطبيب عن بُعد. نستهدف بالتحديد خوارزميات التعمية، ومخططات توليد المفاتيح السرية المصادقة، وتوليد السلاسل العشوائية التي تُعدّ ركيزةً أساسيةً لحماية WBAN. نهدف إلى التوصل إلى نماذج، وطرائق تحقق الشروط الآتية:

- الأداء العالي، ومن ثمّ إمكانية تطبيقها في الزمن الحقيقي.
- بساطة العمليات الحسابية بحيث تستهلك أقل قدر ممكن من موارد الحساسات.
- أمانة ولا يمكن التعرض لها من قبل الخصوم.

ث - مبررات البحث

لا تزال أنظمة التطبيب عن بُعد حتى يومنا هذا محدودة الاستخدام؛ بسبب تحديات الأمان التي تعاني منها. حاول بعض الباحثين تطوير طرائق لحماية البيانات تتناسب مع المتطلبات الخاصة لشبكة WBAN ألا وهي محدودية الطاقة وقدرة المعالجة، والعمل في الزمن الحقيقي. استخدم بعضهم القيم الحيوية في توليد المفاتيح وتبادلها، وفي توليد السلاسل العشوائية، وفي عمليات التعمية، وذلك بهدف الحدّ من استهلاك موارد الحساس [7]، [32]، [36]. ولكن لا تزال طرائقهم تعاني من بعض نقاط الضعف. فبالنسبة لتوليد المفاتيح، تعاني الطرق المطورة من التأخير الزمني، أو التزامن الصارم المطلوب، أو من FAR غير الصفري، وغير ذلك [5]، [13]، [23]. وبالنسبة لتوليد

السلاسل العشوائية بالاعتماد على ECG، فهي تعاني من الإنتاجية المنخفضة غير المناسبة للرعاية الصحية في الزمن الحقيقي [24]، [25]، [32]. أما بالنسبة لخوارزميات التعمية فهي تعاني من التعقيد [37]، [38]. من ذلك كله يمكننا استنتاج أن إيجاد طرائق مناسبة لحماية WBAN لا يزال بحثاً مفتوحاً ذا أهمية عالية.

ج- أهمية البحث

تكمن أهمية هذا البحث في أهمية حماية البيانات الصحية في أنظمة التطبيب عن بعد. يُعدُّ الحفاظ على أمان البيانات الطبية وخصوصيتها أحد أهم التحديات. كما تُعدُّ بيانات المريض حساسة للغاية، وبالتحديد إذا كان يعاني من مرض محرج. يمكن لمثل ذلك المريض أن يتعرض للإذلال أو حتى إلى الاضطراب النفسي إذا تم الإبلاغ عن معلومات مرضه [39]. ومن جهة أخرى من الضروري حماية القرارات الطبية والمعلومات الطبية من الوصول غير المصرح به الذي قد يشكل خطراً على حياة المريض، وأحياناً يؤدي إلى الوفاة [39]. على سبيل المثال، تغيير جرعة الدواء أو إجراءات العلاج، إذا وقعت في اليد الخاطئة [4]. ومن ثمَّ فإنَّ التوصل إلى طرائق الحماية المطلوبة التي تراعي محدودية موارد الحساسات، والعمل في الزمن الحقيقي يحقق تقدماً كبيراً في مجال العناية الصحية الإلكترونية، وحماية البيانات فيها.

تكمن المساهمة التي يقدمها هذا البحث والذي يدرس حماية أنظمة العناية الصحية الإلكترونية، وبالتحديد حماية شبكات WBAN في ثلاث نقاط رئيسية:

أولاً: تطوير وتصميم نموذج جديد لتوليد وتبادل المفاتيح السرية المصادق عليها بين حساسات WBAN؛ وذلك بالاعتماد على الخصائص الزمنية والترددية لإشارة ECG، بحيث يتغلب النموذج المطور على نقاط الضعف في الدراسات السابقة. كما يتميز ببساطة العمليات، وتوليد مفتاح متغير مع الزمن، FAR يساوي الصفر، والتسامح مع ضعف التزامن بين الحساسات.

ثانياً: تطوير وتصميم نموذج مولد سلاسل عشوائية مُعتمد على إشارة ECG يتصف بإنتاجية أعلى بعشرات أو مئات المرات من المولدات المقترحة في الدراسات السابقة، ويتميز ببساطة العمليات.

ثالثاً: تحسين خوارزمية TEA، بالاعتماد على إشارة ECG؛ بهدف استخدامها في تعمية البيانات المتبادلة في WBAN. تستعمل TEA المحسنة القيم السرية، والمفاتيح الناتجة عن مخطط تبادل المفاتيح المطور. تمكّنّا في TEA المحسنة من التوصل إلى خوارزمية آمنة ضد الهجمات التي تتعرض لها TEA التقليدية، وذات أداء أعلى بست عشرة مرة من أداء خوارزمية AES.

ح- لمحة حول الدراسات السابقة

عرّضت العديد من الدراسات السابقة خوارزميات وطرائق لحماية شبكات WBAN. تعمقنا في دراسة تلك التي تعنى بالمجال الدقيق لبحثنا ألا وهو تطوير طرائق وخوارزميات لتعمية البيانات الطبية، وتوليد مفاتيح التعمية المناسبة، والسلاسل العشوائية اللازمة. اعتمد الباحثون على القيم الحيوية في خوارزمياتهم، وذلك بهدف تقليل استهلاك طاقة الحساسات، وزيادة الفعالية [7]، [32]، [36]، [40]. تُعدّ إشارة ECG من أكثر الإشارات التي لاقَت اهتمام الباحثين في هذا المجال لما لها من خصائص يمكن الاستفادة منها، ولأنّ تحصيلها يمكن أن يتم من أي موضع في الجسم [40]، [41]. استخدم بعض الباحثين قيم عينات إشارة ECG في خوارزمياتهم [22]، واستخدم بعضهم الخصائص الترددية لتلك الإشارة [5]، أما بعضهم الآخر فاستفادوا من الخصائص الزمنية لها كالفواصل الزمني بين نبضتين متتاليتين [32]. نورد في الفصل الثالث شرحاً تفصيلياً لجميع الدراسات السابقة المعتمدة في هذه الأطروحة.

خ- التساؤلات

يطرح هذا البحث عدداً من التساؤلات ألا وهي: هل يمكن إيجاد نماذج ومخططات لحماية WBAN يكون استهلاكها لموارد الحساسات أصغر ما يمكن، وتعمل في الزمن الحقيقي؟ هل يمكن لاستخدام القيم الحيوية في مخططات الحماية أن يؤدي إلى رفع أدائها، وجعل استهلاكها للموارد أصغر ما يمكن؟ ما الخصائص الحيوية التي يجب استخدامها للتوصل إلى المخططات المطلوبة؟ هل يمكننا تحقيق عملية تبادل المفاتيح من دون استخدام التعمية غير المتناظرة التي تتصف بالتعقيد؟

د - الفرضيات

في هذه الدراسة نفترض أن القيم الحيوية المُقاسة هي قيم سرّية، يجب ألا يعرفها إلا الأشخاص المخولون بذلك [13]، [23]. ونفترض أيضاً أن الحساسات متزامنة بعضها مع بعض [13]، [22].

ذ - المسلمات

تتعرض جميع شبكات الحساسات اللاسلكية، وبالتحديد شبكات WBAN إلى أنواع متعددة من الهجمات، ومنها: مراقبة البيانات، والتتصت عليها، والوصول غير المرخص لها، وفضحها، والعبث بها، وغير ذلك [4]، [16]، [17]. يتم تحقيق سرية البيانات من خلال عمليات التعمية، كما يتم التحقق من شرعية الحساسات من خلال عمليات المصادقة، والتحقق من الهوية [17]. وللقيام بعمليات التعمية لابد من تبادل المفاتيح السرية بشكل آمن [17] حيث أن فضح المفتاح أو تبادله بشكل غير آمن يؤدي إلى إبطال مفعول عملية التعمية ومن ثمّ انتهاك السرية. ومن المسلمات أيضاً أن إشارة ECG تكون متشابهة، وليست متطابقة بشكل كامل لدى قياسها بشكل متزامن في عدة حساسات موضوعة على الجسم نفسه [13]، [22]، [23].

ر - حدود البحث

تحتاج حماية WBAN إلى تحقيق متطلبات عديدة، ومنها: سرية البيانات، وتكامل البيانات، وحادثة البيانات، ومتاحية الشبكة، ومصادقة الحساسات، والإدارة الآمنة للمفاتيح، وغيرها [4]، [16]، [17]. في بحثنا هذا دُرست سرية البيانات، والإدارة الآمنة للمفاتيح، ومصادقة الحساسات، والحادثة، وطُورت المخططات اللازمة لتحقيق ذلك. أما فيما يتعلق بتكامل البيانات، ومتاحية الشبكة، وغيرها من قضايا حماية المعلومات، فلم نُعالج في هذا البحث.

ز - مناهج البحث وأدواته

بدايةً أجرينا دراسة عامة حول مفهوم حماية شبكات الحساسات اللاسلكية، وبالتحديد شبكات WBAN، وأجرينا دراسة معمقة لمخططات حماية البيانات المعتمدة على القيم الحيوية، وقارنّا فيما بينها، واستنتجنا مزايا كلّ منها ونقاط ضعفها. ثم طورنا نماذج ومخططات وصممناها لتسد ثغرات الدراسات السابقة. بنّينا تلك المخططات

وبرمجناها بلغة C واختبرناها، باستخدام إشارات ECG محصلة من حساسين متزامنين موضوعين على الجسم نفسه والتي استُرجعت من قواعد بيانات MIT-BIH [42]، [43]، [44]. ثم درسنا خصائص تلك المخططات وميزاتها وقارنا نتائج تطبيقها العملي مع النتائج الواردة في الدراسات السابقة.

س - مكونات البحث

يتكون البحث من ثلاثة محاور رئيسة وهي: تطوير وتصميم نموذج لتوليد وتبادل المفاتيح السرية المصادق عليها بين حساسات WBAN بالاعتماد على إشارة ECG، وتطوير وتصميم نموذج مولّد سلاسل عشوائية عالي الإنتاجية مُعتمد على إشارة ECG، وتحسين خوارزمية TEA بالاعتماد على إشارة ECG من أجل رفع أدائها وأمانها.

أما بما يتعلق بأقسام الأطروحة، فهي تتكون من سبعة فصول. نعرض في الفصلين الأول والثاني المفاهيم النظرية حول شبكات WBAN وحماية المعلومات فيها والمفاهيم الأساسية في التعمية وتبادل المفاتيح المصادق عليها وتوليد السلاسل العشوائية. ونعرض في الفصل الثالث الدراسات المرجعية في مجال البحث. أما الفصل الرابع فندرج فيه شرحاً تفصيلياً حول نموذج توليد وتبادل المفاتيح السرية المصادق عليها بالاعتماد على إشارة ECG المصمم والمطور في هذا البحث. وندرج في الفصل الخامس شرحاً لنموذج مولّد السلاسل العشوائية المعتمد على إشارة ECG المصمم والمطور في هذا البحث أيضاً. ونستعرض في الفصل السادس شرحاً لخوارزمية TEA المحسنة. كما نبين المساهمة العلمية والحدثة؛ فضلاً عن مناقشة النتائج التي توصلنا إليها في الفصل السابع.

الفصل الأول

الدراسة النظرية (القسم الأول)

المفاهيم الأساسية حول شبكات الجسم اللاسلكية WBAN

وحمايتها

1-1- تمهيد	30
2-1- شبكة الجسم اللاسلكية	30
1-2-1. عقد شبكة الجسم اللاسلكية	30
2-2-1. طوبولوجيا شبكة الجسم اللاسلكية	32
3-1- أنظمة العناية الصحية الإلكترونية المعتمدة على WBAN	33
1-3-1. طبقات نظام العناية الصحية الإلكتروني المعتمد على WBAN	33
2-3-1. مستويات الاتصال في نظام العناية الصحية الإلكتروني المعتمد على WBAN	34
4-1- حماية شبكات WBAN	37
1-4-1. أهمية حماية شبكات WBAN	37
2-4-1. التهديدات الأمنية لشبكة WBAN	37
3-4-1. متطلبات الأمان في شبكات WBAN	39
4-4-1. تحديات الأمان في شبكات WBAN	41
5-4-1. التقانات المستخدمة في WBAN وأساليب الحماية فيها	42
5-4-1. 1. بلوتوث (Bluetooth)	43
5-4-1. 2. بلوتوث منخفض الطاقة (Bluetooth Low Energy BLE)	44
5-4-1. 3. معيار IEEE 802.15.4 وتقانة Zigbee	45
5-4-1. 4. معيار IEEE 802.15.6	46
5-1- حماية شبكات WBAN بالاعتماد على القيم الحيوية	48
1-5-1. 1. إشارة التخطيط الكهربائي للقلب	50
1-5-1. 1. خصائص إشارة ECG	50
1-5-1. 2. تحصيل إشارة ECG	52
6-1- خاتمة	55

1-1- تمهيد

في الفصل الأول من الأطروحة، نقدم بدايةً تعريف شبكة الجسم اللاسلكية WBAN، والأنواع المختلفة لعقدها، والطوبولوجيا الخاصة بها. ثم نستعرض شرحاً لطبقات تبادل البيانات في أنظمة العناية بالصحة المعتمدة على WBAN، ومستويات الاتصال فيها. بعد ذلك نتوجه للحديث عن أهمية حماية شبكات WBAN، والتهديدات الأمنية التي تتعرض لها، ومتطلبات الأمان الخاصة بها، وكذلك تحديات تحقيق الأمان فيها. كما ندرس معايير الاتصالات المستخدمة في WBAN، وأساليب حماية المعلومات في كل منها. وختاماً نتحدث عن طرائق حماية WBAN بالاعتماد على القيم الحيوية، وبالتحديد إشارة التخطيط الكهربائي للقلب.

1-2- شبكة الجسم اللاسلكية

شبكة الجسم اللاسلكية (WBAN)، هي عبارة عن شبكة مكونة من مجموعة من الحساسات اللاسلكية الموضوعة على جسم الإنسان والتي تتصل بعضها مع بعض، بهدف مراقبة الحالة الصحية للمرضى عن بُعد [1]، [4]. تتكون شبكة الجسم اللاسلكية من أنواع مختلفة من الحساسات التي يمكن وضعها على سطح جسم الإنسان أو حوله أو داخله. تُستخدم لقياس التغيرات في العلامات الحيوية للإنسان، مثل: درجة حرارة الجسم، وضغط الدم، ومعدل أكسجة الدم، والتخطيط الكهربائي للقلب، وغيرها [7]، [45]. كما تحوي هذه الشبكات أيضاً على بعض المشغلات الميكانيكية (actuators) كمضخات الأنسولين وغيرها [4]. يمكن استخدام شبكات WBAN في عددٍ من التطبيقات الطبية، ومنها إظهار الإشارات الحيوية لجسم الإنسان في العيادة أو في المنزل، وفي التطبيقات غير الطبية كإظهار الإشارات الحيوية للرياضيين. أما في أنظمة العناية الصحية الإلكترونية فيمكن، على سبيل المثال، استخدام البيانات التي تُجمع بواسطة الحساسات، لتنبيه المختصين عند وقوع حدث ما يهدد حياة المريض [7].

1-2-1. عقد شبكة الجسم اللاسلكية

اقترح معيار IEEE 802.15.6 الخاص بشبكات WBAN، والذي اعتمد من قبل معهد مهندسي الكهرباء والإلكترونيات (Institute of Electrical and Electronics Engineers IEEE) تصنيفاً لعقد WBAN؛ وفقاً

لطريقة تموضعها بالنسبة للجسم، ودورها في الشبكة [46]. تنتمي جميع عقد WBAN لنفس الجسم، ويمكن تصنيفها بناءً على تموضعها بالنسبة لجسم الإنسان كما يأتي [28]، [46]:

- عقد الزرع (Implant Node): يزرع هذا النوع من العقد إما تحت الجلد وإما داخل أنسجة الجسم.
- عقد سطح الجسم (Body Surface Node): توضع إما على سطح الجسم وإما على بُعد حوالي سنتيمترين من جسم الإنسان.
- عقد خارجية (External Node): لا تتلامس مع جسم الإنسان؛ بل تكون على بُعد بضعة سنتيمترات إلى 5 أمتار من جسم الإنسان.

كما يمكن تصنيف عقد شبكات WBAN تبعاً لدورها في الشبكة كما يأتي [4]، [15]، [28]:

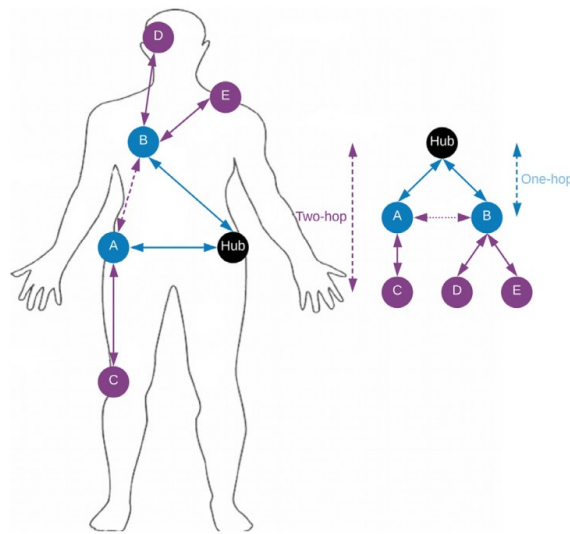
- المنسق (Coordinator): وتدعى هذه العقدة أيضاً الموزع (Hub) أو عقدة المجرى (Sink node). تعمل كبوابة (gateway) للعبور إلى شبكات WBAN أخرى أو إلى الشبكة الخارجية. تمر جميع الاتصالات من شبكة WBAN إلى الشبكة الخارجية عبر هذه العقدة. وتكون مواردها أعلى من موارد العقد الأخرى ضمن WBAN. يمكن أن يكون المنسق أحد عقد WBAN، كما يمكن أن يأخذ المساعد الرقمي الشخصي (Personal Digital Assistant PDA) أو الهاتف الذكي دور منسق شبكة WBAN، حيث تُرسل بقية العقد المعلومات المحصلة إليه من أجل نقلها من المريض إلى الأطباء الذين يتخذون القرارات والإجراءات اللازمة اعتماداً على المعلومات التي يتم الحصول عليها من تلك الحساسات [47].
- العقدة الطرفية (End Node): يكون هذا النوع من العقد مقيّداً بتنفيذ التطبيق المحدد له. كما تتقل هذه العقد المعلومات إلى المنسق، إما من خلال إرسالها إليه مباشرةً أو عن طريق عقدة المبدل.
- المبدل (Relay): وهي عقدة وسيطة تتوضع ضمن مجال اتصال المنسق. تُسهم في نقل البيانات من العقدة الطرفية إلى المنسق إذا كانت بعيدة عنه. على سبيل المثال، إذا كانت العقدة الطرفية على القدم، وخارج نطاق اتصال المنسق الموضوع على المعصم، فسيكون من المطلوب إرسال بياناتها إلى المنسق عن طريق عقدة المبدل.

ويمكن أيضاً تصنيف العقد بناءً على الوظيفة التي تؤديها، فهي: إما أن تقيس قيمة حيوية محددة وإما أن تعمل كمشغل ميكانيكي. يستقبل المشغل الميكانيكي المعلومات من الحساسات، وبناءً عليه يُحدّد آلية التشغيل. على سبيل المثال ضخ كمية محددة من الأنسولين بناءً على المعلومات الناتجة عن قياس عامل السكر في الدم [4]، [48].

تعاني عقد WBAN، وبالتحديد العقد الطرفية، وعقد التبديل من محدودية الموارد من حيث الذاكرة، واستخدام وحدة المعالجة المركزية، واستهلاك الطاقة [6]، [7]. كما تعاني عقد الزرع من صعوبة الوصول إليها لدى الحاجة إلى تغيير إعداداتها أو استبدال وحدة الطاقة. بناءً على ذلك، لابدّ من إيجاد خوارزميات وطرق لحماية بيانات WBAN تراعي تلك القيود.

2-2-1. طبولوجيا شبكة الجسم اللاسلكية

بحسب معيار IEEE 802.15.6، تعتمد شبكة WBAN الطبولوجيا النجمية (star topology)، حيث يكون فيها الموزّع هو العقدة المركزية للشبكة. يمكن أن تأخذ الطبولوجيا النجمية أحد شكلين، إمّا طبولوجيا نجمية بسيطة ذات قفزة واحدة، حيث تتبادل العقد الإطارات (Frames) مباشرة مع الموزّع، وإمّا طبولوجيا نجمية موسعة (extended star topology) ذات قفرتين حيث يكون الاتصال إمّا مباشراً مع الموزّع وإمّا عن طريق المبدل [15].



الشكل 1-1: طبولوجيا WBAN [15].

يجب أن تكون جميع الاتصالات بين عقد WBAN آمنة ضد الهجمات. ويبين الشكل 1-1 طوبولوجيا WBAN.

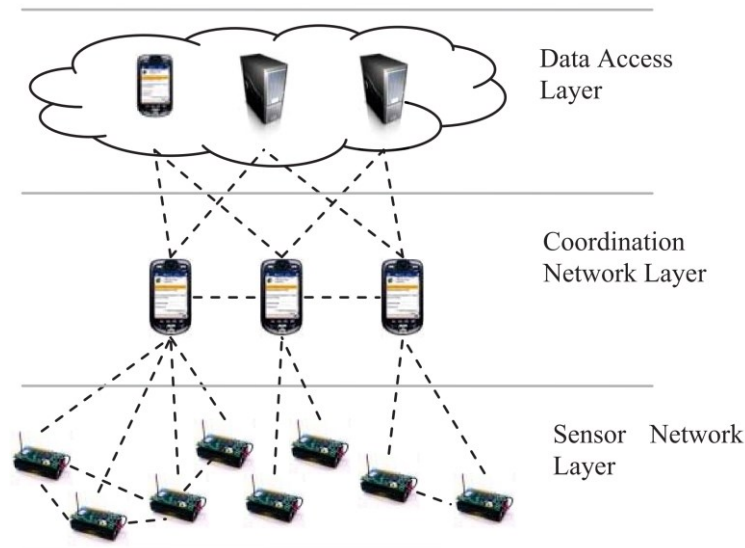
1-3-3- أنظمة العناية الصحية الإلكترونية المعتمدة على WBAN

أنظمة العناية الصحية الإلكترونية، هي الأنظمة التي تُجمَع فيها المعلومات الصحية من خلال شبكة WBAN. تتميز باستقلاليته عن المكان. ويمكن استعمالها ليس فقط في المستشفى؛ وإنما أيضاً في المنزل وفي أي مكان آخر. ففي المستشفيات تتيح حرية الحركة للمريض، أما في المنزل يمكن الاستفادة منها في نقل معلومات المريض إلى الطبيب؛ مما يساعد على إبقائه تحت المراقبة، ويوفر من تكلفة مراجعة الطبيب دورياً [4].

لهذه الأنظمة أهمية كبيرة في رفع وسطي عمر الإنسان، ورفع مستوى حياته، وحمايته من أخطار الموت من خلال الكشف المبكر عن الأزمات الصحية كالأزمات القلبية. كما تفيد في الكشف المبكر عن الأمراض قبل أن تصبح حرجة، السيطرة على النوبات، ومن ثم التخفيف من آثارها، والاتصال المستمر بالمريض، ونقل معلوماته لحظياً في أثناء نقله إلى المستشفى في سيارة الإسعاف.

1-3-1- طبقات نظام العناية الصحية الإلكتروني المعتمد على WBAN

يتكون نظام العناية الصحية الإلكتروني من شبكة ذات بنية هرمية مكونة من ثلاث طبقات [35]، [49]، [50]. يوضح الشكل 1-2 طبقات نظام العناية الصحية الإلكتروني.



الشكل 1-2: طبقات نظام العناية الصحية الإلكتروني المعتمد على WBAN [49].

طبقة شبكة الحساسات (Sensors Network SN):

تتكون هذه الطبقة من الحساسات الطبية التي تُوضَع على جسم الإنسان أو داخله لمراقبة العلامات الحيوية. تُستخدَم هذه الحساسات تقانات اتصال مثل ZigBee أو Bluetooth أو غيرها. وبما أن هذه الحساسات لها نطاق اتصال قصير المدى، يجب أن تكون متصلة بأجهزة أكثر قوة في طبقة شبكة التنسيق؛ لتوصيل البيانات المحصلة إلى المتخصصين في الرعاية الصحية.

طبقة شبكة التنسيق (Coordination Network CN):

تتكون هذه الطبقة من أجهزة كالهاتف المحمول أو PDA أو غيرها، والتي بدورها تتصل مع محطات ثابتة بعيدة كانت أو محلية، من خلال استخدام الشبكات النقالة المخصصة (ad-hoc networks) أو شبكات قائمة على البنية التحتية (Infrastructure based networks). تُجمَع عُقد CN البيانات من طبقة SN وتحللها؛ لأن عقد SN ليس لديها قدرة عالية على تخزين ومعالجة البيانات، أما عقد CN فهي ذات قدرة معالجة أكبر، وذات طاقة أعلى.

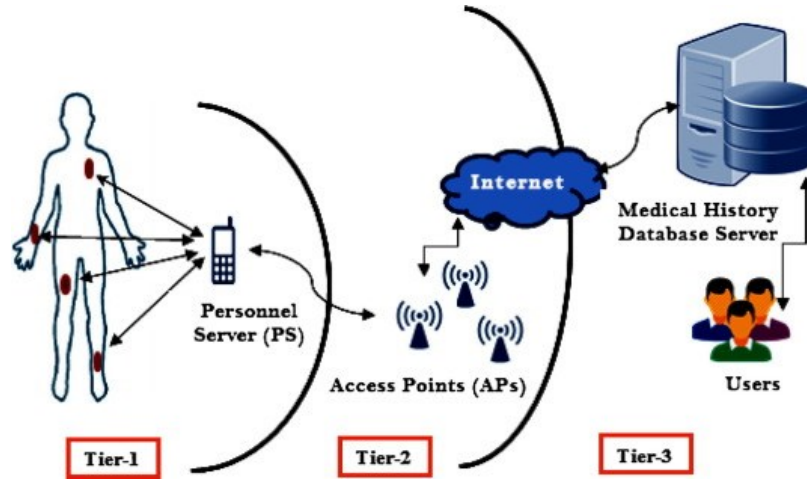
طبقة النفاذ إلى البيانات (Data Access DA):

تتضمن طبقة DA عدداً من مخدمات قواعد البيانات ونقاط الوصول التي يمكن للأطباء استخدامها للوصول إلى البيانات المحصلة. تخزّن مخدمات قواعد البيانات السجلات الطبية للمرضى الذين هم تحت المراقبة وذلك من أجل فترات زمنية طويلة. وتوفّر نقاط الوصول (Access Points APs) واجهة للأطباء للوصول إلى البيانات المحصلة. في هذا البحث، نختص بدراسة أمان نظام العناية بالصحة وذلك بالنسبة لطبقة شبكة الحساسات (SN)

أي بين حساسات شبكة WBAN.

2-3-1. مستويات الاتصال في نظام العناية الصحية الإلكتروني المعتمد على WBAN

تُقسم الاتصالات في أنظمة العناية الصحية الإلكترونية المعتمدة على WBAN إلى ثلاثة مستويات أساسية [4]. يوضح الشكل 1-3 مستويات الاتصال في تلك الأنظمة.



الشكل 1-3: مستويات الاتصال في نظام العناية الصحية الإلكترونية المعتمد على WBAN [4].

المستوى الأول (Tire 1)، الاتصال داخل شبكة WBAN (Intra-WBAN):

في هذا المستوى، تتصل عقد حساسات WBAN بعضها مع بعض ضمن مساحة جسم المريض. يعمل المخدّم الشخصي (Personal Server PS) كبوابة لنقل المعلومات إلى المستوى التالي؛ أي كنقطة وصول إلى المستوى الثاني. قد يكون المخدّم الشخصي هو نفسه المنسق أو قد يكون جهازاً آخر [4]. تُستخدَم الاتصالات اللاسلكية في هذا المستوى الترددات الراديوية (Radio Frequency RF) والتي يمكن أن تُستخدَم ثلاثة نطاقات ترددية مختلفة، وهي [51]:

- خدمات القياس الطبي اللاسلكي عن بُعد (Wireless Medical Telemetry Services WMTS) تتضمن نطاقات التردد من 608 MHz إلى 614 MHz، ومن 1395 MHz إلى 1400 MHz، ومن 1427 MHz إلى 1432 MHz.
- حزمة الترددات الراديوية من دون ترخيص للتطبيقات الصناعية والعلمية والطبية (Unlicensed Industrial, Scientific, and Medical ISM) وتتضمن النطاقات من 2.4 GHz إلى 4.4835 GHz.
- خدمات الاتصالات للزرعات الطبية (Medical Implant Communication Service MICS) وتتضمن النطاقات من 402 MHz إلى 405 MHz.

ويمكن أيضاً في هذا المستوى إذا كانت الحساسات كلها داخل الجسم كالحساسات النانوية استخدام طرائق الاتصال التقليدية كالاتصالات بالأمواج فوق صوتية أو الكهرومغناطيسية أو استخدام الاتصالات الجزيئية التي تستخدم جزيئات جسم الإنسان لنقل البيانات. وتقتصر بعض الدراسات استخدام جسم الإنسان كقناة اتصال بالاستفادة من خصائصه الموصلة لتحقيق الاتصال بين الأجهزة الموجودة على الجسم والمنسق، شريطة أن يمس المنسق الجسم فعلياً [52].

المستوى الثاني (Tire 2)، الاتصال خارج شبكة WBAN (Inter-WBAN):

يربط هذا المستوى الفجوة بين PS والجهة المقدمة لخدمة العناية الصحية؛ وذلك عبر نقاط الوصول. ومن ثم يسعى الاتصال على هذا المستوى إلى ربط شبكات WBAN بنظم أو شبكات أخرى، بحيث يمكن استرجاع المعلومات بسهولة من خلال وسائل متعددة، مثل الإنترنت [4]. تُستخدم الأمواج الراديوية بشكل أساسي للاتصال، مثل: الاتصال بالمجال القريب (Near Field Communication NFC) ذو التردد 13.56 MHz والبلوتوث منخفض الطاقة (Bluetooth Low Energy LE) ذو التردد 2.4 GHz و Zigbee ذو التردد 2.4 GHz و WiFi Direct ذو التردد 2.4 GHz أيضاً [51].

المستوى الثالث (Tire 3)، الاتصال ما وراء WBAN (Beyond-WBAN Communication):

تعد قاعدة البيانات الطبية جزءاً مهماً من اتصالات المستوى الثالث، فهي تحوي التاريخ الطبي والملف الشخصي الخاص بالمرضى. يسمح هذا المستوى من الاتصال لمقدمي الخدمات الطبية باستعادة معلومات المرضى عبر الإنترنت [4]. تؤمن هذه المرحلة عدداً من خيارات الاتصال بالمُخدّم الطبي (Medical Server MS)، ومنها تقانات 3G/4G و WiFi وغيرها [51]. كما يمكن أن يصبح PS جسراً بين المستوى الأول والثالث، وذلك باستخدام تقانات 4G / 3G / GPRS التي تقوم بوصله مباشرةً بشبكة المستوى الثالث [4].

في بحثنا هذا، نسعى لتحقيق أمان نظام العناية بالصحة وذلك في المستوى الأول (Tire 1) من مستويات

الاتصال، أي على مستوى الاتصال داخل شبكة WBAN.

1-4-4- حماية شبكات WBAN

1-4-1. أهمية حماية شبكات WBAN

في أنظمة العناية الصحية الإلكترونية تقوم الحساسات الطبية بتحصيل بيانات جسم المريض، وترسل رسائل عن تلك البيانات إلى الطبيب أو إلى مخدم المستشفى كما وضعنا في الفقرات السابقة. في أثناء ذلك قد يتم مهاجمة شبكة WBAN، على سبيل المثال، التتصت على البيانات من القنوات اللاسلكية والتقاطها وتعديلها [4]. ومن ثم يُعدُّ الحفاظ على أمان تلك البيانات وخصوصيتها أحد أهم التحديات؛ إذ يجب الحفاظ على أمان معلومات المريض من ناحية؛ للتأكد من أن بياناته محمية من المستخدمين غير المصرح لهم وذلك أثناء جمعها ونقلها ومعالجتها وتخزينها، ومن ناحية أخرى، يجب الحفاظ على خصوصية المعلومات، أي إعطاء المريض السلطة على التحكم في جمع معلوماته الشخصية واستخدامها [4]، [53]، حيث تُعدُّ بيانات المريض حساسة للغاية، خاصةً إذا كان يعاني من مرض محرج أو إذا كان ذا مكانة معينة [39]. يمكن لذلك المريض أن يعاني من الإذلال أو حتى الاضطراب النفسي إذا تم الإبلاغ عن معلومات مرضه. ومن بالغ الأهمية أيضاً حماية القرارات الطبية والمعلومات الطبية من الوصول غير المصرح به الذي قد يشكل خطراً على حياة المريض، وأحياناً يؤدي إلى الوفاة [39]، على سبيل المثال، تغيير جرعة الدواء أو إجراءات العلاج، إذا وقعت في اليد الخاطئة [4]. ومن ثم، لا بد من تطبيق آليات حازمة للحفاظ على أمان WBAN.

1-4-2. التهديدات الأمنية لشبكة WBAN

تتعرض شبكات WBAN لأنواع متعددة من الهجمات والتهديدات الأمنية والتدخلات الخارجية التي يمكن أن تخترق الشبكة. فيما يأتي نعرض الأنواع الأكثر شيوعاً للهجمات الأمنية على WBAN:

الوصول غير المرخص (Unauthorized Access): أي إمكانية الوصول إلى عقد الشبكة، والتحكم بها، والاتصال معها من قبل الأشخاص غير المصرح لهم بذلك [4].

هجوم منع الخدمة (Denial of Service Attack): ويتم ذلك من خلال التشويش (Jamming) على عقدة أو مجموعة من العقد والذي يمكن أن يكون تشويشاً ثابتاً أو تشويشاً متقطعاً [28]، [54]، فضلاً عن ذلك، يمكن للمهاجم أن ينتهك بروتوكول الاتصال، وينقل الرسائل باستمرار في محاولة لتوليد التصادم (Collision) [28]، [54]. يمكنه أيضاً استخدام آليات إغراق الشبكة (Flooding) لاستنفاد الذاكرة عن طريق إرسال حزم إضافية غير ضرورية بشكل متكرر، والتي يتعذر على النظام التعامل معها. لا يهدف ذلك إلى تعطيل الشبكة، وتخریبها، وتدميرها فحسب؛ وإنما أيضاً إلى إضعاف قدرة الشبكة على توفير خدمات الطوارئ الضرورية [4].

هجوم سيبيل (Sybil Attack): هو الهجوم الذي يمتلك فيه الحساس الخبيث هويات متعددة بشكل غير مشروع [54]. لمهاجمة بروتوكول التوجيه، يعتمد هجوم سيبيل على توجيه مسارات متعددة من خلال عقدة خبيثة واحدة تأخذ هويات عقد متعددة [54].

هجوم تكرار العقدة (Node Replication Attack): وهو يشبه هجوم سيبيل، ولكن بدلاً من التوصل إلى عقدة تستخدم هويات متعددة، يسعى المهاجم إلى استبدال ذاكرة عقدة ما (العقدة الخبيثة) بذاكرة عقدة أخرى. يصعب في هذا الهجوم اكتشاف أن العقدة أصبحت زائفة، ومن ثم يمكنها أن تُتلف الحزم أو أن تُوجهها بشكل خاطئ [54]. قد تقوم العقدة المنسوخة برفض توجيه الرسائل، أو توجيهها عن قصد إلى العقد غير الصحيحة [4].

هجوم تحليل حركة المرور (Traffic Analysis Attack): في شبكات WBAN تُجمع البيانات من خلال العقد، وتُوجّه في النهاية إلى المنسق. في كثير من الأحيان، يتمكّن المهاجم من تحديد العقد الرئيسة في الشبكة، أو عقدة المنسق، ويتم ذلك حتى من دون فهم محتويات الحزم إذا كانت تلك الحزم مُعمّاة. يعتمد هجوم تحليل حركة المرور على ملاحظة أن العقد الأقرب إلى عقدة المنسق تميل إلى إرسال رزم أكثر من تلك التي تبعد عنها [54].

فضح البيانات (Data Exposure): وتعني قدرة المهاجم على قراءة محتوى الرسائل المتبادلة بين حساسات WBAN [4].

العبث بالبيانات وتعديلها (Data tampering and modification): في هذا الهجوم لا يتم التوصل إلى قيم البيانات الطبية بطريقة غير مشروعة فحسب؛ وإنما تغييرها أيضاً. على سبيل المثال، يمكن للخصم التقاط حساس التخطيط الدماغى وإعاقته وإرسال معلومات خاطئة إلى الطبيب [4]، [16]. ويمكن أيضاً في هذا النوع من الهجمات تكرار رسائل سابقة، حيث يستخدم المهاجم بيانات المريض أو رسائله القديمة على أنها رسائل حديثة؛ مما قد يؤدي إلى خلل في تقديم العناية الصحية.

المراقبة والتنصت (Monitor and Eavesdropping): ويُعدُّ الهجوم الأكثر وضوحاً على الخصوصية. يتم من خلاله التنصت على البيانات؛ مما يُمكن الخصم من اكتشاف محتويات الاتصال. كما يُمكن للخصم أيضاً تحليل حركة المرور للتوصل إلى معلومات التحكم، ومعلومات حول بنية شبكة الحساسات [16]، [54].

هجوم تمويه الخصم (Camouflage Adversary Attack): يُمكن للخصم إدخال عقدة زائفة أو اختراق عقدة ما في شبكة الحساسات، ليتسنى بعد ذلك لهذه العقدة أن تظهر وكأنها عقدة عادية لجذب الحزم، ثم إعادة توجيهها إلى العقد التي تُحلَّل الخصوصية [16]، [54].

الهجمات الفيزيائية (Physical Attacks): وتعني التدمير الفيزيائي للعقدة أو العبث بها [28]، [54].

3-4-1. متطلبات الأمان في شبكات WBAN

بناءً على التهديدات الأمنية التي تتعرض لها WBAN، نستنتج عدداً من المتطلبات الأمنية التي يجب تحقيقها من أجل حماية الشبكة، نذكر منها:

- **سرية البيانات (Data Confidentiality):** يجب حماية البيانات من الوصول غير المصرح به والذي

قد يشكل خطراً على حياة المريض. يمكن أن توفر التعمية سرية هذه البيانات الحساسة [16]، [17]،

[55].

- **تكامل البيانات (Data Integrity):** يشير تكامل البيانات (سلامة البيانات) إلى التدابير المتخذة لحماية محتوى الرسالة والحفاظ على دقتها واتساقها. على سبيل المثال، حماية البيانات من التعديلات التي يمكن للخصم أن يطبقها عليها [4]، [16]، [17].
- **حداثة البيانات (Data Freshness):** يجب أن تكون البيانات محمية من تسجيلها، وإعادة استخدامها من قبل الخصم على أنها بيانات حديثة. هناك نوعان من حداثة البيانات: حداثة قوية (Strong freshness) تهتم بموضوع التأخير الزمني وترتيب الإطارات، وحداثة ضعيفة (weak freshness) تقتصر على ترتيب الإطارات، ولكنها لا توفر أي ضمانات من حيث التأخير [4]، [17]، [54]. يمكن تحقيق الحداثة من خلال استخدام عداد للرسائل، وربطها بزمان إرسالها.
- **متاحة الشبكة (Network Availability):** نظام العناية بالصحة يحمل معلومات مهمة وحساسة للغاية قد تكون منقذة للحياة، فمن بالغ الأهمية أن تكون الشبكة متاحة للاستخدام للمرضى في جميع الأوقات، وفي حالات الطوارئ [4]، [17]، [54].
- **مصادقة البيانات (Data Authentication):** تقوم عقد الشبكة بحساب رمز مصادقة الرسائل (MAC)؛ باستخدام مفتاح سري مشترك. يؤكد الحساب الصحيح لرمز MAC لدى العقدة المستقبلة للرسالة أن الرسالة قد أُرسِلت من قبل عقدة موثوق بها [16]، [17]، [55].
- **الإدارة الآمنة (Secure Management):** تُعنى الإدارة الآمنة بإضافة عقد WBAN وإزالتها بطريقة آمنة. كما تُعنى أيضاً بإدارة توزيع مفاتيح التعمية على عقد الحساسات [4].
- **الجدارة (Dependability):** يجب أن يكون نظام العناية بالصحة موثقاً ويمكن الاعتماد عليه؛ إذ يُشكّل عدم الاسترجاع الصحيح للبيانات المتبادلة بين حساسات WBAN مصدراً للقلق. لمعالجة هذه المشكلة، يمكن استخدام تقنيات تصحيح الخطأ [4].

• **المرونة (Flexibility):** يحتاج المريض إلى المرونة في قابلية الوصول إلى البيانات الطبية الخاصة به.

على سبيل المثال، في حالة الطوارئ، يمكن إعطاء ترخيص بالتعامل مع بيانات المريض من قبل طبيب ليس بالضرورة أن يكون من الذين أُعطوا إذنًا بذلك سابقاً [4].

نختص في هذه الأطروحة، بدراسة وتحقيق أمان شبكة WBAN بما يتعلق بسرية البيانات، والمصادقة، والإدارة الآمنة، والحدثة.

1-4-4. تحديات الأمان في شبكات WBAN

لشبكات WBAN في تطبيقات الرعاية الصحية تحديات فريدة في تحقيق الأمن والخصوصية بسبب العوامل الآتية:

قيود الموارد: عادةً ما تكون الحساسات الطبية صغيرة جداً، وهي أصغر من حساسات WSN، ومن ثم تكون قدرتها محدودة جداً من حيث الطاقة والذاكرة وقدرة المعالجة. بناءً على ذلك، يجب أن تكون وظائف الحماية خفيفة وفي الوقت نفسه آمنة بما يكفي لحماية البيانات الطبية [49]، [51]، [56].

الطبولوجيا الديناميكية للشبكة: تتغير طبولوجيا شبكة WBAN باستمرار عبر الزمن. عند تغيير الطبولوجيا، يجب ألا تؤدي إعادة إنشاء معاملات الأمان، مثل مفاتيح التعمية، إلى كثيرٍ من الحمل الزائد على الشبكة [49]، [51]. تحتاج بنية حماية WBAN أيضاً إلى أن تكون قابلة للتطوير حيث تكون أعداد العقد متغيرة [49].

التنقل: تتحرك الحساسات الطبية والمنسق في كل مرة يتحرك فيها الجسم. عندما تتغير العقد موقعها، يجب أن تبقى جميع وظائف ومفاتيح التعمية فيها قابلة للاستخدام [49].

البيئة غير المحمية: تنتشر عقد WBAN في بيئات غير محمية مما يزيد الحاجة إلى حمايتها جيداً [49].

قابلية التوسع: في شبكات WBAN، هناك احتمال كبير بأن يُزاد عدد حساسات الشبكة، ومن ثم يجب أن تكون الشبكة ديناميكية بما يكفي لكي تسمح بإضافة حساس جديد من دون أن يؤدي ذلك إلى خلل في أمن الشبكة [51].

إدارة المفاتيح: هناك خيارات محتملة عدّة لإدارة المفاتيح، وهي [51]:

- أ. توزيع المفاتيح ما قبل النشر، حيث تُخزن مجموعة المفاتيح في العقد قبل نشرها على جسم الإنسان.
- ب. التوزيع النشط للمفاتيح، حيث يتم تبادل المفاتيح بعد نشر العقد.
- ت. تبادل المفاتيح عند الطلب، حيث يتم تبادل المفاتيح بعد نشر العقد، أي في أثناء إجراء الاتصالات.
- ولكن تعد إمكانات التخزين والمعالجة لحساسات WBAN محدودة للغاية، مقارنةً بالإمكانات المطلوبة لتطبيق تقنيات إدارة المفاتيح.

تعدُّ الوصول المادي: بالنسبة لحساسات WBAN التي تكون مزروعة داخل الجسم، يكون من الصعب الوصول الفيزيائي إليها من أجل حل مشاكل الأمان والخصوصية التي قد تتعرض لها أو من أجل تغيير الوسائط المتعلقة بحماية الشبكة كمفاتيح التعمية [51].

في هذا البحث، نسعى إلى تطوير طرق وخوارزميات تُحقِّق أمان شبكة WBAN وتراعي كافة التحديات المذكورة.

1-4-5. التقانات المستخدمة في WBAN وأساليب الحماية فيها

كما ورد سابقاً، هناك العديد من تقانات الاتصال المُستخدمة في WBAN [53]. فيما يلي، نورد شرحاً لآليات الحماية المُستخدمة في تلك التقانات.

الجدول 1-1: التقانات المستخدمة في WBAN وخوارزميات الحماية المستخدمة فيها.

التقانة	خوارزميات الحماية المستخدمة فيها
Bluetooth	SHA-256 لتحقيق تكامل البيانات AES-CCM لتعمية الرسائل ومصادقتها Secure Simple Pairing SSP لإنشاء المفاتيح
Bluetooth Low Energy	AES-CCM لتعمية الرسائل ومصادقتها 256 Elliptic Curve Diffie-Hellman (ECDH) للتوقيع والمصادقة
IEEE 802.15.4 & ZigBee	AES-CTR للتعمية؛ باستخدام مفتاح طوله 128 bit AES-CBC-MAC لمصادقة الرسائل AES-CCM لتعمية الرسائل ومصادقتها
IEEE 802.15.6	Diffie-Hellman لتبادل المفاتيح AES-CCM لتعمية الرسائل ومصادقتها

نسعى في هذا البحث إلى التوصل إلى طرائق وآليات حماية تكون أقل تكلفة وأكثر فاعلية لتطبيقها في شبكات WBAN من آليات الحماية المستخدمة في التقانات المستخدمة في شبكات WBAN. ويبين الجدول 1-1 ملخصاً حول التقانات المستخدمة في WBAN، وخوارزميات الحماية المستخدمة في كلٍ منها.

1.5-4-1. بلوتوث (Bluetooth)

صممت تقنية بلوتوث، لتكون معياراً للاتصال اللاسلكي قصير المدى. بفضل هذه التقنية، يمكن لكل جهاز أن يتصل في الوقت نفسه مع ما يصل إلى سبعة أجهزة أخرى. تعمل أجهزة بلوتوث في نطاق ISM بتردد 2.4 GHz وتغطية تتراوح من 1 إلى 100 متر، ويكون الحد الأقصى لمعدل البيانات هو 3 Mbit/sec [45]. تعمل جميع أجهزة بلوتوث، وفق واحدٍ من أربعة أنماط حماية [57]، [58]:

- وضع الأمان 1: غير آمن (non-secure).
- وضع الأمان 2: فرض الأمان على مستوى الخدمة (service level enforced security).
- وضع الأمان 3: فرض الأمان على مستوى الوصلة (link level enforced security).
- وضع الأمان 4: فرض الأمان على مستوى الخدمة مع تبادل مُعَمَّى للمفاتيح (service level enforced security with encrypted key exchange).

لا تمنح الأوضاع 1 و3 أماناً على مستوى الخدمة. يمكن لوضع الأمان 2 تحقيق أي مجموعة من خدمات الأمان الأساسية الآتية: المصادقة، السرية، والتحويل (authorization). يُحدّد وضع الأمان 4 خمسة مستويات حماية. في هذا الوضع، يُستخدم SHA-256 كتابع بصمة (Hash function) من أجل التحقق من صحة البيانات. ويُستخدم AES (Advanced Encryption Standard) وفق النمط CCM (Counter with CBC-MAC) للتعمية. كما يُستخدم الاقتران البسيط الآمن (Secure Simple Pairing SSP) لإنشاء المفاتيح. يتم فرض الوضع 4 كوضع إلزامي لإصدارات بلوتوث الحديثة.

1-4-5.2. بلوتوث منخفض الطاقة (Bluetooth Low Energy BLE)

تم اشتقاق بلوتوث منخفض الطاقة من معيار بلوتوث. وهو أكثر ملاءمة لتطبيقات WBAN، حيث يكون استهلاك الطاقة فيه أقل. تم تصميم BLE لوصل الأجهزة الصغيرة بالأجهزة المحمولة لاسلكياً. غالباً ما تكون هذه الأجهزة صغيرة جداً بحيث لا تتحمل استهلاك الطاقة، ومن ثم لا تتحمل التكلفة المرتبطة ببيت بلوتوث التقليدي. توفر تقانة BLE معدل بيانات يصل إلى 1 Mbit/sec. إن معدل البيانات الاسمي (Nominal Data Rate)، زمن الاستجابة (Latency) المنخفض، واستهلاك الطاقة المنخفض، يجعل BLE مناسباً للتواصل بين حساسات WBAN و AP [45].

إذا أرادت الأجهزة التواصل مع بعضها بشكل آمن، يجب أن يتم إقرانها (Pairing devices). يتم تنفيذ عملية الاقتران هذه عن طريق جهاز مركزي (مثل الهاتف الذكي). تتضمن هذه العملية مصادقة هوية الجهازين المقترنين، وتعمية الاتصال بينهما باستخدام مفتاح قصير الأمد (Short-term Key STK)، ثم توزيع المفاتيح طويلة الأمد (Long-term Keys LTK) المستخدمة لتعمية البيانات. تحتفظ الأجهزة بالمفتاح LTK للقيام بعملية الاتصال بشكل أسرع في المرات القادمة [59]، [60].

تُعمى البيانات في BLE باستخدام AES-128-bit، وفق النمط CCM، ويُستخدَم LTK مع هذه الخوارزمية كمفتاح سري مشترك ذي طول 128 bit. ويتم تحقيق المصادقة في BLE من خلال توقيع البيانات رقمياً.

في BLE هناك وضعان للأمان، وهناك مستويات أمان عدّة لكل وضع. يحقق وضع الأمان الأول حماية الاتصال عن طريق التعمية، ويحتوي على أربعة مستويات [61]:

- مستوى الأمان 1: لا يوجد أمان (لا يوجد مصادقة ولا تعمية).
- مستوى الأمان 2: الاقتران مُعمى، وغير مصادق عليه.
- مستوى الأمان 3: الاقتران مصادق عليه، ومُعمى وفق AES-CCM.
- مستوى الأمان 4: وفيه تكون اتصالات BLE آمنة، ومصادق عليها، ومقترنة بالتعمية، باستخدام خوارزمية

AES-CCM ويتم تبادل مفاتيح التعمية وفق Elliptic Curve Diffie-Hellman P-256 (ECDH).

أما وضع الأمان الثاني، فيفرض حماية الاتصال عن طريق توقيع البيانات، ويحتوي على مستويين:

- مستوى الأمان 1: الاقتران غير مصادق عليه مع توقيع البيانات.

- مستوى الأمان 2: مصادقة الاقتران مع توقيع البيانات.

وهناك أيضاً وضع أمان ثالث، وهو وضع الأمان المختلط الناتج عن تطبيق وضعي الأمان 1 و 2 معاً.

1-4-5.3. معيار IEEE 802.15.4 وتقانة Zigbee

IEEE 802.15.4 هو معيار خاص بشبكات المنطقة الشخصية اللاسلكية منخفضة معدل البيانات (Low-Rate

Wireless Personal Area Networks LR-WPANs). فهو يضع معياراً للطبقة الفيزيائية، وطبقة التحكم

بالوصول من أجل LR-WPAN، وهو يشكل أساساً لتقانة الاتصال Zigbee وغيرها.

ZigBee، هي واحدة من تقانات الشبكات اللاسلكية المستخدمة على نطاق واسع في البيئات منخفضة

الطاقة. يستهدف ZigBee تطبيقات التردد اللاسلكي التي تتطلب معدل بيانات منخفضاً، وعمر بطارية طويلاً،

وشبكة آمنة. يُحدّد معيار IEEE 802.15.4 طبقات التحكم في الوصول الفيزيائي والوصول إلى الوسيط الفيزيائي

في تقانة ZigBee. تعمل الأجهزة اللاسلكية المعتمدة على تقانة ZigBee في نطاقات تردد 868 MHz

و 915 MHz و 2.4 GHz. أحد عيوب Zigbee وهو معدل البيانات المنخفض 250 Kbit/sec؛ مما يجعله غير

مناسب لتطبيقات شبكة WBAN في الزمن الحقيقي [45].

في IEEE 802.15.4 تُستخدم خوارزمية AES لتعمية البيانات، ويُستخدم رماز مصادقة الرسائل

(Message Authentication Code MAC) للتحقق من صحة البيانات التي يتم إرسالها، حيث يُلحق بالرسالة.

يتم تحقيق المصادقة أيضاً من خلال إنشاء أجزاء مُعمّاة من إطار IEEE، باستخدام مفتاح الشبكة، فإذا تلقت

العقدة رسالة من عقدة غير موثوقة، فسيكون MAC الرسالة غير متوافق مع ما يجب إنشاؤه، باستخدام المفتاح

الحالي، ومن ثم يتم تجاهل هذه الرسالة. يمكن في IEEE 802.15.4 تحديد أنماط أمان عدّة ومنها [62]:

- AES-CTR: في هذا النمط تُعمّى البيانات، باستخدام خوارزمية AES-128-bit؛ وفق نمط العداد (CTR)

لحساب رمز المصادقة.

- AES-CBC-MAC: وفيه يكون رمز مصادقة الرسائل مرفقاً بنهاية البيانات. يعتمد طوله على مستوى الأمان المحدد في سياسة الأمان المختارة. يُحسب MAC من أجل ترويسة إطار 802.15.4 وبياناته.
- AES-CCM: وهو مزيج من النمطين السابقين.

يُطبّق ZigBee طبقتين إضافيتين للأمان على الطبقات الأعلى من IEEE 802.15.4، وهي طبقة الشبكة وطبقة التطبيق. تعتمد جميع سياسات الأمان على خوارزمية التعمية AES-128-bit. هناك ثلاثة أنواع من المفاتيح [62]:

- المفاتيح الرئيسية: يتم تثبيتها مسبقاً في كل عقدة. وتتمثل مهمتها في الحفاظ على سرية تبادل مفاتيح الارتباط بين أي عقدتين في أثناء عملية إنشاء المفاتيح.
- مفاتيح الارتباط: وهي فريدة بين كل زوج من العقد. تُدار هذه المفاتيح بواسطة طبقة التطبيق. تُستخدم لتعمية جميع البيانات بين كل جهازين، ولهذا تستهلك المزيد من موارد الذاكرة في كل جهاز.
- مفتاح الشبكة: هو مفتاح طوله 128 bit فريد ومشارك بين جميع أجهزة الشبكة. يُنشأ من قبل مركز ثقة (Trust center)، وهو عقدة موثوقة مسؤولة عن ذلك، وعادةً ما تكون عقدة المنسق، ويُجدد على فترات مختلفة. يجب أن تحصل كل عقدة على مفتاح الشبكة من أجل الانضمام إليها. بمجرد أن يقرر مركز الثقة تغيير مفتاح الشبكة، ينتشر المفتاح الجديد عبر الشبكة، باستخدام مفتاح الشبكة القديم. يجب على مركز الثقة أن يُصادق كل جهاز يحاول الانضمام إلى الشبكة وأن يتحقق من شرعيته.

4.5-4-1 معيار IEEE 802.15.6

وهو أول معيار مخصص لشبكات WBAN يخدم التطبيقات الطبية وغير الطبية المختلفة، ويدعم الاتصالات داخل جسم الإنسان وحوله [63]، [64]. يُعرّف هذا المعيار طبقة التحكم في الوصول إلى الوسائط (Media Access Control layer MAC) [65] ويستخدم نطاقات تردد مختلفة لنقل البيانات بما في ذلك: النطاق الضيق (Narrowband NB) الذي يشمل النطاقات 400 MHz و 800 MHz و 900 MHz، والنطاقين 2.3 GHz و 2.4 GHz، والنطاق العريض للغاية (Ultra-Wideband UWB)، ونطاق الاتصال ضمن جسم الإنسان (Human Body Area Network HBAN).

Body Communication HBC) الذي يستخدم الترددات في حدود 1050 MHz. تُعدُّ هذه المواصفات القياسية خطوة إلى الأمام في شبكات الحساسات اللاسلكية القابلة للارتداء، فهي مصممة خصيصاً للاستخدام مع مجموعة واسعة من معدّلات نقل البيانات، واستهلاك أقل للطاقة، وعدد كبير من العقد (256 عقدة)، وأولويات مختلفة للعقد؛ وفقاً لمتطلبات التطبيق. يمكن أن يلبي هذا المعيار معظم متطلبات تطبيقات شبكة WBAN عن طريق تحقيق 680 Kbit/sec كأقصى معدل لنقل البيانات، ولكن هذا المعدل غير قادر على مواجهة متطلبات التطبيقات التي تحتاج إلى جودة عالية لنقل الصوت أو الفيديو [45]. يدعم IEEE 802.15.6 ثلاثة مستويات أمان مع خصائص أمان مختلفة، وهي [65]، [66]:

- مستوى الاتصال غير الآمن (Unsecured Communication Level): تُرسل البيانات في إطارات غير محمية. لا يحتوي هذا المستوى على آليات لمصادقة البيانات وتحقيق تكاملها أو سرّيتها أو حمايتها.
- مستوى المصادقة (Authentication Level): تُرسل البيانات مع رمز مصادقتها، ولكن من دون تعمية. هذا المستوى لا يدعم السرية أو الخصوصية.
- المصادقة والتعمية (Authentication and Encryption): تُنقل البيانات في إطارات مصادقة ومُعَمَّاة. يُحدّد أحد مستويات الأمان في أثناء عملية الارتباط. ويُفعّل مفتاح رئيس (Master Key MK) للاتصال السري أحادي الوجهة (Unicast). بعد ذلك، يُنشأ مفتاح مؤقت متبادل (Pairwise Temporal Key PTK) يُستخدَم من أجل تعمية جلسة واحدة. بالنسبة للاتصال الآمن عبر البث متعدد الوجهات (Multicast)، يتم مشاركة مفتاح المجموعة المؤقت (Group Temporal Key GTK) مع كامل المجموعة [65]، [66].

بشكل عام، تعتمد بروتوكولات الأمان في IEEE 802.15.6 على تبادل المفتاح، وفق طريقة Diffie-Hellman الذي يستخدم تعمية المنحنى القطعي (Elliptic Curve Cryptography ECC)، وهي إحدى طرق التعمية غير المتناظر. يُستخدم رمز مصادقة الرسائل المعتمد على التعمية (Cipher-based Message Authentication Code CMAC) لتوليد رموز مصادقة الرسائل وMK. تبدأ العقدة عملية الاقتران الآمن عن طريق إرسال طلب اقتران آمن إلى الموزع. يستجيب الموزع إما من خلال قبول الانضمام أو رفض الاقتران. إذا

تلقت العقدة جواباً يشير إلى رفض الاقتراح، فإنها تتوقف عن إجراء الارتباط الحالي. أما إذا تلقت العقدة جواباً يشير إلى الانضمام، يُفَعَّل المفتاح MK بين العقدة والموزع من خلال اتفاق متبادل، والذي سَيُسْتَخَذَم فيما بعد لإنشاء PTK.

لإنشاء PTK، ترسل العقدة (أو الموزع) إطار طلب PTK إلى الموزع (أو العقدة). يستجيب المتلقي إما عن طريق قبول الانضمام أو رفضه. يتوقف المرسل عن الإجراء إذا تلقى جواباً سلبياً، فيما عدا ذلك، يستمر في إرسال طلبات إطار PTK إلى المتلقي. ويُوزَع GTK بين العقد باستخدام PTK. تُعَمَّى الإطارات ويُصادق عليها باستخدام AES-128-bit وفق النمط CCM [65]، [66].

1-5- حماية شبكات WBAN بالاعتماد على القيم الحيوية

كما هو واضح من الفقرة السابقة تُستخدَم تقانات الاتصالات في WBAN طرائق التعمية التقليدية، والتوقيع الرقمي و MAC ومخططات التعمية AES-CTR و AES-CBC-MAC و AES-CCM، وهي طرائق آمنة توفر حماية جيدة لشبكات WBAN؛ فضلاً عن تلك التقانات، تضمنت العديد من الدراسات السابقة طرائق أخرى وخوارزميات يمكن استخدامها لحماية WBAN. استخدم بعض الباحثين خوارزميات التعمية الكتلية (Block Cipher) المتناظرة [67]، [68]، أو التعمية الدفقية (Stream Cipher) المتناظرة [69]. وبعضهم استخدم التعمية غير المتناظرة كتعمية المنحني الإهليلجي [70]، [71] لتحقيق السرية، وخوارزميات التوقيع الرقمي [72] لتحقيق المصادقة، وتكامل البيانات. أما بعضهم الآخر فقد دمج بين التعمية المتناظرة والتعمية غير المتناظرة [49]، [73]، [74]. ولكن تعاني تلك الخوارزميات من صعوبة تنفيذها ضمن حساسات WBAN محدودة الطاقة وقدرة المعالجة؛ نظراً للعمليات المعقدة اللازمة لإتمامها [28].

اعتمدت بعض الدراسات على القيم الحيوية في حماية شبكات WBAN؛ وذلك من خلال الاستفادة من خصائص تلك القيم في تحقيق متطلبات الأمان والخصوصية. وتُعَدُّ التقنيات المعتمدة على القيم الحيوية أكثر فعالية من الطرق التقليدية [13]، [20]، [24]، [29]. يمكن استخلاص القيم الحيوية واستخدامها لإثبات الهوية؛

وذلك لأن كل شخص يكون مميزاً بخصائصه الفيزيولوجية أو السلوكية الاستثنائية. يمكن الاستفادة من بعض الخصائص الحيوية الساكنة المُقاسة في تحقيق الأمن والخصوصية، مثل مسح شبكية العين مسحاً ضوئياً أو مسح البصمات [28]. كما يمكن الاستفادة من القيم الحيوية الديناميكية، مثل تغيّر معدل نبضات القلب (Heartbeat Rate Variability HRV)، حيث يتغير الفاصل الزمني بين نبضات القلب عشوائياً. وهناك عددٌ من القيم الحيوية المتغيرة التي يمكن الاستفادة منها.

هناك أسبابٌ عدّة لتفضيل الحماية القائمة على القيم الحيوية [7]، [32]، [36]. فمن خلال تلك القيم يمكن توليد الأرقام العشوائية، باستهلاك أصغري للموارد [19]. كما يمكن الاستفادة منها في توليد مفاتيح التعمية؛ وذلك بالاعتماد على ظاهرة التشابه بين القيم المقاسة بشكل متزامن في حساسات عدّة موضوعة على الجسم نفسه. تُطبّق رموز تصحيح الخطأ على تلك القيم المقاسة في كلّ من الحساسات، للتوصل إلى قيم متطابقة يمكن تكوين المفتاح السري المشترك المطلوب اعتباراً منها [20]، [75]. يتيح ذلك تشكيل المفاتيح بأقل قدر ممكن من استهلاك الطاقة [7]. وبناءً عليه، فإن التقنيات الحيوية هي أكثر فعالية من التقنيات الأخرى المستخدمة في شبكات WBAN لتحقيق متطلبات الأمان والخصوصية، وهذا ما يدفعنا إلى اعتماد مبادئ هذه التقنيات في دراستنا.

الجدول 1-2: القياسات الحيوية والخصائص الواجب توافرها لاستخدامها في حماية بيانات WBAN.

الخصائص	التوصيف
شاملة	يملكها الجميع.
مميزة	مختلفة بما فيه الكفاية بين شخص وآخر.
مستمرة	تُولد باستمرار.
قابلة للحصول	تُجمع وتُقاس كمياً بسهولة.
غير عرضة للهجوم	يصعب إعادة إنتاجها أو التوصل إليها بسهولة.
استهلاك محدود للموارد	يجب أن يدعم استخدام الإشارة الحيوية التوصل إلى نظام ذي أداء جيد يستهلك موارد محدودة من حيث الطاقة، وتعقيد الحساب، وموارد التخزين في الذاكرة، قابل للمعالجة بسرعة عالية مع دقة معترف بها.

بشكل عام، يجب على القياسات الحيوية المستخدمة في حماية بيانات WBAN أن تفي بالخصائص الموضّحة في الجدول 2-1 [40].

تُعتبر إشارة التخطيط الكهربائي للقلب من أبرز الإشارات الحيوية التي يُمكن استخدامها لتحقيق حماية WBAN وذلك لتمتعها بالخصائص اللازمة. نورد في الفقرة التالية شرحاً عن تلك الإشارة وخصائصها والتي سنستخدمها في مخططات وخوارزميات الحماية المطوّرة في هذا البحث.

1-5-1. إشارة التخطيط الكهربائي للقلب

يسجّل التخطيط الكهربائي للقلب (ECG) النشاط الكهربائي لعضلة القلب، حيث إن عضلة القلب تُنتج نبضات كهربائية صغيرة تنتشر وتتسبب في حدوث الانقباض [76]. يمكن الكشف عن تلك النبضات من خلال جهاز التخطيط الكهربائي للقلب.

ويمكن استخلاص خصائص إشارة ECG في المجال الزمني مثل المدة الزمنية للإشارة، والمطال، وشكل المنحني، وغيرها. ويمكن استخلاص خصائصها أيضاً في المجال الترددي؛ باستخدام تحويل فورييه، أو تحويل التجيب المتقطع (Discrete cosine transformation)، وغيرها [41]، [77]. سنستخدم في مخططات الحماية المطوّرة في هذا البحث كلّ من الخصائص الزمنية والخصائص الترددية لإشارة ECG.

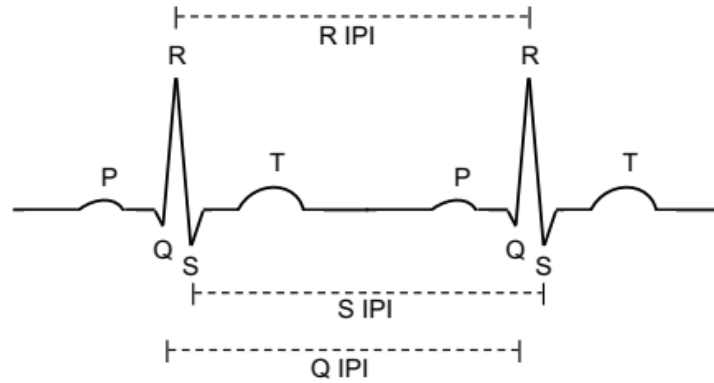
1-5-1.1. خصائص إشارة ECG

أولاً، خصائص إشارة ECG في المجال الزمني

أ. الموجة P والمركبة QRS والموجة T

تتكون إشارة ECG الطبيعية من الموجة P، والمركبة QRS، والموجة T. تُمثّل الموجة P الإشارة الكهربائية للتيار الذي يسبب تقلص الأذنين، وتُمثّل المركبة QRS التيار الذي يسبب تقلص البطينين، أما الموجة T فتُمثّل إعادة استقطاب البطينين [76]، كما هو مبين في الشكل 1-4. تُعدّ المركبة QRS الشكل الموجي الأكثر تميزاً للإشارة.

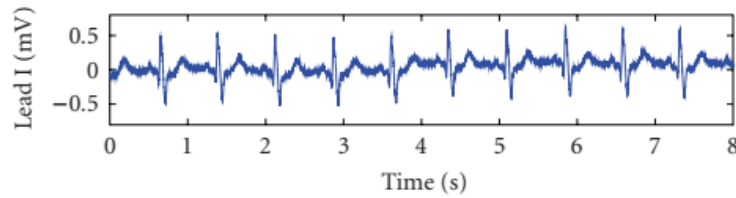
تتمتع القمم R بأكبر سعة من بين جميع الموجات؛ مما يجعل كشفها سهلاً. ومع ذلك، ليس من السهل دائماً الكشف عن الموجة QRS؛ وذلك بسبب الأنواع المختلفة من الضجيج التي يمكن أن تتعرض لها إشارة ECG.



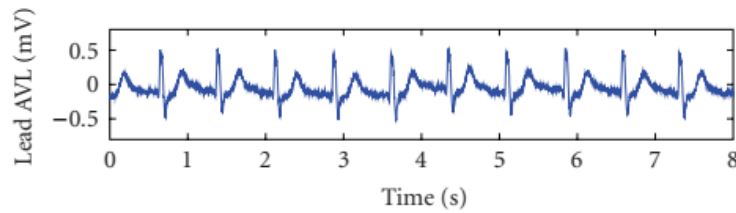
الشكل 4-1: إشارة ECG [41].

ب. الفاصل الزمني بين نبضتين متتاليتين

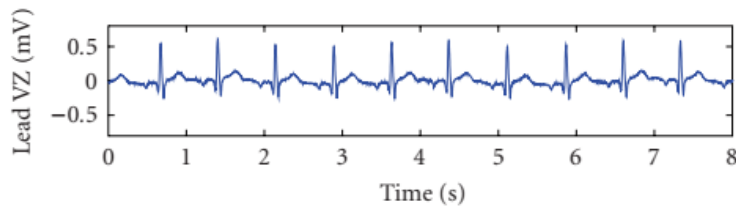
يُطلق على الفاصل الزمني بين قمتين R، أي R-R اسم الفاصل الزمني بين النبضات (Inter Pulse Interval IPI)، وهو يُمثل الفترات الزمنية بين النبضات المتتالية، كما هو موضح في الشكل 4-1.



(a)



(b)



(c)

الشكل 5-1: إشارة ECG مسجلة بشكل متزامن في ثلاثة أقطاب (حساسات) مختلفة موضوعة على الجسم نفسه [20].

يبين الشكل 1-5 قياساً متزامناً لإشارة ECG نفسها، ولكن في ثلاثة أقطاب مختلفة موضوعة على الجسم نفسه. من الملاحظ أن أشكال مركبات QRS قد تختلف بعضها عن بعضٍ، إلا أن قيم IPI في القياسات الثلاثة، وبتحقيق التزامن المناسب، تكون متطابقة بشكل ملحوظ. يعد التزامن الدقيق مطلباً رئيساً من أجل الحصول على تسلسلات IPI متطابقة في حساسات مختلفة [20].

ت. تغير معدل ضربات القلب

يُنْتَجُ تغير معدل ضربات القلب (Heart Rate Variability HRV) عن اختلاف الفاصل الزمني بين ضربات القلب من وقت لآخر. يتمتع HRV بخصائص فريدة وطبيعية عشوائية، يمكن استخدامها في حماية الاتصالات ضمن WBAN [40]، [78].

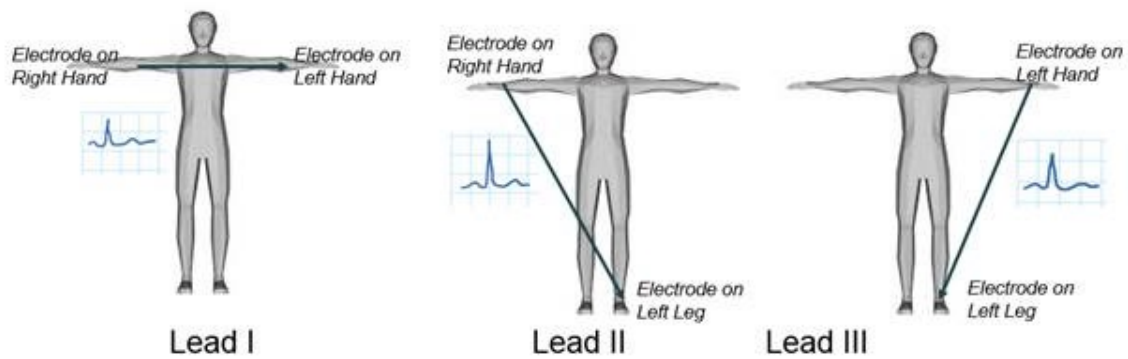
ثانياً، خصائص إشارة ECG المستخلصة في المجال الترددي:

يمكن اتباع طرائق عدّة للحصول على خصائص إشارة ECG في المجال الترددي. منها التحليل المويجي (Wavelet Distribution) الذي يساعد على تحسين عملية التصنيف وخاصةً بالنسبة لتطبيقات التعرف إلى الأشخاص والمصادقة. ويمكن أيضاً استخلاص الخصائص الترددية لإشارة ECG بتطبيق تحويل فورييه عليها والذي سنعتمده في دراستنا نظراً لبساطته. كما أن هناك العديد من الطرق الأخرى التي يمكن اتباعها للحصول على الخصائص الترددية لإشارة ECG [41].

1-5-1. 2. تحصيل إشارة ECG

يُنْتَجُ عن تقلصات جدار عضلة القلب تيارات كهربائية تنتشر في جميع أنحاء الجسم. تولّد تلك التيارات جهوداً مختلفة في نقاط الجسم المختلفة، والتي يمكن استشعارها بواسطة أقطاب كهربائية موضوعة على الجلد. تلك الأقطاب الكهربائية هي عبارة عن محولات بيولوجية مصنوعة من المعادن والأملاح. تُحَصَّل إشارة ECG من خلال الرسم البياني لتغيرات الجهد الكهربائي بين الأقطاب الكهربائية الموضوعة على جسم الإنسان [79].

تُقاس إشارة ECG باستخدام الأقطاب الكهربائية بعد وضعها في أماكن مناسبة على جلد الإنسان. يمكن الكشف عن التيارات الكهربائية التي ينشئها القلب من خلال الجلد، لأن جسم الإنسان يحتوي على سوائل بها أيونات تسمح بالتوصيل الكهربائي. تتصف الإشارة الكهربائية للقلب بمطالات صغيرة من رتبة ميكرو فولت. وكما ذكرنا، يَنْتُج التمثيل البياني لتخطيط القلب عن طريق حساب فرق الجهد الكهربائي بين كل قطبين كهربائيين، لذلك، يُعدّ تحديد مكان توضع القطب عاملاً مهماً في قياس مخطط كهربية القلب؛ حيث يمكن أن تُنتج المواضع المختلفة أشكال موجية مختلفة للإشارة نفسها. على سبيل المثال، ينتج عن نظام مكوّن من ثلاثة مسارٍ (Leads)، يطلق عليها أيضاً قنوات، ثلاثة أشكال موجية تمثل النشاط الكهربائي نفسه لعضلة القلب كما هو مبين في الشكل 1-6. يقيس المسرى I فرق الجهد بين أعلى الطرف الأيمن من الجسم وأعلى الطرف الأيسر، وذلك بشكل أفقي. يقيس المسرى II فرق الجهد بين الطرف الأيمن، عند نفس نقطة قياس المسرى I، والطرف الأيسر، وذلك بشكل قطري. بينما يقيس المسرى III فرق الجهد بين أعلى الطرف الأيسر وأسفل الطرف الأيسر من الجسم. يقدم المسرى II والمسرى III معلومات تتعلق بالقسم السفلي من عضلة القلب. بينما يقدم المسرى I معلومات عن القسم الجانبي من القلب. يسمّى النظام المكوّن من ثلاثة أقطاب، والذي تم وصفه أعلاه، مثلث Einthoven نسبةً للعالم الذي طوّر أول جهاز لتخطيط القلب [80].



الشكل 1-6: نظام تحصيل إشارة ECG مكوّن من ثلاثة مسارٍ [79].

يمكن أن يصل عدد المساري في أنظمة التخطيط الكهربائي للقلب إلى اثني عشر مسرى. يُستخدم التخطيط الكهربائي المكوّن من اثني عشر مسرى في المستشفيات لتحديد سبب عدم انتظام ضربات القلب على وجه التحديد.

ولكن، في أنظمة التطبيب عن بعد كذلك المستخدمة لمراقبة المرضى أثناء النقل إلى المستشفى والأنظمة المصممة للاستخدام اليومي على المدى الطويل، تكون الأنظمة ثلاثية المسرى هي الأكثر ملاءمة [81].

قد تتكون بعض أنظمة تخطيط القلب من مسرى وحيد. تستخدم الأنظمة أحادية المسرى قطبين كهربائيين لتمكّن من اكتشاف إشارة ECG واحدة. في هذه الأنظمة، يُحدّد توضع الأقطاب الكهربائية نوع المعلومات التي سيتم الحصول عليها من تخطيط القلب. على سبيل المثال، يُظهر المسرى II ذروة R أعلى من المسرى I مما يجعله أكثر ملاءمة لاكتشاف الفاصل الزمني R-R. لكن كلا المسريين I و II يقيسان الموجة P بطريقة يمكن استخدامها في الكشف عن أمراض قلبية معينة. تتمثل المزايا الرئيسة لأنظمة التخطيط الكهربائي للقلب أحادية المسرى في انخفاض التكلفة، كما تستخدم عناصر أقل من النظام المكوّن من اثني عشر مسرى، فهي لا تتطلب الكثير من المرفقات المرفقة للجسم مما يجعل المريض قادراً على الحركة والعمل بشكل طبيعي وخاصةً لدى استخدام أقطاب لاسلكية. ولكن، يتمثل العيب الأساسي لتخطيط القلب أحادي المسرى في نقص المعلومات المفيدة في التشخيصات الطبية لأمراض القلب. لا يمكن الكشف عن بعض أمراض القلب بواسطة مسرى وحيد، فهي تتطلب مزيداً من المعلومات المحصّلة من زوايا متعددة للقلب والتي يتم تقديمها في النظام المكون من اثني عشر مسرى. ومع ذلك، فقد أظهرت الأبحاث أن الأنظمة أحادية المسرى من المرجّح لها أن تصبح قابلة للاستخدام في التطبيقات الطبية وذلك من خلال تطويرها باستخدام الإلكترونيات الدقيقة والحساسات الحيوية، ومن خلال تحسين الخوارزميات المطبقة فيها. من أبرز تطبيقات الأنظمة وحيدة المسرى تحصيل إشارة ECG باستخدام الهاتف الذكي أو الساعة الذكية [80].

لمراعاة متطلبات أنظمة التطبيب عن بعد تم تطوير أنظمة لتحصيل إشارة ECG تعمل لاسلكياً يمكن استخدامها ضمن شبكات WBAN [81]. يمكن في تلك الأنظمة استخدام أي عددٍ مطلوب من المساري وذلك بناءً على الحالة الصحية للمريض وعلى الآفة القلبية التي يجب مراقبتها.

في دراستنا هذه نفترض أن كل حساس من حساسات شبكة WBAN يحوي قطباً كهربائياً يُشكّل مسرى مع قطب آخر (حساس آخر، أو قطب ثابت)، وبالتالي يُمكنه تحصيل إشارة ECG. يمكن استخدام إما الأنظمة

متعددة المساري أو الأنظمة وحيدة المسرى؛ ففي كلا الحالتين يستطيع الحساس استخلاص خصائص إشارة ECG في المجال الزمني (مثل IPI) وفي المجال الترددي (مثل المركبات الترددية العظمى لتحويل فورييه السريع للإشارة). تكون الخصائص المُستخلصة بشكل متزامن في كل الحساسات متشابهة، نتيجة تحصيل نشاط القلب الكهربائي نفسه [13] [20]. في دراستنا هذه لا نُعنى بتحديد مواضع الأقطاب والتي يتم تحديدها بناءً على نوع الآفة القلبية التي يسعى الطبيب لمراقبتها، وإنما نُعنى فقط بالحصول على الخصائص الزمنية والترددية الأساسية للإشارة والتي ستُستخدَم في حماية بيانات شبكة WBAN.

1-6- خاتمة

في ختام هذا الفصل، وبعد أن درسنا المفاهيم الأساسية حول شبكات WBAN وأنماط العُقد فيها والطوبولوجيا الخاصة بها، وبعد أن درسنا المعايير والبروتوكولات التي تستخدمها، وآليات الحماية فيها، لَحِظْنَا أن تلك الآليات معقدة، وبعضها يعتمد التعمية غير المتناظرة التي تستهلك طاقة الحساس. استنتجنا أن استخدام القيم الحيوية وبالتحديد إشارة ECG في مخططات حماية WBAN يمكن أن يؤدي إلى توفير طاقة الحساس، وزيادة الفعالية. في الفصل التالي نتابع دراسة المفاهيم النظرية، وبالتحديد المبادئ الأساسية حول التعمية، وتبادل المفاتيح، وتوليد السلاسل العشوائية واختبارها، وذلك من أجل تغطية جميع الجوانب العلمية التي ثُمَكُنَّا من بناء المخططات المناسبة لحماية شبكات WBAN.

الفصل الثاني

الدراسة النظرية (القسم الثاني)

المفاهيم الأساسية حول التعمية وتبادل المفاتيح

وتوليد السلاسل العشوائية

57	1-2- تمهيد
57	2-2- التعمية
57	1-2-2. التعمية المتناظرة
59	1-2-2. 1. خوارزمية التعمية متناهية الصغر
61	2-2-2. 2. التعمية غير المتناظرة
63	3-2- المصادقة
63	4-2- تبادل المفاتيح السرية
64	1-4-2. 1. تبادل المفاتيح المصادق عليها
64	5-2- الأرقام العشوائية
65	1-5-2. 1. تعريف العشوائية والسلسلة الثنائية العشوائية
65	2-5-2. 2. أنواع مولّدات الأرقام العشوائية
65	2-5-2. 1. مولّدات الأرقام العشوائية
66	2-5-2. 2. مولّدات الأرقام شبه العشوائية
67	3-5-2. 3. اختبارات العشوائية
70	3-5-2. 1. مجموعة اختبارات NIST الإحصائية
73	3-5-2. 2. برنامج اختبار سلاسل الأرقام شبه العشوائية ENT
74	3-5-2. 3. مجموعة اختبار Diehard
74	6-2- خاتمة

2-1-تمهيد

نُقدّم في هذا الفصل شرحاً للمفاهيم الأساسية حول التعمية، والمصادقة، وتبادل المفاتيح المصادق عليها، وتوليد السلاسل العشوائية واختبارها، حيث نسعى في بحثنا هذا إلى تطبيق تلك المفاهيم من أجل حماية شبكات WBAN. كما نقدّم شرحاً لخوارزمية التعمية TEA التي سيتم استخدامها في مخططات حماية WBAN المطوّرة في هذا البحث. ونورد في هذا الفصل أيضاً، شرحاً للاختبارات الإحصائية المُستخدَم لفحص العشوائية، والتي سنطبقها لاحقاً على السلاسل العشوائية المولّدة باستخدام المولّد المطوّر في هذا البحث لاختبار عشوائيتها.

2-2-التعمية

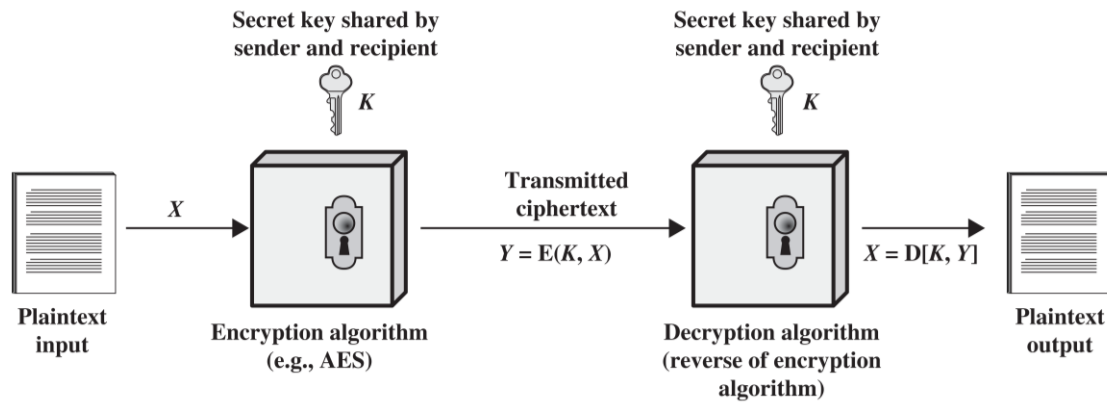
التعمية (Cryptography) هي عملية تحويل البيانات من شكل قابل للقراءة إلى شكل غير قابل للقراءة أو المعالجة إلا بعد فك تعميّتها. وتُعَدّ التعمية وحدة البناء الأساسية لأمن المعلومات. وهي من أهم الطرائق المستخدمة لضمان عدم سرقة معلومات النظام أو قراءتها من قبل أشخاص غير مصرح لهم أو من قبل المهاجم. يمكن تنفيذ عمليات التعمية من خلال مخططات وخوارزميات خاصة والتي تقسم إلى قسمين أساسيين، التعمية المتناظرة، والتعمية غير المتناظرة [17]، [82].

2-2-1. التعمية المتناظرة

ويطلق على التعمية المتناظرة (Symmetric Encryption) أيضاً اسم التعمية بالمفتاح السري (Secret Key Encryption). يتكون مخطط التعمية المتناظرة من خمسة عناصر رئيسة كما هو مبين في الشكل 2-1، وهي [17]:

- النص الصريح (Plaintext): وهو الرسالة الأصلية أو المعطيات التي تشكل دخل الخوارزمية.
- خوارزمية التعمية (Encryption Algorithm): وهي مجموعة عمليات تحويل مختلفة على النص الصريح.

- المفتاح السري (Secret Key): وهو قيمة غير معتمدة على النص الصريح، تشكل أيضاً دخلاً للخوارزمية. تُنتج الخوارزمية قيم خرج مختلفة؛ بالاعتماد على المفتاح السري المستخدم في كل مرة.
- النص المُعمّى (Cyphertext): وهو الرسالة غير الواضحة الناتجة كخرج لخوارزمية التعمية. وتعتمد على كلٍ من النص الصريح والمفتاح السري. حيث يُنتج عن نص صريح واحد نصان مُعمّيان مختلفان إذا استخدم مفتاحان سريان مختلفان. يظهر النص المُعمّى على شكل سلسلة عشوائية من المعطيات غير المفهومة.
- خوارزمية فك التعمية (Decryption Algorithm): وهي خوارزمية دخلها هو النص المُعمّى والمفتاح السري؛ بينما خرجها هو النص الصريح.



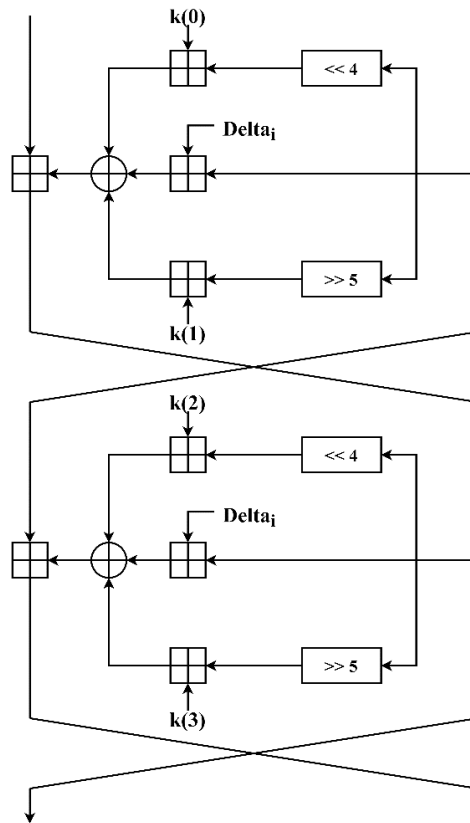
الشكل 2-1: نموذج مبسط حول التعمية المتناظرة [17].

يتطلب الاستخدام الآمن للتعمية المتناظرة أمرين أساسيين: الأمر الأول، أن تكون الخوارزمية المستخدمة قوية، فيجب ألا يتمكن المهاجم من فك تعمية النص المُعمّى أو اكتشاف المفاتيح حتى ولو توفر لديه عدد من النصوص الصريحة والنصوص المُعمّاة الموافقة لها. أما الأمر الثاني، فيجب على كلٍ من المرسل والمستقبل الحصول على نسخة من المفتاح السري بشكل آمن، وأن يبقى هذا المفتاح سرياً بينهما. فإذا استطاع أحد ما الحصول على المفتاح أو اكتشافه، فستصبح كل الاتصالات التي تستخدم هذا المفتاح مقروءةً بالنسبة له [17]. ومن الأمثلة الشهيرة حول أنظمة التعمية المتناظرة الأكثر شيوعاً، AES، DES، RC4، RC5 وغيرها العديد. إضافةً للأمثلة السابقة نذكر أيضاً خوارزمية التعمية متناهية الصغر (TEA) التي سنورد شرحاً تفصيلياً عنها في

الفقرة التالية، وذلك نظراً للاعتماد عليها في المخططات المطوّرة في هذا البحث. استخدمنا خوارزمية TEA في مخطط تبادل المفاتيح المطوّر، كما أجرينا عليها تحسينات لرفع أدائها، ولجعلها آمنة ضد الهجمات التي تتعرض لها TEA التقليدية؛ بهدف استخدامها في تعمية البيانات المتبادلة في WBAN.

1.1-2-2. خوارزمية التعمية متناهية الصغر

خوارزمية التعمية متناهية الصغر (TEA) هي الخوارزمية الأكثر فعالية من بين خوارزميات التعمية المتناظرة الشائعة، ومن ثم فهي الأسرع. تتميز برمز مصدري ذي حجم صغير للغاية بحيث يستهلك أدنى حدّ ممكن من الذاكرة [83]. كما أنها تتألف من عمليات بسيطة جداً؛ مما يجعلها الأقل استهلاكاً للموارد من بين خوارزميات التعمية المتناظرة والأكثر مناسبة لتطبيقات الزمن الحقيقي، وحماية شبكات الحساسات اللاسلكية ذات الموارد المنخفضة [84]، [85].



الشكل 2-2: جولة واحدة من جولات خوارزمية التعمية TEA، حيث k تمثل المفاتيح الجزئية، Δ_i هي إحدى مضاعفات الثابت السحري، و i تمثل رقم الجولة. [83]

تُعمي خوارزمية TEA كتلاً حجم كلٍ منها 64 bit؛ باستخدام مفتاح سري طوله 128 bit؛ وذلك بتنفيذ الخوارزمية لعدد من الجولات يتراوح بين 8 و 64 جولة بناءً على درجة الأمان المطلوبة والأداء المطلوب. يتم تقسيم المفتاح إلى 4 مفاتيح جزئية، ويتم استخدام المفاتيح الجزئية نفسها في جميع جولات التنفيذ، حيث تُنفذ عمليات الخلط بالطريقة نفسها في جميع الجولات. يبين الشكل 2-2 جولة واحدة من جولات TEA، حيث $k(0)$ ، $k(1)$ ، $k(2)$ و $k(3)$ تُمثل المفاتيح الجزئية، و Δ_i هي إحدى مضاعفات الثابت السحري¹، و i تُمثل رقم الجولة.

خوارزمية 2-1: شبه الرماز لعملية التعمية وفق خوارزمية TEA.

```

Input:
v[2], k[4], delta=2654435769
Output:
v[2] // After encryption

sum ← 0, v0 ← v[0], v1 ← v[1]
for i ← 0 to rounds do
{
    sum += delta;
    v0 += ((v1<<4) + k[0]) ^ (v1 + sum) ^ ((v1>>5) + k[1])
    v1 += ((v0<<4) + k[2]) ^ (v0 + sum) ^ ((v0>>5) + k[3])
}
v[0]=v0; v[1]=v1;

```

خوارزمية 2-2: شبه الرماز لعملية فك التعمية وفق خوارزمية TEA.

```

Input:
v[2], k[4], delta=2654435769
Output:
v[2] // After decryption

sum ← 0, v0 ← v[0], v1 ← v[1]
for i ← 0 to rounds do
{
    v1 -= ((v1<<4) + k[0]) ^ (v1 + sum) ^ ((v1>>5) + k[1])
    v0 -= ((v0<<4) + k[2]) ^ (v0 + sum) ^ ((v0>>5) + k[3])
    sum -= delta;
}
v[0]=v0; v[1]=v1;

```

تبيّن الخوارزمية 2-1 شبه الرماز لعملية التعمية وفق خوارزمية TEA. تُمثل rounds عدد الجولات. كما تُمثل $k[4]$ مصفوفة المفاتيح الجزئية، طول كل عنصر من عناصرها 32 bit، وتمثل $v[2]$ الكتلة المعمة قبل وبعد

¹ الثابت السحري هو رقم ثابت قيمته تساوي 2654435769 وهي مختارة بحيث تكون مساوية $\phi/2^{23}$ حيث ϕ تمثل النسبة الذهبية والتي تساوي $\frac{1+\sqrt{5}}{2}$.

التعمية، وهي مصفوفة مكوّنة من عنصرين طول كلّ منهما 32 bit. وتبيّن الخوارزمية 2-2 شبه الرماز لعملية فك التعمية.

تعاني خوارزمية TEA من وجود مفاتيح متكافئة (equivalent keys) حيث يكون كل مفتاح مكافئاً لثلاثة مفاتيح أخرى، مما يخفّض من الحجم الفعلي للمفتاح إلى 126 bit بدلاً من 128 [84]. كما أنها تعاني من كونها عرضة لبعض الهجمات الأمنية، وهي:

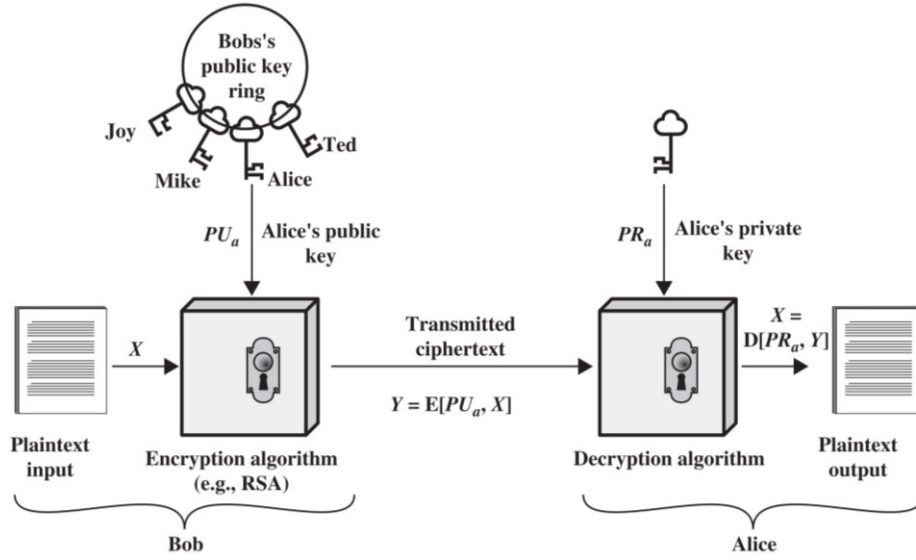
- هجوم جمع البت (Bitsum attack)، وهو هجوم يعتمد على الترابط بين مجموع الواحدات في النص المعمّى ومجموع الواحدات في مفتاح التعمية [86].
- هجوم تحليل التعمية التفاضلي (differential cryptanalysis) [87]، وهو يعتمد على دراسة تأثير اختلاف دخل خوارزمية التعمية على اختلاف خرجها، واكتشاف المواضع التي تُظهر فيها النصوص المُعمّاة خصائص غير عشوائية بما يكفي، واستغلال تلك الخصائص للتوصل إلى مفتاح التعمية.
- هجوم المفاتيح المرتبطة (related-key attack) [88]، والذي يقوم فيه محلّل التعمية بمراقبة عمليات التعمية أو فك التعمية باستخدام عدة مفاتيح سرية لا يعرفها ولكن يعرف بعض العلاقات الرياضية التي تربط بينها.

يمكن ملاحظة أن هذه الهجمات جميعها ناتجة عن استخدام نفس المفتاح في كافة جولات TEA [88].

2-2-2. التعمية غير المتناظرة

نَتَجّ المبدأ العالم للتعمية غير المتناظرة (Asymmetric Encryption)، والذي يطلق عليها أيضاً التعمية بالمفتاح العام (Public-key Encryption)، عن محاولة التعامل مع اثنتين من أصعب المسائل المتعلقة بالتعمية المتناظرة. المسألة الأولى هي مسألة توزيع المفاتيح، حيث تتطلب التعمية المتناظرة أن يكون بين الطرفين المشتركين في عملية التراسل مفتاحاً مشتركاً، والذي يجب إيصاله إليهما بطريقة آمنة للغاية. أما المسألة الثانية، فهي مسألة

التوقيع الرقمي (Digital Signature)، حيث تحتاج الوثائق الإلكترونية إلى ما يكافئ التوقيع الحقيقي للوثائق الورقية بما في ذلك التحقق من هوية صاحب الوثيقة، ومن صحة مضمونها [17]، [82].



الشكل 2-3: التعمية غير المتناظرة [17].

تعتمد خوارزميات التعمية غير المتناظرة على استخدام مفتاح لعملية التعمية، ومفتاح آخر مختلف، إنما مرتبط بالأول، خاص بعملية فك التعمية. يكون أحد المفتاحين مفتاحاً عاماً (Public key) متاحاً للجميع، أما المفتاح الآخر، فيكون مفتاحاً خاصاً (Private key) سرياً غير متاح لأحد سوى مالكه. يجب أن تمتلك هذه الخوارزميات ميزة مهمة ألا وهي: أن يكون من غير الممكن حسابياً تحديد المفتاح الخاص بمجرد معرفة خوارزمية التعمية والمفتاح العام. يبين الشكل 2-3 مخطط التعمية غير المتناظرة والذي تتحقق فيه السرية من خلال تعمية النص من قبل المرسل (وليكن Bob) بالمفتاح العام للمستقبل (ولتكن Alice)، ويفك المستقبل التعمية بمفتاحه الخاص.

تَعتمد خوارزميات التعمية غير المتناظرة على مبادئ رياضية معقدة، ومن ثم فهي أبطأ من التعمية المتناظرة، ويتطلب تنفيذها استهلاكاً كبيراً للموارد. من الأمثلة الشهيرة حول أنظمة التعمية غير المتناظرة الأكثر شيوعاً خوارزمية RSA، وخوارزمية ECC، وغيرها [17]، [82].

2-3- المصادقة

وهي الخدمة التي تسعى إلى تكوين اتصالات موثوقة؛ حيث تُقدّم خدمة المصادقة ضماناً للمستقبل بأن الرسالة التي وصلته صادرة فعلاً من المصدر الذي يدّعي أنها منه. تقدّم المصادقة خدمتين أساسيتين [17]:

- مصادقة الكيان النّد (Peer entity authentication): تؤمّن عملية إثبات الهوية أو التحقق منها لكلا طرفي الاتصال. وتعمل هذه الخدمة عند تأسيس الاتصال أو في طور التراسل.

- مصادقة مصدر البيانات (Data origin authentication): تعمل هذه الخدمة على تأكيد صحة مصدر البيانات. لا تؤمّن هذه الخدمة حماية ضد عمليات نسخ البيانات أو تعديلها.

ويمكن استخدام آليات المصافحة (Handshake) لتحقيق المصادقة، ولكنها في بعض الأحيان تعاني من هجمات إعادة الإرسال. طُوّرت خدمات خاصة لتحقيق المصادقة مثل Kerberos. يمكن أيضاً استخدام التعمية غير المتناظرة في تحقيق المصادقة؛ وذلك بمساعد طرف ثالث موثوق به [17].

2-4- تبادل المفاتيح السرية

لكي تعمل التعمية المتناظرة بشكل صحيح، يجب أن يشترك طرفا الاتصال بالمفتاح نفسه، والذي يجب أن يبقى سرياً. تهدف عملية تبادل المفاتيح (Key Exchange) إلى تمكين طرفي التعمية المتناظرة من تبادل المفتاح السري المشترك بينهما عبر قنوات اتصال غير آمنة. لا يمكن إرسال مفتاح التعمية السري من خلال طرق الاتصال التقليدية غير الآمنة؛ لأن التقاطه من قبل أي مهاجم سيجعل ذلك المهاجم قادراً على فك تعمية جميع المراسلات بين الطرفين. ومن ثمّ هناك حاجة إلى تطبيق آليات وبروتوكولات تقوم بتوفير التوزيع الآمن للمفاتيح. غالباً ما يتضمن توزيع المفاتيح استخدام المفاتيح الرئيسية MK، التي تدوم طويلاً والتي تكون نادرة الاستخدام، ومفاتيح الجلسات التي تُنشأ وتُوزّع للاستخدام المؤقت بين طرفين [17]، [82].

علاوة على ذلك، عادةً ما يكون من المرغوب فيه إجراء تغييرات متكررة على المفاتيح للحد من كمية البيانات المخترقة فيما لو عرف المهاجم المفتاح. لذلك، فإن قوة أي نظام تسمية تكمن في تقنية توزيع المفاتيح. ويمكن تحقيق عملية توزيع المفاتيح بعدة طرق، على النحو الآتي [17]:

- يمكن لطرفي الاتصال تبادل المفاتيح فيزيائياً.
 - إذا كان هناك مفتاح سري مشترك بين طرفي الاتصال متفق عليه سابقاً، يمكن لأحد الطرفين إرسال المفتاح الجديد إلى الطرف الآخر، بعد تسميته باستخدام المفتاح القديم.
 - إذا كان لدى كل من الطرفين اتصال مُعمّى بطرفٍ ثالث، فيمكن للطرف الثالث تسليم المفتاح عبر القنوات المُعمّاة إلى الطرفين الأول والثاني. ولكن يشترط أن يكون الطرف الثالث موثقاً.
- وتُستخدَم كذلك أنظمة التسمية غير المتناظرة في عمليات تبادل المفاتيح السرية للتسمية المتناظرة. كما أُوجدت أنظمة خاصة تعتمد على مبادئ التسمية غير المتناظرة من أجل تبادل المفاتيح السرية، وأحد أبرز الأمثلة حولها هي خوارزمية Diffie-Hellman [17].

2-4-1. تبادل المفاتيح المصادق عليها

يتضمن الأمان الذي يجب أن تحققه بروتوكولات تبادل المفاتيح المصادق عليها (Authenticated Key Exchange AKE) جانبين أساسيين، هما: أولاً، توفير المصادقة؛ أي التحقق من هويات الأطراف المشاركة في تنفيذ البروتوكول. ثانياً، تبادل المفاتيح السرية بشكل آمن وضمان أن المفتاح غير معروف من قبل الخصوم. بالتالي، يضمن تبادل المفاتيح المصادق عليها أن المفتاح غير معروف إلا من قبل الأطراف المصرح لها [89].

2-5-الأرقام العشوائية

تتَشأ الحاجةُ إلى الأرقام العشوائية وشبه العشوائية في عددٍ من تطبيقات حماية المعلومات. على سبيل المثال، تُستخدَم أنظمة التسمية الشائعة مفاتيح يجب إنشاؤها بطريقة عشوائية. كما يتطلب عدداً من بروتوكولات التسمية

أيضاً مدخلات عشوائية أو شبه عشوائية في نقاط مختلفة [30]. من هنا تظهر الحاجة إلى إيجاد آليات فعّالة لتوليد سلاسل من البتات تتميز بالعشوائية اللازمة لتخدم احتياجات التطبيقات سابقة الذكر.

2-5-1. تعريف العشوائية والسلسلة الثنائية العشوائية

يمكن تعريف العشوائية على أنها الحالة التي تقتصر إلى وجود نمط معيّن للأحداث، مما يجعل التنبؤ بالأحداث المستقبلية صعباً وغير ممكن. أما السلسلة الثنائية العشوائية (Random Binary Sequence RBS) فيمكن تعريفها على أنها سلسلة البتات التي يكون فيها احتمال ظهور كلٍّ من "0" و "1" يساوي 0.5 بالضبط. يتم إنتاج جميع عناصر السلسلة بحيث تكون مستقلة بعضها عن بعض، ولا يمكن التنبؤ بقيمة العنصر التالي في تلك السلسلة؛ بغض النظر عن عدد العناصر التي أنتجت سابقاً [30].

2-5-2. أنواع مولّدات الأرقام العشوائية

هناك نوعان أساسيان من المولّدات المستخدمة لإنتاج السلاسل العشوائية: مولّدات الأرقام العشوائية (Random Number Generators RNGs)، ومولّدات الأرقام شبه العشوائية (Pseudo Random Number Generators PRNGs). يُنتج كلا النوعين سلسلة من الأصفار والواحدات يمكن تقسيمها إلى سلاسل فرعية أو كتل من الأرقام العشوائية [30].

2-5-2. 1. مولّدات الأرقام العشوائية

يستخدم RNG مصدراً غير حتمي (أي مصدراً إنتروبياً)؛ جنباً إلى جنب مع بعض عمليات المعالجة لإنتاج العشوائية. يمكن تعريف مصدر الإنتروبية على أنه مصدر مادي للمعلومات، تكون مخرجاته إما عشوائية في حد ذاتها أو يمكن جعلها عشوائية بتطبيق بعض عمليات المعالجة. تُستخدم عمليات المعالجة للتغلب على أي ضعف في مصدر الإنتروبية الذي قد ينتج عنه أرقام غير عشوائية. يتكون مصدر الإنتروبية عادةً من بعض القيم الفيزيائية، مثل الضجيج في الدارة الكهربائية، وتوقيت عمليات المستخدم كحركات فأرة الحاسوب، أو التأثيرات الكمومية في أنصاف النواقل [30].

يمكن استخدام مخرجات RNG مباشرة كرقم عشوائي أو يمكن استخدامها كمداخلات لمولد الأرقام شبه العشوائية. لاستخدام مخرجات RNG مباشرة، يجب أن يفي ناتج RNG بمعايير صارمة تُقاس بالاختبارات الإحصائية من أجل التأكد من عشوائية المصادر الفيزيائية التي تُستخدم كمداخلات RNG. على سبيل المثال، قد يحتوي مصدراً فيزيائياً ما على تراكيب لبنى نمطية، والذي قد يبدو عشوائياً، ولكن يُثبت أنه غير عشوائي لدى اختباره باستخدام الاختبارات الإحصائية [30].

قد تكون المخرجات الناتجة عن RNG ضعيفة العشوائية عند تقييمها بالاختبارات الإحصائية. فضلاً عن ذلك، قد يستغرق إنتاج أرقام عشوائية عالية الجودة وقتاً طويلاً للغاية؛ مما يجعل استخدام RNG غير مرغوب فيه عند الحاجة إلى كمية كبيرة من الأرقام العشوائية. لإنتاج كميات كبيرة من الأرقام العشوائية، قد تكون مولّدات الأرقام شبه العشوائية هي الأفضل [30].

2-5-2. 2. مولّدات الأرقام شبه العشوائية

يستخدم PRNG مُدخلًا واحدًا أو أكثر ويولد أرقاماً متعددة شبه عشوائية. تسمى مدخلات PRNG البذور (seeds) والتي يجب أن تكون عشوائية وغير متوقعة. وبالتالي، يجب أن يحصل PRNG على بذوره من مخرجات RNG؛ أي يتطلب PRNG وجود RNG مرافق. لضمان عدم القدرة على التنبؤ بمخرجات PRNG، يجب توخي الحذر في طريقة الحصول على البذور [30].

عادةً ما تكون مخرجات PRNG توابع حتمية للبذرة؛ أي إن العشوائية الحقيقية تقتصر على توليد البذور عشوائياً. تؤدي الطبيعة الحتمية لعملية التوليد إلى مصطلح "شبه عشوائي"؛ نظراً لأن كل عنصر في سلسلة شبه عشوائية يمكن استنتاجه من بذرته. ومن المفارقات أن الأرقام شبه العشوائية غالباً ما تبدو عشوائية أكثر من الأرقام العشوائية التي يتم الحصول عليها من المصادر الفيزيائية. من أجل إنتاج سلسلة شبه عشوائية بشكل صحيح، يتم إنتاج كل قيمة في السلسلة من القيمة السابقة باستخدام تحويلات تقدّم عشوائية إضافية. يمكن لسلسلة من هذه التحويلات القضاء على الارتباطات الإحصائية بين المدخلات والمخرجات. ومن ثم، قد يكون لمخرجات PRNG خصائص إحصائية أفضل وتُنتج بشكل أسرع من إنتاج RNG [30].

2-5-3. اختبارات العشوائية

في تطبيقات حماية المعلومات، يجب أن تكون الأرقام العشوائية وشبه العشوائية المُستخدمة غير متوقعة. يمكن تطبيق اختبارات إحصائية مختلفة على سلسلة ما لمحاولة تقييمها ومقارنتها بسلسلة عشوائية حقيقية. فالعشوائية هي خاصية احتمالية. بمعنى أن خصائص السلسلة العشوائية يمكن تحديدها وتوصيفها من خلال المصطلحات الاحتمالية. تكون نتيجة الاختبارات الإحصائية، عند تطبيقها على سلسلة عشوائية حقيقية، معروفة مسبقاً ويمكن وصفها بمصطلحات احتمالية. هناك عدد لا حصر له من الاختبارات الإحصائية الممكن إجراؤها. كلٌ منها يقيّم وجود نمط (pattern) أو عدم وجوده، والذي، إذا اكتُشف وجوده، يشير إلى أن السلسلة غير عشوائية. ونظراً إلى أن هناك العديد من الاختبارات للحكم فيما إذا كانت سلسلة ما عشوائية أم لا، لا يمكن اعتبار أن مجموعة محددة من الاختبارات "كاملة". بالإضافة إلى ذلك، يجب تفسير نتائج الاختبار الإحصائي بعناية وحذر لتجنب الاستنتاجات الخاطئة حول مولّد معين [30].

في مجموعة الاختبارات الإحصائية المقدّمة من قِبل المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standards and Technology NIST) في [30]، تمت صياغة الاختبارات الإحصائية بحيث تقوم باختبار فرضية العدم (null hypothesis) والتي نرمز لها H_0 . في [30]، تعني فرضية العدم أن السلسلة التي يتم اختبارها عشوائية. هناك فرضية أخرى مقترنة بفرضية العدم وهي الفرضية البديلة (alternative hypothesis) والتي نرمز لها H_a ، وهي تعني أن السلسلة ليست عشوائية. لدى إجراء كل اختبار، يتم استنباط قرار إما قبول فرضية العدم أو رفضها، أي استنتاج ما إذا كان المولّد جيّداً (يُنتج قيماً عشوائية) أم لا، وذلك بناءً على السلاسل التي يُنتجها والتي يتم اختبارها.

من أجل كل اختبار، يجب اختيار إحصاءات العشوائية (Randomness Statistics) المُعتمدة واستخدامها لتحديد قبول أو رفض افتراض عشوائية السلسلة المُختبرة. في ظل افتراض العشوائية، فإن مثل هذه الإحصاءات يكون لها توزّع محدّد للقيم الاحتمالية. يُحدّد التوزّع المرجعي النظري لهذه الإحصاءات في ظل افتراض العشوائية بالطرائق الرياضية. وتُحدّد قيمة حرجة (critical value) اعتباراً من التوزّع المرجعي؛ عادةً ما تكون تلك القيمة

في نهايات التوزيع، ولتكن عند النقطة 99%. في أثناء الاختبار، تُحسب القيمة الإحصائية للاختبار من أجل السلسلة المختبرة. تُقارن القيمة الناتجة بالقيمة الحرجة، فإذا تجاوزت القيمة الناتجة عن الاختبار القيمة الحرجة، يُرفض افتراض عشوائية السلسلة المختبرة. خلافاً لذلك، تُقبل فرضية العشوائية [30].

من الناحية العملية، فإن السبب وراء نجاح اختبار الفرضيات الإحصائية هو أن التوزيع المرجعي والقيمة الحرجة يعتمدان على الافتراض المؤقت للعشوائية. إذا كان افتراض العشوائية صحيحاً بالنسبة للبيانات المُختبرة، يكون احتمال تجاوز القيمة الإحصائية الناتجة عن الاختبار للقيمة الحرجة منخفضاً جداً (على سبيل المثال، 0.01%). من ناحية أخرى، إذا تجاوزت القيمة الإحصائية الناتجة عن الاختبار القيمة الحرجة (أي إذا وقع الحدث ذو الاحتمال المنخفض)، يُستنتج أن افتراض عشوائية السلسلة المختبرة مشكوك فيه أو خاطئ. في هذه الحالة، يُنتج عن الاختبار الاستنتاجات التالية: رفض H_0 (رفض العشوائية) وقبول H_a (قبول عدم العشوائية) [30].

الجدول 1-2: الربط بين الحالة الحقيقية للعشوائية مع النتائج المستخلصة من الاختبار [30].

الخلاصة		الحالة الحقيقية
قبول H_0	قبول H_a (رفض H_0)	
لا يوجد خطأ	خطأ من النمط I	البيانات عشوائية (H_0 صحيحة)
خطأ من النمط II	لا يوجد خطأ	البيانات ليست عشوائية (H_a صحيحة)

اختبار الفرضية الإحصائية هو طريقة لتوليد استنتاج واحد من أصل استنتاجين مُحتمَلين، إما قبول فرضية العدم H_0 (أي أن البيانات عشوائية)، أو قبول الفرضية البديلة H_a (أي أن البيانات غير عشوائية). يربط الجدول 1-2 بين الحالة الحقيقية لعشوائية البيانات والنتيجة التي تم التوصل إليها باستخدام الاختبار. إذا كانت البيانات عشوائية في الحقيقة، فإن استنتاج رفض فرضية العدم H_0 (أي استنتاج أن البيانات غير عشوائية) سيحدث عدداً قليلاً من المرات، أي بنسبة مئوية منخفضة. هذا الاستنتاج يُسمى خطأ من النمط I. إذا كانت البيانات غير عشوائية في الحقيقة، فإن استنتاج قبول فرضية العدم H_0 (أي استنتاج أن البيانات عشوائية) يُسمى خطأ من النمط II. إن استنتاج قبول H_0 عندما تكون البيانات عشوائية حقاً، واستنتاج رفض H_0 عندما تكون البيانات غير عشوائية، هي الاستنتاجات الصحيحة [30].

يُطلق على احتمال حدوث خطأ من النمط I، مستوى دلالة الاختبار (Level of significance). يمكن تعيين قيمة هذا الاحتمال قبل بدء الاختبار ويُشار إليه بالرمز α . بالتالي، α هي احتمال أن يشير الاختبار إلى أن السلسلة ليست عشوائية عندما تكون السلسلة عشوائية بالفعل. أي، تُظهر السلسلة خصائص غير عشوائية حتى عندما يتم إنتاجها من قبل مولّد سلاسل عشوائية جيّد. تكون قيمة α المتعارف عليها في تطبيقات التشفير حوالي 0.01 [30].

يُشار إلى احتمال حدوث خطأ من النمط II بالرمز β . بالتالي، β هي احتمال أن يشير الاختبار إلى أن السلسلة عشوائية عندما تكون غير عشوائية؛ أي أن المولّد السيئ قد أنتج سلسلة تُظهر خصائص عشوائية. على عكس α ، فإن β ليست ثابتة ويمكن أن تأخذ العديد من القيم المختلفة نظراً لوجود عدد لا حصر له من الطرق التي يمكن أن تولّد تدفقاً غير عشوائي، وكل طريقة مختلفة ينتج عنها β مختلفة. يُعدّ حساب β أكثر صعوبة من حساب α ؛ بسبب الأنواع العديدة الممكنة من عدم العشوائية [30].

يتمثل أحد الأهداف الأساسية لاختبارات NIST في تقليل احتمال حدوث خطأ من النمط II، أي تقليل احتمال افتراض عشوائية سلسلة يتم إنتاجها بواسطة مولّد سيئ بالحقبة. ترتبط الاحتمالات α و β بعضها مع بعض، ومع طول السلسلة المُختبرة n بحيث إذا تم تحديد قيمة اثنين منهم، يتم تحديد القيمة الثالثة تلقائياً. عادةً ما يتم تحديد طول العيّنة المُختبرة n وقيمة α ، ثم يتم تحديد النقطة الحرجة والتي ستنتج أصغر قيمة مقابلة لـ β . أي يتم اختيار حجم عيّنة مناسب بالإضافة إلى اختيار احتمال مقبول لإقرار أن مولّداً سيئاً قد أنتج سلسلة عشوائية بالفعل، ثم يتم اختيار الحد الفاصل لقبول العشوائية، بحيث يكون احتمال قبول سلسلة غير عشوائية على أنها عشوائية أصغر ما يمكن [30].

يَنبُج عن كل اختبار قيمة إحصائية تابعة للبيانات المُختبرة، رمزها P ، والتي تلخّص قوة الدليل ضد فرضية العدم. بالنسبة لاختبارات NIST، فإن كل قيمة P هي احتمال أن يَنبُج عن مولّد سلاسل عشوائية مثالي سلسلة أقل عشوائيةً من المطلوب، وذلك بناءً على نوع عدم العشوائية الذي يقوم الاختبار بتقييمه. إذا كانت قيمة P الناتجة عن الاختبار تساوي 1، فإن السلسلة المُختبرة تبدو أنها عشوائية بشكل كامل. إذا كانت قيمة P تساوي 0،

فإن السلسلة يبدو أنها غير عشوائي تماماً. يمكن اختيار مستوى الأهمية (α) للاختبارات بحيث إذا كانت $P \geq \alpha$ ، يتم قبول فرضية العدم؛ أي يبدو أن السلسلة عشوائية. إذا كانت $P < \alpha$ ، فسيتم رفض فرضية العدم؛ أي يبدو أن السلسلة غير عشوائية. يتم عادةً اختيار α ضمن المجال $[0.01, 0.001]$. على سبيل المثال، تشير قيمة α المساوية 0.01 إلى أنه يمكن توقع رفض عشوائية سلسلة واحدة من أصل 100 سلسلة ناتجة عن مولد سلاسل عشوائية جيد. تعني القيمة $P \geq 0.01$ أن السلسلة ستُعتبر عشوائية بثقة تبلغ 99%. وتعني القيمة $P < 0.01$ أن السلسلة غير عشوائية بثقة 99% [30].

بشكل عام، يتم وضع الافتراضات التالية فيما يتعلق بالسلاسل الثنائية العشوائية التي سيتم اختبارها [30]:

- أن يكون حدث ظهور الصفر (0) أو الواحد (1) متساوٍ في أي مرحلة من مراحل توليد سلسلة البتات العشوائية. أي أن يكون احتمال ظهور كل من الصفر أو الواحد هو $1/2$ بالضبط. وبالتالي، العدد المتوقع للأصفار (أو الواحدات) في سلسلة طولها n bit هو $n/2$.
- يجب أن يملك الاختبار قابلية التوسع، بمعنى أن أي اختبار يكون قابلاً للتطبيق على سلسلة ما يجب أن يكون قابلاً للتطبيق على السلاسل الفرعية الناتجة عنها. إذا كانت السلسلة عشوائية، فيجب أن تكون أي سلسلة فرعية ناتجة عنها عشوائية أيضاً، وبالتالي فيجب أن تتجاوز أي سلسلة فرعية اختبارات العشوائية أيضاً.
- يجب أن يكون سلوك المولد ثابتاً. بالتالي، لا يكفي اختبار RNG بالنسبة للسلاسل المولدة من سلسلة قيم فيزيائي واحدة فقط.

2-3-1. مجموعة اختبارات NIST الإحصائية

هي مجموعة من اختبارات العشوائية وَصَّعَهَا المعهد الوطني للمعايير والتكنولوجيا (NIST)، يتم من خلالها كشف انحرافات السلسلة الثنائية عن العشوائية. ينصب تركيز مجموعة الاختبار هذه على فحص عشوائية السلاسل المستخدمة لأغراض التعمية [30].

تتكون مجموعة اختبارات NIST من خمسة عشر اختباراً. تركز هذه الاختبارات على مجموعة متنوعة من الأنماط المختلفة التي يمكن أن توجد في تسلسل بتات معين. بالنسبة لعددٍ من الاختبارات في مجموعة الاختبار هذه، تم افتراض أن طول السلسلة العشوائية، n ، كبير (من مرتبة 10^3 bit إلى 10^7 bit). معظم الاختبارات قابلة للتطبيق من أجل سلاسل أطوالها أقل من ذلك. فيما يأتي نعرض لمحة مبسطة عن كل اختبار (لمزيد من التفاصيل حول أهداف وتوصيف كل اختبار، وموسطاته، وشروط تطبيقه يمكن العودة إلى المرجع [30]):

اختبار التردد (Frequency Test): يركز هذا الاختبار على نسبة الأصفار والواحدات التي تظهر في السلسلة المختبرة. الغرض منه تحديد فيما إذا كان عدد الواحدات والأصفار في السلسلة متماثلاً تقريباً. يعتمد اجتياز جميع الاختبارات اللاحقة على اجتياز هذا الاختبار.

اختبار التردد ضمن الكتلة (Frequency Test within a Block): يركز هذا الاختبار على نسبة الواحدات الموجودة داخل كتل طولها M -bit. الغرض من هذا الاختبار هو تحديد ما إذا كان تردد الواحدات في سلسلة جزئية طولها M -bit يقارب $M/2$ ، كما هو متوقع في ظل افتراض العشوائية.

اختبار سلاسل البتات المتماثلة المتتالية (Runs Test): يركز هذا الاختبار على العدد الإجمالي لسلاسل البتات المتماثلة المتتالية في السلسلة المختبرة (أي التسلسل غير المنقطع من البتات المتطابقة) والتي تدعى Runs. الغرض من هذا الاختبار هو تحديد ما إذا كان عدد تلك السلاسل (Runs) بأطوال مختلفة مناسب لسلسلة عشوائية.

اختبار أطول سلسلة واحداث متتالية ضمن الكتلة (Test for the Longest Run of Ones in a Block): يركز هذا الاختبار على إيجاد أطول سلسلة Run مكونة من الواحدات داخل كتل طولها M -bit. الغرض من هذا الاختبار هو تحديد ما إذا كان طول أطول Run من الواحدات ضمن السلسلة المختبرة يتوافق مع طول أطول Run يمكن توقعها في سلسلة عشوائية.

اختبار رتبة المصفوفة الثنائية (Binary Matrix Rank Test): ينصب تركيز هذا الاختبار على رتبة (rank) المصفوفات الجزئية المنفصلة (disjoint sub-matrices) للسلسلة بأكملها. الغرض من هذا الاختبار هو التحقق من الارتباط الخطي بين السلاسل الجزئية ذات الطول المحدد من السلسلة الأصلية.

اختبار تحويل فورييه المتقطع (Discrete Fourier Transform Test): يركز هذا الاختبار على قيم الترددات العظمى في تحويل فورييه المتقطع للسلسلة المختبرة. الغرض من هذا الاختبار هو اكتشاف الميزات الدورية (أي الأنماط المتكررة القريبة من بعضها بعضاً) في السلسلة المختبرة.

اختبار مطابقة القوالب غير المتداخلة (Non-overlapping Template Matching Test): يركز هذا الاختبار على عدد تكرارات السلاسل المستهدفة المحددة مسبقاً. الغرض من هذا الاختبار هو اكتشاف المولدات التي تُنتج عدداً كبيراً من التكرارات لنمط غير دوري. بالنسبة لهذا الاختبار، تُستخدم نافذة حجمها m -bit للبحث عن نمط محدد طوله m -bit أيضاً. إذا لم يُعثر على النمط، فإن النافذة تنزلق بمقدار bit واحد. أما إذا عُثر على النمط، يُعاد تعيين النافذة وتُزاح إلى الجزء الذي يلي النمط الذي تم العثور عليه، ويُستأنف البحث.

اختبار مطابقة القوالب المتداخلة (Overlapping Template Matching Test): يركز هذا الاختبار على عدد مرات ظهور السلاسل المستهدفة المحددة مسبقاً. يستخدم هذا الاختبار نافذة m -bit للبحث عن نمط محدد طوله m -bit. إذا لم يُعثر على النمط، تنزلق النافذة بمقدار bit واحد. الفرق بين هذا الاختبار والاختبار السابق هو أنه عند العثور على النمط، تنزلق النافذة بمقدار bit واحد قبل استئناف البحث.

اختبار الإحصاء العام (Universal Statistical Test): الغرض من هذا الاختبار هو اكتشاف فيما إذا كان من الممكن ضغط السلسلة المختبرة بشكل كبير من دون فقدان المعلومات. تُعدّ السلسلة القابلة للضغط بشكل كبير غير عشوائية.

اختبار التعقيد الخطي (Linear Complexity Test): يعتمد هذا الاختبار على طول سجل الإزاحة ذو التغذية الخلفية الخطية (linear feedback shift register LFSR). الغرض من هذا الاختبار هو تحديد ما إذا كانت السلسلة معقدة بدرجة كافية ليتم اعتبارها عشوائية أم لا. تتميز السلاسل العشوائية بأن LFSR يكون طويلاً. يشير LFSR القصير جداً إلى عدم العشوائية.

الاختبار التسلسلي (Serial Test): يركز هذا الاختبار على تردد ظهور نماذج البتات المتداخلة ذات طول m -bit عبر السلسلة بأكملها. الغرض من هذا الاختبار هو تحديد ما إذا كان عدد تكرارات 2^m سلسلة متداخلة

ذات طول m -bit هو مناسب للتسلسل العشوائي. يجب أن يكون لكل نمط m -bit في السلاسل العشوائية فرصة الظهور نفسها.

اختبار الإنتروبية التقريبية (Approximate Entropy Test): ينصب تركيز هذا الاختبار على تردد ظهور جميع الأنماط المتداخلة الممكنة ذات طول m -bit عبر السلسلة بأكملها. الغرض من الاختبار هو مقارنة تردد ظهور الكتل المتداخلة بطولين متعاقبين $(m, m+1)$ مع التردد المتوقع لسلسلة عشوائية.

اختبار المجاميع التراكمية (Cumulative Sums Test): يركز هذا الاختبار على قيمة الانحراف الأعظمي عن الصفر للسلسلة المختبرة والذي يمكن تحديده بالمجموع التراكمي لعناصر السلسلة (البتات) بعد تقييسها لتأخذ القيم $(-1, +1)$. الغرض من الاختبار هو تحديد ما إذا كان المجموع التراكمي لعناصر السلاسل الجزئية في السلسلة المُختَبَرَة كبيراً جداً أو صغيراً جداً بالنسبة للسلوك المتوقع للسلاسل العشوائية. بالنسبة للسلسلة العشوائية، يجب أن تكون تلك القيم قريبة من الصفر.

اختبار انحرافات العشوائية (Random Excursions Test): الغرض من هذا الاختبار هو تحديد ما إذا كان عدد مرات ورود حالة معينة داخل دورة اختبار ما ينحرف عما يجب أن يكون بالنسبة لسلسلة عشوائية. هذا الاختبار هو سلسلة من ثمانية اختبارات.

اختبار متغير انحرافات العشوائية (Random Excursions Variant Test): يركز هذا الاختبار على إجمالي عدد المرات التي يُعْتَر فيها على حالة معينة في مسيرة عشوائية تراكمية. الغرض من هذا الاختبار هو اكتشاف الانحرافات عن العدد المتوقع من أجل سلسلة عشوائية. هذا الاختبار هو سلسلة من ثمانية عشر اختباراً.

2-3-5. برنامج اختبار سلاسل الأرقام شبه العشوائية ENT

برنامج اختبار سلاسل الأرقام شبه العشوائية ENT (ENT A Pseudorandom Number Sequence Test) هو برنامج يقوم بتطبيق اختبارات مختلفة على سلاسل البايتات المخزنة في الملفات لفحص عشوائيتها. يُعَدُّ هذا البرنامج مفيداً في تقييم مولّدات الأرقام شبه العشوائية لتطبيقات أخذ العينات الإحصائية وخوارزميات الضغط والتطبيقات الأخرى التي تكون فيها كثافة معلومات الملف ذات أهمية. وهو مكون من ستة اختبارات [90].

مجموعة ENT، غير مخصصة لتطبيقات التعمية، وهي واحدة من الاختبارات التي تُستخدَم عادةً في بداية فحص العشوائية لتجاهل المولدات الضعيفة من دون الحاجة إلى اختبارات إضافية [91].

2-3-3. مجموعة اختبار Diehard

مجموعة اختبار Diehard (Diehard test suite)، هي عبارة عن مجموعة اختبارات لاختبار مولّدات الأرقام العشوائية. الغرض منها هو اختبار المولّدات، وليس الملفات ذات المحتوى العشوائي. هذا الاختبار دقيق للغاية. يتمثل الهدف الإضافي لتصميمه في توفير بعض المؤشرات عن سبب فشل المولّد في الاختبار، حيث يمكن استخراج هذه المعلومات في أثناء عملية الاختبار [92]. وهو مكون من خمسة عشر اختباراً.

2-6- خاتمة

في ختام هذا الفصل، وبعد أن درسنا المفاهيم الأساسية حول التعمية، وتبادل المفاتيح المصادق عليها، وتوليد السلاسل العشوائية واختبارها؛ يمكننا أن نستنتج أن التعمية المتناظرة وبالتحديد خوارزمية TEA، هي الأبسط والأقل استهلاكاً للموارد، ولكن يجب تحسينها بحيث تصبح منيعة ضد الهجمات التي تتعرض لها. كما يمكننا أن نستنتج أيضاً، أن مصادقة الكيانات المتصلة بعضها مع بعض يمكن تحقيقه من خلال عملية تبادل المفاتيح المصادق عليها. أما بما يتعلق بتوليد السلاسل العشوائية، فبينما أنه لا بد من إخضاع السلاسل الناتجة عن مولّدات الأرقام العشوائية للاختبارات الإحصائية للتحقق من عشوائيتها.

في الفصل القادم، نُقدّم ملخصاً حول الدراسات السابقة التي طُبِّقَت فيها المفاهيم النظرية الواردة في الفصلين الأول والثاني، والتي تسعى لتحقيق حماية شبكات WBAN بالاعتماد على القيم الحيوية وبالتحديد إشارة ECG.

الفصل الثالث

الدراسة المرجعية

1-3- تمهيد	76
2-3- الدراسات السابقة حول توليد المفاتيح في WBAN بالاعتماد على القيم الحيوية	76
3-3- تحليل نتائج الدراسات السابقة في توليد المفاتيح الحيوية ومناقشتها	86
1-3-3. مقارنة بين مخططات تبادل المفاتيح المعتمدة على ECG الواردة في الدراسات السابقة	86
2-3-3. الشروط الواجب توافرها في خوارزمية تبادل المفاتيح المعتمدة على ECG	87
3-3-3. عدم الكفاية في الدراسات السابقة حول توليد المفاتيح وتبادلها بالاعتماد على ECG	88
4-3- الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على القيم الحيوية	90
5-3- تحليل الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على القيم الحيوية ومناقشتها	92
1-5-3. مقارنة بين الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على ECG	93
2-5-3. عدم الكفاية في الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على ECG	94
6-3- الدراسات السابقة حول تعمية البيانات في شبكات WBAN	94
7-3- تحليل الدراسات السابقة في تعمية البيانات في WBAN ومناقشتها	97
8-3- خاتمة	97

3-1- تمهيد

نُقدّم في هذا الفصل ملخصاً عن الدراسات السابقة في حماية شبكات WBAN بالاعتماد على إشارة ECG بما في ذلك توليد المفاتيح السرية المصادق عليها وتبادلها، وتوليد السلاسل العشوائية، والتعمية. ثم ندرج دراسة تحليلية ومناقشة لتلك الدراسات السابقة؛ تتضمن المقارنة فيما بينها، وإظهار مواضع عدم الكفاية في كلّ منها.

3-2- الدراسات السابقة حول توليد المفاتيح في WBAN بالاعتماد على القيم الحيوية

من أجل تلبية متطلبات حماية شبكات WBAN، اقترحت الدراسات السابقة عدداً من مخططات الحماية القائمة على التعمية. بشكل عام، تعتمد فعالية تلك المخططات القائمة على التعمية إلى حد كبير على الطريقة المتبعة لإدارة المفاتيح [7]. تُشكل عملية إدارة المفاتيح، بما فيها من الطرائق اللازمة لإنشاء المفاتيح السرية المشتركة وتبادلها بين عقد الحساسات إحدى التحديات الكبيرة في تصميم مخططات حماية WBAN [14]. اقترحت بعض الدراسات توزيع المفاتيح السرية بشكل مسبق على الحساسات، أي قبل بداية تشغيل الشبكة. تكمن المشكلة الرئيسة في التوزيع المسبق للمفاتيح في استخدام نفس المفاتيح لفترات زمنية طويلة؛ مما قد يعرضها لهجمات تحليل التعمية، ومن ثمّ الفضح [19]. كما أن استخدام الطرق التقليدية في تبادل المفاتيح لا يتناسب مع محدودية موارد حساسات WBAN، فمعظمها يعتمد مبادئ التعمية غير المتناظرة المكلفة للغاية [20].

لحل المشاكل المذكورة للتو، تُستخدم البيانات الحيوية التي يتم تحصيلها بوساطة حساسات WBAN من أجل استخراج مفتاح التعمية، أو من أجل تبادله والاتفاق عليه [7]، [93]. يُطلق على المفتاح المُستخرج من القيم الحيوية اسم المفتاح الحيوي (Biometric key) [7]، [93]. تأتي فكرة استخدام خصائص الإشارات الحيوية في توليد المفتاح والاتفاق عليه، من ملاحظة أن جسم الإنسان ديناميكي ومعقد، وأن الحالة الفيزيولوجية للجسم فريدة تماماً في لحظة معينة [13]. في مخططات تبادل المفاتيح المعتمدة على القيم الحيوية، تُحصّل الحساسات الإشارات الحيوية ثم تُعالجها لاستخراج الخصائص التي ستُستخدم لتحقيق عملية توليد المفاتيح، والاتفاق عليها، وإدارتها، ومصادقتها أيضاً [7]. يمكن الاستفادة من تشابه تلك الخصائص عند قياسها بشكل متزامن في حساسات عدة موضوعة على الجسم نفسه، أي تلك التي تنتمي إلى شبكة WBAN نفسها [94]، [95].

إن استخدام الإشارات الحيوية يقضي على الحاجة إلى التوزيع الصريح للمفاتيح، والذي يهدد أمان الشبكة، كما يسمح للحساسات بالاتفاق على المفاتيح عند الحاجة؛ أي تغييرها بشكل ديناميكي [13]. إن استخدام الخصائص الحيوية لن يزيد من الأمان والخصوصية فحسب؛ بل يزيد أيضاً من فعالية شبكة WBAN ويقلل من استهلاك الموارد الناتج عن تطبيق الطرق التقليدية لتبادل المفاتيح المعتمدة على التعمية غير المتناظرة [28].

تُظهر القيم الحيوية خصائص عشوائية كافية يمكن استخدامها لتوليد مفاتيح التعمية. وهناك سببان أساسيان لتفضيل المفتاح الحيوي عن المفتاح الناتج عن مولّدات الأرقام شبه العشوائية: أولاً، تتطلب مولّدات الأرقام شبه العشوائية حسابات ثقيلة، مقارنةً بطرق توليد المفاتيح الناتجة عن القيم الحيوية. ثانياً، تتصف القيم العشوائية الناتجة عن الإشارات الحيوية بأنها مستقلة عن بعضها بعضاً، ومن ثم تكون المفاتيح الحيوية الناتجة أيضاً مستقلة عن بعضها. أما مولّدات الأرقام شبه العشوائية، تستخدم خوارزمية رياضية وبذور من أجل توليد الأرقام العشوائية. إذا كُشِفَت الخوارزمية والبذور، يصبح تسلسل الأرقام العشوائية الناتجة مكشوفاً أيضاً [19]، [30]. وبحسب [13]، تُستخدَم الإشارات الحيوية من أجل توليد المفاتيح وتبادلها للأسباب الآتية:

- الطول والعشوائية: تتمتع الإشارات الحيوية بالطول والعشوائية ومن ثم يمكن للمفاتيح المتفق عليها أن تكون أيضاً طويلة، وعشوائية لمنع هجوم البحث الشامل (Brute force attack).
- زمن الاستجابة المنخفض: الزمن اللازم لتحصيل الإشارة الحيوية المطلوبة صغير.
- التميز (distinctiveness): تختلف الإشارة الحيوية من شخصٍ لآخر. ومن ثم فإن معرفة الخصائص المشتقة من الإشارة الحيوية لجسم معين، لن تسمح بتخمين الخصائص المشتقة من جسم آخر. ومن السمات المهمة للمفتاح المبني على الإشارات الحيوية أنه يحقق المصادقة بين الحساسات المتصلة. وبالتالي يضمن عدم إمكانية الاتفاق على المفتاح السري المشترك إلا من قبل حساسات تنتمي إلى شبكة WBAN نفسها، أي موضوعة على الجسم نفسه.

- التباين الزمني (Temporal variance): أي اختلاف قيم الإشارات الحيوية من لحظةٍ إلى أخرى. بالتالي فإن معرفة الإشارات الحيوية في لحظة معينة لن يساعد على معرفة المفاتيح التي سيُتفق عليها في العمليات المستقبلية لتبادل المفاتيح.

تركز جميع الأعمال السابقة في مجال توليد المفاتيح وتبادلها بالاعتماد على القياسات الحيوية على الاستفادة من تشابه القيم الحيوية المقاسة بشكل متزامن في حساسات عدة موضوعة على الجسم نفسه، وتجاوز العقبات الناتجة عن الاختلافات الطفيفة بين تلك القيم [7]، [96]. استخدم معظم الباحثين إشارة ECG، لبناء مخططاتهم.

في WBAN، ليس من السهل تطبيق التعمية المتناظرة التقليدية باستخدام المفاتيح المكوّنة من الإشارات الحيوية بشكل مباشر؛ وذلك بسبب الضجيج الذي تتعرض له تلك الإشارات والذي يؤدي إلى عدم التطابق بين المفاتيح الحيويين المُتَشَكِّلِينَ بين طرفي التعمية (الحساسين الموضوعين على نفس الجسم، أي المُنتَمِينَ إلى نفس شبكة WBAN). في التعمية المتناظرة التقليدية، مهما كان الاختلاف صغيراً (على سبيل المثال bit واحد فقط) بين مفتاح التعمية ومفتاح فك التعمية فهو يكفي لفشل عملية فك التعمية. لمواجهة هذه المشكلة، من الممكن توظيف طرق قويّة للغاية لتصحيح الأخطاء واستخدام بروتوكولات إعادة إرسال الطلّب؛ ولكن سيؤدي ذلك إلى زيادة كبيرة في التعقيد واستهلاك كبير جداً لطاقة الحساسات. قد يكون البديل الأكثر فاعليّةً هو استخدام مخطط تشفير مُصمّم بطبيعته لتصحيح الاختلافات بين المفاتيح، وممثّل على ذلك، مخطط القبو الغامض (Fuzzy Vault).

القبو الغامض هو نمط تعمية متسامح مع الأخطاء، يَعمَدُ على التشابه بين مجموعتين سريّتين يتم تشكيل كلٍّ منهما في أحد طرفي التعمية [97]. لشرح مبادئ القبو الغامض، نفرض أن هناك طرفي اتصال وهما Alice و Bob يريدان تبادل قيمة سرية ما ولكن k . تقوم Alice بوضع القيمة السريّة k في القبو الغامض وقفلها باستخدام مجموعة من العناصر ولتكن A ، وهي مجموعة مختارة من المجموعة العامّة U . لكي يتمكن Bob من التوصل إلى القيمة السرية k ، يُحاول فك قفل القبو الغامض باستخدام المجموعة B وهي مجموعة ذات طول مماثل لطول

المجموعة A ، وهي مختارة أيضاً من المجموعة العامة U . يستطيع Bob أن يتوصل إلى قيمة k إذا كانت المجموعتان A و B متقاطعتان بشكل كبير [97].

يمكن تطبيق مبادئ القبو الغامض عملياً باستخدام كثيرات الحدود. لكي تخفي Alice القيمة السرية k باستخدام المجموعة A ، تقوم بتشكيل كثير حدود p بمتحول وحيد x ، بحيث يقوم p بتشفير k بطريقة ما. على سبيل المثال، يمكن تضمين k من خلال معاملات كثير الحدود p . تقوم Alice بحساب ناتج تطبيق التابع p على كل عنصر من عناصر A (يمثل كل عنصر من عناصر A قيمة المتحول x)، أي تقوم Alice بإسقاط كافة عناصر A على نقاط تقع على كثير الحدود p ومن ثم تُشكّل المجموعة $R = \{(a_i, p(a_i))\}$ ، حيث i هي دليل العنصر من المجموعة A . بعد ذلك تولّد Alice مجموعة نقاط عشوائية نسميها نقاط الضجيج، وهي نقاط لا تقع على p ، ونُضيفها إلى المجموعة R . بالتالي تكون وظيفة R إخفاء p عن المهاجم. عندما يستقبل Bob المجموعة R يُشكّل المجموعة Q وهي مجموعة جزئية من R بحيث $Q = \{(u, v) : (u, v) \in R \ \& \ u \in B\}$ أي تكون فيها قيمة u بالنسبة لكل نقطة مساويةً لإحدى قيم عناصر B . من ثم يستطيع Bob أن يتكشف العديد من نقاط R التي تقع على p ، ولكن قد تتضمن المجموعة المُكتشفة من قبل Bob القليل من نقاط الضجيج. باستخدام توابع تصحيح الأخطاء مثل BCH أو Reed-Solomon يصبح Bob قادراً على إعادة بناء p بشكل دقيق؛ وبالتالي التوصل إلى k . أمّا إذا كانت B لا تتقاطع بشكل كافٍ مع A ؛ بالتالي يكون من غير المجدي لـ Bob أن يحصل على k وذلك بسبب وجود العديد من نقاط الضجيج ضمن المجموعة المُكتشفة [13]، [97].

تعتمد قوة هذه الخوارزمية على مسألة إعادة بناء كثير الحدود، بالتالي يتطلب تطبيقها قدرات حسابية عالية جداً، وذلك يشكّل عائقاً أمام تطبيقها ضمن حساسات WBAN ضعيفة الموارد.

في [20] اقترح الباحثون طريقتين لتبادل المفاتيح الحيوية، الأولى، هي: الإدارة القائمة للمفتاح أحادية النقطة (Single-point Fuzzy Key Management). في هذه الطريقة، يتم إنشاء مفتاح تعمية سري مشترك بين كافة حساسات الشبكة وذلك في أحد الحساسات، ثم يُوزع المفتاح الناتج على بقية حساسات الشبكة. استُخدمت قيم IPI كخصائص حيوية مشتركة بين الحساسات؛ وذلك من أجل تبادل المفاتيح فقط، وليس من أجل إنشائها. طالما

أن قيمة IPI المُشتقة من الحساس المرسل مشابهة بدرجة كافية لقيمة IPI المُشتقة من الحساس المستقبل، يجب أن ينجح تبادل المفاتيح. ويمكن تلخيص هذه الطريقة وفق الآتي. لتكن r هي تسلسل IPI المُشتق من إشارة ECG المقاسة في الحساس المرسل و u هي التمثيل الثنائي لها. ولتكن r' هي تسلسل IPI المُشتق من إشارة ECG نفسها ولكن المقاسة في الحساس المُستقبل بالتزامن مع الحساس المرسل و u' هي التمثيل الثنائي لها. وليكن k_{session} مفتاح سري مولّد في الحساس المرسل باستخدام مولّد أرقام عشوائية، وهو الذي نريد إرساله إلى الحساس المُستقبل بشكل آمن. يُشترط أن يكون k_{session} مساوٍ لإحدى كلمات رماز تصحيح الأخطاء المُستخدَم في هذه الطريقة. وليكن k' هو المفتاح الذي سيتم استعادته في الحساس المُستقبل والذي يجب أن يكون مطابقاً لقيمة k_{session} . لتبادل المفتاح k_{session} ، يُحسب الحساس المرسل القيمة COM كما في العلاقة (1-3):

$$\text{COM} = F(u, k_{\text{session}}) = \underbrace{h(k_{\text{session}})}_a, \underbrace{u \oplus k_{\text{session}}}_d \quad (1-3)$$

حيث $h(.)$ هو تابع البصمة و $\oplus$ هو تابع XOR. باستخدام تابع فك الترميز $f(.)$ يُنشئ الحساس المُستقبل المفتاح k' باستخدام u' كما في العلاقة (2-3):

$$k' = G(u', \text{COM}) = f(k_{\text{session}} + (u' \oplus u)) = f(k_{\text{session}} + e) \quad (2-3)$$

حيث $f(.)$ هو تابع تصحيح الأخطاء ذو t بت (أي يستطيع تصحيح الأخطاء مع مسافة هامينغ تصل إلى t). كلما كانت r و r' متشابهتان، أي $|e| \leq t$ ، كلما زاد احتمال نجاح توزيع المفتاح. يتم التحقق من نجاح عملية تبادل المفاتيح باستخدام رمز التحقق $a = h(k_{\text{session}})$ حيث يجب أن يكون: $h(k') = a = h(k_{\text{session}})$.

أحد العوائق الرئيسية لاعتماد هذا المخطط هو أن بتات IPI ذات الدلالة الأعلى يمكن تقديرها من قبل الخصم، فهي تتغير بشكل طفيف عبر الزمن. ومن ناحية أخرى، تختلف بتات IPI ذات الدلالة الأدنى والمقاسة في الحساس المُستقبل، في معظم الأحيان، عن تلك المقاسة في الحساس المرسل بدرجة كبيرة؛ مما يجعل من غير الممكن التوصل إلى قيم IPI متطابقة بين الحساسين حتى ولو استُخدمت أرمزة تصحيح الأخطاء.

أما الطريقة الثانية المقترحة في [20] أيضاً، هي: الإدارة القائمة للمفتاح متعددة النقاط (Multipoint Fuzzy Key Management) وفيها يتم إنشاء المفتاح اعتباراً من قيم IPI المُقاسة في كل عقدة، حيث يكون المفتاح المنشأ هو نسخة معدلة عن تلك القيم. يتم إنشاء k_{session} اعتباراً من الإشارة الحيوية r المُقاسة في الحساس المُرسِل، حيث لوحظ أن إشارات ECG لديها ما يكفي من الانتروبية لتوليد مفاتيح تشفير جيدة. يتم توليد 8 bit فقط من المفتاح اعتباراً من كل قيمة IPI. بالتالي، يكون التغير الوحيد في هذا المخطط عن المخطط السابق هو أن k_{session} نفسها قد أصبحت نسخة من u . بناءً على تصميم WBAN، فإن عُقد الحساسات الأخرى (المُستقبلة) لديها أيضاً إمكانية الوصول إلى نُسخ مشابهة من u . أي يتم إعادة توليد مفتاح التعمية في كل حساس اعتباراً من القياسات الحيوية المشتركة والمُقاسة على التزامن. في هذا المخطط، لم يعد هناك حاجة لإرسال نسخة كاملة من المفتاح بعد إجراء عملية XOR له مع u ، وإنما يُرسل رمز التحقق فقط، للتحقق من تطابق المفتاح المُتشكّل لدى المُرسِل مع المفتاح المُتشكّل لدى المُستقبِل. إضافةً إلى ذلك، يمكن تغيير طول رمز التحقق الذي سيتم إرساله من أجل ضبط كفاءة عرض الحزمة الترددي، وذلك بناءً على جودة التحقق المطلوبة.

تتمثل محدودية هذا الأسلوب بأنه من أجل تكوين مفتاح طوله 128 bit يجب أن يتم تحصيل إشارة ECG لمدة 54 ثانية. ولكن المفتاح الناتج عن الإشارة المحصلة خلال تلك المدة الزمنية قد لا يكون عشوائياً بدرجة كافية. ومن ثم، قد تستغرق هذه الخوارزمية وقتاً طويلاً جداً لإنشاء المفتاح السري المناسب.

تقدم الورقة البحثية [13] مخطط الاتفاق على المفتاح بالاعتماد على الإشارة الحيوية (Physiological-Signal-based Key Agreement PSKA)، وهو مخطط يعمل بطريقة التوصيل والتشغيل، أي ليس هناك حاجة إلى التهيئة أو النشر المسبق للمفاتيح؛ وإنما بمجرد نشر الحساسات على الجسم يصبح بإمكانها البدء بعملية تبادل المفاتيح والتواصل بشكل آمن. يعتمد هذا المخطط على مبادئ القبول الغامض [97] في إخفاء المفتاح قبل إرساله إلى الحساس الآخر؛ وذلك باستخدام خصائص ECG. لا يُستخدَم هذا المخطط الإشارات الحيوية في إنشاء المفاتيح وإنما يُستخدَمُها في تبادل المفاتيح والاتفاق عليها فقط. كما تمت معالجة الإشارات الحيوية في المجال الترددي؛ بدلاً من المجال الزمني. وبشكل مُختصر نعرض فيما يلي كيفية تطبيق مبادئ القبول الغامض في مخطط PSKA:

- بدايةً يُشكّل كل من الحساس المرسل والحساس المستقبل شعاع الخصائص (شعاع يحوي خصائص مُستخلصة من إشارة ECG). يتم ذلك من خلال تحصيل عينات إشارة ECG بشكل متزامن، بمعدل أخذ عينات محدد ولمدة محددة، ثم تقسيم العينات المُحصّلة إلى نوافذ وإجراء تحويل فورييه السريع (Fast Furrier Transform FFT) لكل نافذة. بعد ذلك، تُستخرج المركبة الترددية العظمى لكل نافذة ومن ثم يُشكّل شعاع الخصائص والذي يتكوّن من القيم المُستخرجة من جميع النوافذ.
- يبنّي الحساس المرسل كثير حدود p من الدرجة v والذي تُختار معاملاته عشوائياً بحيث تُشكّل تلك المعاملات مدموجةً بعضها مع بعض المفتاح السري. ثم يحسب المجموعة P وهي مجموعة النقاط الناتجة عن تطبيق كثير الحدود p على كلّ عنصر من عناصر شعاع الخصائص. ثم يُشكّل المجموعة C المكوّنة من عناصر P مضافاً إليها نقاط الضجيج. يُرسل الحساس المرسل المجموعة C إلى الحساس المستقبل بالإضافة إلى عدّة قيم ومنها أرقام تعريف الحساسات، وقيمة تدل على الحادثة، ورمز مصادقة المفتاح والذي يُستخدَم للتحقق فيما إذا تمت عملية تبادل المفاتيح بنجاح.
- عندما يستقبل الحساس المستقبل تلك الرسالة، يُفك القفل عن طريق حساب المجموعة Q (وذلك بنفس الطريقة المُتبعة لفك القفل وفق القبول الغامض والمشروحة في فقرة سابقة) باستخدام شعاع الخصائص المُشكّل لديه. لكي يتمكن الحساس المستقبل من فك قفل القبول الغامض بنجاح، يجب أن يكون عدد نقاط المجموعة Q أكبر من v (درجة كثير الحدود)، أي يجب أن يتطابق أكثر من v عنصر من شعاع الخصائص المكوّن لدى كلّ من الحساسين. بعد ذلك يُعيد الحساس المستقبل بناء كثير الحدود باستخدام استيفاء لاغرانج ومن ثم يستعيد المفتاح من خلال دمج معاملات كثير الحدود الناتج بعضها مع بعض. وأخيراً يتحقّق الحساس المستقبل من تطابق المفتاح المكوّن لديه مع المفتاح المكوّن لدى الحساس المرسل من خلال حساب رمز التحقق والتأكد من تطابقه مع رمز التحقق المرسل من قبل الحساس المرسل. إذا نجح فك القفل، يُرسل الحساس المستقبل رداً إلى الحساس المرسل لإبلاغه بذلك.

بدراسة هذا المخطط تمكّننا من استنتاج أن الرسائل اللازم تبادلها من أجل تشكيل المفتاح تكون طويلة جداً، وذلك بسبب احتوائها على نقاط الضجيج المستخدمة في مخطط القبو الغامض. فكلما ازداد عدد تلك النقاط يزداد أمان عملية تبادل المفاتيح؛ وبالمقابل يزداد استهلاك طاقة الحساس.

في [23] قدم الباحثون مخطط تبادل مفاتيح جديد، (ECG-Improved Jules Sudan ECG-IJS)، يسمح للحساسات بتبادل مفتاح سري مشترك تم إنشاؤه بالاعتماد على إشارات ECG. يعمل المخطط المقترح بطريقة التوصيل والتشغيل. لا يستخدم هذا المخطط نقاط الضجيج لإخفاء المفتاح، فهو يعمل وفق طريقة القبو الغامض المعدلة؛ أي وفق مخطط Improved Jules Sudan (IJS). يعتمد هذا المخطط على تشكيل كثير حدود اعتباراً من قيم شعاع الخصائص المستنتج لدى الحساس المرسل، ثم إرسال جزء فقط من معاملاته إلى الحساس المستقبل من دون تعميّتها. يتم القيام بذلك من أجل التخلص من الحاجة إلى إرسال Vault ذي الحجم الكبير والذي يحوي نقاط ضجيج كثيرة جداً. من أجل استعادة المفتاح لدى الحساس المستقبل، يُعاد بناء كثير الحدود اعتباراً من قيم شعاع الخصائص المُتشكّل في ذلك الحساس، ومن جزء المُعاملات الذي تم استقباله. ويمكن وصف مخطط ECG-IJS على النحو التالي. يقوم الحساس المرسل بتنفيذ الخطوات التالية:

- استخراج شعاع الخصائص F من إشارة ECG، وتشكيل السر K اعتباراً منه.
- استخدام عناصر شعاع الخصائص F ، والتي نرسم لها بـ x ، كجذور لبناء كثير حدود p من الدرجة s ، ذو متغيّر وحيد، بحيث يكون $p(x)=0$.
- حساب مُعاملات كثير الحدود p ، ثم استنتاج كثير الحدود المُقتطع منه، وهو كثير الحدود من الدرجة $s-1$ حتى الدرجة $s-t$ ، ثم إرسال معاملات كثير الحدود المُقتطع، وعددها t معاملاً، إلى الحساس المستقبل.
- عندما يتلقى الحساس المستقبل المجموعة الفرعية من معاملات كثير الحدود $(t$ معامل)، يُصبح بإمكانه إعادة بناء كثير الحدود ذي المتغيّر الوحيد بالاعتماد على إشارة ECG المُقاسة لديه. يتم استعادة المفتاح لدى الحساس المستقبل كما يلي:

- استخراج شعاع الخصائص F' من إشارة ECG.

- بناء كثير الحدود p_{high} من الدرجة s باستخدام المُعاملات التي تم استقبالها.
 - تطبيق كثير الحدود السابق على كافة عناصر F' للحصول على مجموعة من الأزواج (نقاط).
 - استخدام مفكك الترميز Reed-Solomon للبحث عن كثير حدود p_{low} من الدرجة $s-t-1$ بحيث يكون $p_{high}(x) - p_{low}(x) = 0$ ، حيث x هي عناصر شعاع الخصائص F' .
 - إعادة بناء السر K بالاعتماد على المُعاملات المُستقبلة والمُعاملات المُستَعادة.
- يتكون شعاع الخصائص في كل من الحساسين، F و F' ، من القمم (peaks) الناتجة عن تحويل فورييه السريع لعينات ECG المقاسة بشكل متزامن بين الحساسين ولمدة زمنية ثابتة وهي أربع ثوانٍ.

نلاحظ في هذا المخطط أن إعادة بناء كثير الحدود تتطلب تنفيذ عمليات معقدة. كما يتمثل الضعف في هذا المخطط بأن قيمة معدل القبول الخاطئ (False Acceptance Rate FAR) تكون أكبر من الصفر عندما يكون عدد المعاملات المرسلَة (t) أكبر من الصفر. وهنا لا بد أن نُعرّف معدل القبول الخاطئ (FAR) ومعدل الرفض الخاطئ (False Rejection Rate FRR). FAR: هو معدل قبول عقد خبيثة على أنها عقد شرعية في شبكة WBAN محددة، وبالتالي هو معدل تشكيل مفتاح سري مشترك مع عقد غير شرعية واعتبارها عقداً شرعيةً. FRR: وهو معدل رفض عقد شرعية من قبل عقد أخرى ضمن شبكة WBAN نفسها واعتبارها عقداً غير موثوقة، وبالتالي هو معدل رفض تشكيل مفتاح سري مشترك مع عقد شرعية.

في [22] استُخدِمت إشارة ECG لإنشاء مفاتيح التعمية المتناظرة وتوزيعها بشكل موثوق وآمن. يعتمد النهج المقترح على ثلاثة كيانات لإنشاء المفتاح. تلك الكيانات هي عبارة عن عقدتين تريدان تبادل المفتاح فيما بينهما، وعقدة ثالثة مسؤولة عن تحقيق هذه العملية بشكل آمن. لتحقيق ذلك، يجب أن تمتلك العقد الثلاث إشارة ECG مسجلة بشكل متزامن بالكامل. يُستخدم رمز تصحيح الخطأ وتوابع البصمة من أجل إنجاز عملية تبادل المفاتيح. بدراسة هذه الطريقة نلاحظ أن الحاجة إلى كيان ثالث تؤدي إلى زيادة استهلاك الطاقة والموارد. كما نلاحظ أن هذه الطريقة تحتاج لعدد كبير من المراحل، وعدد كبير من عمليات التعمية وتصحيح الخطأ. وهي أيضاً تفرض قيوداً صارمة جداً على التزامن المطلوب بين الحساسات في أثناء تحصيل إشارة ECG. ويمكن أن تقشل عملية

تشكيل المفاتيح في عددٍ من المرات؛ نتيجة الاختلاف البسيط بين القيم المحصلة بالتزامن في حساسات عدّة موضوعة على الجسم نفسه.

في [5] يُقدّم أحد أحدث البروتوكولات المُقترحة في هذا المجال. على عكس البروتوكولات الحالية، يتيح البروتوكول المُقترح للحساسات المُتصلة إمكانية استخدام مستويات الجلسة السابقة لتشكيل مفتاح آمن يمكن استخدامه خلال فترة زمنية محددة. يؤدي ذلك إلى تقليل الزمن المطلوب لإنشاء المفتاح المُشترك، وكذلك تجنب إعادة إرسال الخصائص المُستخرجة عبر وسيط النقل، وبالتالي إحباط هجمات التنصّت، مع الحفاظ على عشوائية المفتاح. يمكن تلخيص البروتوكول المُقترح في [5] كما يلي. بدايةً، يقوم الحساسان بتحصيل الإشارة الحيوية بشكلٍ متزامن ولفترة زمنية محددة ولتكن t . يقوم كل من الحساسين باستخراج خصائص الإشارة المُحصّلة لديه وتخزينها في شعاع الخصائص. يُشترط على الخصائص المُستخرجة أن تكون ديناميكية. يتم تغيير ترتيب خصائص الإشارة في شعاع الخصائص باستخدام خوارزمية إعادة ترتيب معروفة لدى الحساسين. بعد ذلك، يُرسل الحساس المُرسل قيمة زمنية ونسخة من شعاع الخصائص بعد إضافة الضجيج إليه. تشير القيمة الزمنية المُرسلة إلى الفترة الزمنية التي تكون خلالها الخصائص المُستخرجة صالحة. نظراً لأن الحساسين يقومان بتحصيل نفس الإشارة، يمكن للحساس المُستقبل تحديد الخصائص المُشتركة من خلال إجراء عملية تقاطع بسيطة بين بين شعاع الخصائص المصحوب بالضجيج الذي تم استقباله من المُرسل وشعاع الخصائص المكوّن لديه. بعد ذلك، يقوم المُستقبل بتطبيق تابع البصمة على القيم المُشتركة لكي يحصل على المفتاح، ثم يقوم بإرسال أدلة الخصائص المُشتركة إلى المُرسل. يقوم المُرسل باستقبال أدلة القيم المُشتركة ثم تطبيق تابع البصمة على القيم المقابلة لها من أجل الحصول على المفتاح. في الاتصال التالي، يجب على المُرسل بدايةً التحقق من صلاحية المؤقت. إذا كان المؤقت لا يزال صالحاً، يُرسل المُرسل شعاع يحوي أدلة الخصائص المُشتركة بعد أن يتم تغيير ترتيبها، بالإضافة إلى ناتج تابع البصمة المُطبّق على المفتاح الجديد المولّد. المفتاح الجديد هو عبارة تطبيق تابع البصمة على الخصائص المقابلة للأدلة المُرسلة بعد عملية تغيير الترتيب. يستخدم المُستقبل الأدلة المُستقبلة ويحدد الخصائص المُشتركة ويولّد

المفتاح من جديد. لسوء الحظ، تعاني هذه الخوارزمية من نقطة ضعف أو وهي الحاجة إلى تحصيل إشارة ECG في الحساسات المتصلة وفق تزامن عالٍ جداً.

3-3- تحليل نتائج الدراسات السابقة في توليد المفاتيح الحيوية ومناقشتها

كما رأينا في الفقرة السابقة، تعتمد معظم الدراسات السابقة في توليد المفاتيح الحيوية السرية المشتركة وتبادلها على تشابه خصائص إشارة ECG المحصلة بشكل متزامن في حساسات مختلفة ضمن شبكة WBAN نفسها (أي في حساسات تنتمي للجسم نفسه). واجه الباحثون في الدراسات السابقة تحدياً رئيساً، ألا وهو التخلص من الاختلافات بين تلك الخصائص والتي تنتج عن الضجيج وعوامل أخرى [41]. وذلك لأن مثل هذه الاختلافات قد تحول دون تشكيل مفاتيح متطابقة في الحساسات المختلفة ضمن الشبكة نفسها.

3-3-1. مقارنة بين مخططات تبادل المفاتيح المعتمدة على ECG الواردة في الدراسات السابقة

يبين الجدول 3-1 مقارنة لمخططات تبادل المفاتيح الواردة في الدراسات السابقة، وذلك من نواحٍ أساسيةٍ عدّة. نلاحظ من الجدول أن بعض المخططات اعتمدت على خصائص إشارة ECG في المجال الزمني، أما بعضها الآخر فاعتمد على خصائص المجال الترددي لإشارة ECG. كما أن بعض المخططات اعتمدت على قيم ECG في توليد المفاتيح وتبادلها أما بعضها الآخر فقد استخدم تلك القيم من أجل تبادل المفاتيح فقط. أما توليدها فيتم باستخدام مولّدات الأرقام العشوائية. ونلاحظ أيضاً أن حجم البيانات المتبادلة يتفاوت من مخططٍ لآخر، وكان أسوأها في [13]. وكذلك الأمر بالنسبة لزمن تحصيل الإشارة المطلوبة، وكان أكبره في [20]. في [5] تولّد مفاتيح سرية من جميع الأطوال، وفي بعض المخططات تولّد مفاتيح بطول 128 bit فقط، أما بعضها الآخر فلم يُحدّد طول المفاتيح المولّدة. فيما يتعلق بدرجة التزامن المطلوب بين الحساسات، فنلاحظ أن بعض المخططات تتطلب تحقيق تزامناً صارماً للغاية. كما تحتاج معظم المخططات إلى توابع تصحيح الأخطاء، وفي معظمها أيضاً يكون FAR وFRR أكبر من الصفر.

الجدول 3-1: مقارنة بين مخططات تبادل المفاتيح المعتمدة على ECG.

المخطط المقترح في [5]	المخطط المقترح في [22]	ECG-IJS [23]	PSKA [13]	Multipoint fuzzy key management [20]	
المجال الترددي	المجال الزمني	المجال الترددي	المجال الترددي	المجال الزمني	مجال استخراج ECG خصائص
في توليد المفاتيح وتبادلها	في توليد المفاتيح وتبادلها	في تبادل المفاتيح	في تبادل المفاتيح	في توليد المفاتيح	الاستفادة من ECG خصائص
متوسط 129 Byte	صغير (عشرات البايتات)	صغير (عشرات البايتات)	كبير جداً، 2^{13} نقطة، حجم كل منها عدة بايتات	صغير (عشرات البايتات)	الحمل الناتج عن الاتصالات اللازمة
4 ثوانٍ	–	4 ثوانٍ	4 ثوانٍ	أكثر من 54 ثانية	زمن تحصيل ECG
كافة الأطوال	128 bit	–	128 bit	–	طول المفتاح الناتج
غير مستخدم	BCH	Reed– Solomon	يستخدم في Fuzzy-vault	BCH	استخدام توابع تصحيح الأخطاء
صارمة	صارمة	–	متسامح مع التزامن الضعيف	–	درجة التزامن المطلوبة
$> 0\%, > 0\%$	0%, 0%	$> 0\%, > 0\%$ تعتمد على درجة كثير الحدود	$> 0\%, > 0\%$ تعتمد على درجة كثير الحدود	$> 0\%, > 0\%$ تعتمد على معاملات BCH	FRR و FAR

3-3-2. الشروط الواجب توافرها في خوارزمية تبادل المفاتيح المعتمدة على ECG

يمكن أن نلاحظ من الدراسات السابقة مجموعة من الشروط التي يجب توافرها في مخطط تبادل المفاتيح المعتمد على ECG والتي يمكن تلخيصها في النقاط الآتية:

- الاستهلاك المحدود للموارد. لكي يكون استهلاك الموارد محدوداً، لا بد أن يتمتع المخطط ببساطة عمليات المعالجة، وأن يكون حجم البيانات المتبادل مقبولاً؛ فضلاً عن الاكتفاء بكيانين على الأكثر من أجل تحقيق عملية تبادل المفاتيح (أي عدم الحاجة لكيان ثالث).
- يجب أن يكون زمن إتمام عملية تبادل المفاتيح مقبولاً؛ مما يتيح تغيير المفتاح دورياً بحسب متطلبات التطبيق.

- التسامح مع ضعف التزامن، ومن ثم لا يؤدي الاختلاف البسيط في تزامن الحساسات إلى عدم القدرة على التوصل إلى مفتاح سري مشترك.
- أن تكون FAR تساوي الصفر، فإذا كانت أكبر من الصفر يكون هناك خطر تشكيل مفتاح سري مشترك مع كيان ضار (حساس غير موثوق، ولا ينتمي إلى WBAN نفسها).
- ديناميكية المفتاح، وقابلية تبديله بمفتاح آخر جديد خلال فواصل زمنية محددة مسبقاً أو عند الحاجة.
- العمل وفق طريقة التوصيل والتشغيل ومن ثم إلغاء الحاجة للتحميل المسبق للمفاتيح أو بعض القيم الأخرى في الحساسات، وبناءً عليه يمكن إضافة أي حساس مباشرة للشبكة من دون الحاجة إلى إعادة ضبط المفاتيح والقيم السرية الأخرى في باقي حساسات الشبكة.
- ضمان أمان الشبكة في أثناء إقلاعها، وعدم تبادل المفاتيح بشكلها الصريح في أثناء الإقلاع؛ مما قد يؤدي إلى فضحها والتعرض لها.

3-3-3. عدم الكفاية في الدراسات السابقة حول توليد المفاتيح وتبادلها بالاعتماد على ECG

من الدراسات السابقة، يمكن أن نرى بوضوح أن العثور على مخطط تبادل مفاتيح سرية، بالاعتماد على القيم الحيوية لا يزال مجالاً مفتوحاً للبحث، وهو ذو أهمية بالغة؛ لأن كلاً من الدراسات السابقة لا تزال تعاني من بعض نقاط الضعف. في بعض المخططات قد يشكل اختلاف ترتيب شعاع الخصائص المشتركة بين الحساسين أو اختلاف عدد الخصائص أو أحد تلك الخصائص عائقاً أمام الحصول على المفتاح السري المشترك [97]. وكما هو الحال في [20]، يؤدي الاعتماد على IPI إلى الحاجة إلى زمن طويل جداً لإنشاء المفاتيح السرية، كما أن الخانات ذات المرتبة الأدنى من قيم IPI تختلف بشكل ملحوظ بين حساسين موضوعين على الجسم نفسه مما يسبب بعض العقبات في تشكيل المفتاح السري اعتباراً منها. أما بالنسبة للاعتماد على الخصائص الترددية وبالتحديد مؤشر المركبة الترددية العظمى (Peak Index) في تحويل فورييه السريع لإشارة ECG كخصائص مشتركة بين الحساسين الموضوعين على الجسم نفسه، لم يعط نتائج عملية مرضية لدى تجربتها (يُبرهن على ذلك

في الفصل التالي). وتحتاج المخططات التي تستند إلى مبادئ Fuzzy Vault، مثل PSKA [13]، إلى عمليات معالجة معقدة، كما تحتاج أيضاً إلى إرسال رسائل طويلة جداً تتضمن عدداً كبيراً من نقاط الضجيج. يؤدي ذلك كله إلى استهلاك كبير لطاقة الحساس. يتغلب ECG-IJS [23] على الحاجة إلى إرسال نقاط الضجيج باستخدام IJS، لكنه يعاني من التعقيد الحسابي العالي؛ إذ يحتاج إلى إعادة بناء كثيرات الحدود، كما يعاني من FAR غير الصفري. علاوة على ذلك، تتطلب بعض المخططات، مثل [22] و [5] تزامناً صارماً للغاية يصعب تحقيقه دائماً. يُوضّح الجدول 2-3 المتطلبات الواجب تحقيقها في مخططات تبادل المفاتيح المعتمدة على القيم الحيوية، ومدى تحقيقها في كلّ من الدراسات السابقة. ومن الجدول 2-3، نستنتج أنه حتى الآن لا يوجد مخطط تبادل مفاتيح سرية مُعتمد على إشارة ECG يستوفي جميع الشروط المطلوبة.

الجدول 2-3: المتطلبات الواجب تحقيقها في مخطط تبادل المفاتيح المعتمد على القيم الحيوية، ومدى مراعاة تلك المتطلبات في الدراسات السابقة.

المتطلبات الواجب تحقيقها في مخططات تبادل المفاتيح المعتمدة على القيم الحيوية	Multipoint fuzzy key management [20]	PSKA [13]	ECG-IJS [23]	المخطط المقترح في [22]	المخطط المقترح في [5]
الاستهلاك المحدود للموارد	بساطة عمليات المعالجة	✓	×	✓	✓
	عدم الحاجة لتدخل كيان ثالث من أجل توليد المفاتيح وتبادلها	✓	✓	×	✓
	حجم البيانات المتبادلة مقبول	✓	×	✓	✓
زمن مقبول لإتمام عملية توليد المفاتيح	×	✓	✓	-	✓
التسامح مع ضعف التزامن	-	✓	-	×	×
FAR يساوي الصفر	×	×	×	✓	×
ديناميكية المفتاح (أي المفتاح متغير مع الزمن)	✓	✓	✓	✓	✓
العمل وفق تقنية Plug-and-Play	✓	✓	✓	✓	✓
ضمان أمان شبكة WBAN في أثناء إقلاعها	✓	✓	✓	✓	✓

3-4- الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على القيم الحيوية

تُعَدُّ مَوَلَّدات الأرقام العشوائية إحدى المستلزمات الضرورية لتحقيق حماية البيانات وعمليات التعمية. في هذا السياق، يمكن الاستفادة من حقيقة أن بعض الحساسات تُسجِّل الإشارات الحيوية، ومن ثمَّ يمكن استخراج العشوائية من تلك الإشارات المسجلة.

كما ذكرنا سابقاً يَستخدِم RNG مصدراً إنتروبياً، جنباً إلى جنب مع بعض عمليات المعالجة، لإنتاج العشوائية. قد يستغرق إنتاج الأرقام العشوائية عالية الجودة باستخدام RNGs زمناً طويلاً. بالتالي، لإنتاج عدد كبير من الأرقام العشوائية، قد يكون PRNG هو الأفضل. غالباً ما تَستخدِم شبكات الحساسات اللاسلكية PRNGs لتوليد السلاسل الثنائية العشوائية (RBSs) [24]، [31]. ولكن يستخدم PRNG البذور التي يجب أن تكون عشوائية وغير متوقعة والتي يتم الحصول عليها من RNG واختيارها بعناية وحمايتها. كما تتطلب PRNGs تنفيذ حسابات ثقيلة للحصول على العشوائية المطلوبة؛ مما يؤدي إلى استهلاك الموارد [24].

طَوَّر بعضُ الباحثين RNGs قائمة على القياسات الحيوية بهدف تجنب استخدام PRNGs في حساسات WBAN، ومن ثمَّ توفير طاقة الحساس [24]، [25]، [32]، [27]، [26]. درس بعضهم مؤخراً هذا الموضوع بالنسبة للإشارات العصبية [33]، [34]. يتمثل القيد الرئيس لهذه الدراسات في طول التسجيلات المستخدمة وحقيقة أن أجهزة التحسس لمخطط كهربائية الدماغ (Electroencephalogram EEG) للأغراض الطبية لها إمكانات محدودة [25]. ورَكَّز معظم الباحثين على استخدام إشارة ECG لتحقيق الهدف المطلوب.

اكتسب الفاصل الزمني بين دقات القلب المتتالية، IPI، اهتمام عددٍ من الباحثين في مجال أمن المعلومات [25]. كل قيمة IPI تتحرف عن الأخرى بشكل بسيط. لذلك، تَستَخِلصُ معظم أساليب توليد السلاسل العشوائية البتات الأربع ذات الدلالة الأدنى فقط من كل IPI، ثم تقوم بتجميعها لإنتاج RBSs طول كل منها 128 bit. يتمثل الجانب السلبي الرئيس لتلك التقنيات التقليدية في أنها تستغرق زمناً طويلاً جداً حيث إن الحساسات يجب أن تكتشف ما لا يقل عن 33 نبضة قلب لتوليد RBS ذات طول 128 bit. بالنسبة للبالغين، فإن معدل نبضات القلب

الطبيعي هو 60-100 نبضة في الدقيقة، وبالتالي تتطلب تلك التقنيات زمن معالجة كبير يتراوح بين 25 و30 ثانية لتقوم بتوليد RBS طولها 128 bit [24].

قدم الباحثون في [32] طريقة يمكن أن تستخرج 16 bit من كل نبضة قلب، وذلك باستخدام الفواصل الزمنية RR، RQ، RS، RP، وRT (الشكل 1-4) لتوليد RBS. تتمثل محدودية بحثهم بأن استخدام خمس فترات مختلفة يتطلب مزيداً من عمليات المعالجة اللازمة للترميز. اختبر الباحثون العشوائية من خلال اختبار احتمال ظهور الأرقام الثنائية من 0 حتى 3. فإذا كان احتمال ظهور كلٍ منها يساوي 0.25 تكون السلاسل عشوائية. استطاعت السلاسل المولدة اجتياز ذلك الاختبار بنجاح ومن ثم ادعى الباحثون أن الأرقام المولدة عشوائية.

من أجل تحسين الفعالية الزمنية، اقترح الباحثون في [24] جمع ثنائي قيم IPI متتالية لإنتاج RBS ذات طول 128 bit، وذلك بتطبيق التعمية وفق النمط CBC لتقليل أخطاء القياس، وتوليد متتاليات ثنائية من نبضات القلب. يتم توليد سلاسل عشوائية طولها 128 bit بأربع مراحل رئيسة يمكن تلخيصها كما يأتي. بدايةً، تُطبّق خوارزمية فعّالة للكشف عن الموجة QRS، بحيث تكون ذات معدل كشف عالٍ، وتُقاس الفواصل الزمنية بين كل قمتين R متتاليتين. بعد ذلك تُشكّل متتاليات تراتبية متزايدة اعتباراً من قيم IPI، ثم تُطبّق تقنية التعمية الكتلية وفق النمط CBC على قيم IPI الناتجة. أخيراً، يُستخرج 16 bit عشوائي من كل قيمة ناتجة، ثم تُدمج كل ثنائي قيم من القيم الناتجة بشكلٍ متتالٍ لتكوين سلسلة عشوائية طولها 128 bit.

إن هذه الطريقة أسرع بأربع مراتٍ من الأساليب التقليدية القائمة على IPI، ولكنها لا تزال تعاني من ضعف الفعالية الزمنية. اختبر الباحثون المولّد المطور باستخدام مجموعات مختلفة من البيانات، منها لأشخاص أصحاء، ومنها لمرضى القلب، ومنها للذين يعانون من عدم انتظام ضربات القلب. درس الباحثون عشوائية السلاسل الناتجة من خلال إجراء تسعة اختباراتٍ من مجموعة الاختبار NIST، وقد نجحت السلاسل المولدة باجتيازها. كما درسوا التميّز (Distinctiveness) من خلال حساب مسافة هامينغ (Hamming Distance HD) بين السلاسل العشوائية المولدة من بيانات أشخاص مختلفين، وتبيّن أن وسطي HD يساوي تقريباً نصف طول السلسلة المولدة؛ مما يبرهن أنها متميّزة.

مما سبق يتبين لنا أن تشكيل أرقام عشوائية، استناداً إلى قيم IPI يتصف بأداء منخفض للغاية. 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 [25]. بناءً على ذلك لم يستخدم الباحثون في [25] قيم IPI في توليد RNG؛ وإنما اعتمدوا على قيم عينات إشارة ECG. في مخططهم المقترح يتم توليد القيم العشوائية وفق الآتي. يتم إجراء المعالجة المسبقة لسجلات ECG لإزالة الضجيج باستخدام مرشح تمرير الحزمة. لاستخلاص القيم العشوائية، بدايةً، تُقسم إشارة ECG المحصلة إلى نوافذ يحوي كل منها على ذروة R واحدة (نبضة قلب واحدة). يتم تجاهل أول وآخر خمسين نافذة لضمان تسجيل الإشارة بشكل صحيح. يُجرى بعد ذلك التحليل المويجي لكل نافذة. ثم يُخفّض أخذ العينات من الإشارة بمقدار النصف، وتكرّر العملية لزيادة مستوى التحليل. يكون عدد التكرارات مشروط بمستوى التحليل المعتمد. أخيراً، تُستخرج البتات العشوائية بتحويل الجزء الكسري من كل معامل من معاملات التحويل المويجي إلى قيمة بدون إشارة طولها 32 bit، ثم تُقتطع 8 bit الدنيا منها. في هذا المخطط، هناك معاملين يجب ضبطهما. المعامل الأول هو مستوى التحليل المويجي L، حيث تم اختبار المولد من أجل مستويات التحليل 1، 2، 3، 4. الثاني هو التحويل المويجي المستخدم (على سبيل المثال، Daubechies أو coiflets).

هذه الطريقة هي أفضل من سابقتها من حيث الإنتاجية، ولكنها تحتاج إلى تنفيذ عمليات التحليل المويجي وهي عمليات حسابية قد تؤدي إلى استهلاك طاقة الحساس. تم دراسة عشوائية السلاسل المولدة بإجراء اختبارات NIST، ENT، وDiehard. كما تم أيضاً فحص التميز من خلال حساب HD بين السلاسل المولدة، وأثبتت التجارب أن وسطي HD يساوي تقريباً نصف طول السلاسل المولدة، مما يثبت تميزها.

3-5- تحليل الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على القيم الحيوية ومناقشتها

كما هو واضح من الدراسات السابقة، فقد اعتمد معظم الباحثين على إشارة ECG في توليد السلاسل العشوائية. من تلك الدراسات، نلاحظ أن معظم مولّدات الأرقام العشوائية القائمة على ECG اعتمدت على قيم IPI كمصدر للإنتروبية. ولكن، كما ذكرنا سابقاً، فإن أداء تلك الطرائق منخفض جداً، فهي وبأفضل الأحوال تستطيع استخراج

16 بتاً عشوائياً من كل IPI. فضلاً عن ذلك، وبناءً على بعض الدراسات الحديثة، يمكن تحديد الفاصل الزمني بين نبضتي قلب، باستخدام الكاميرات، وتحليل لون البشرة؛ مما يجعل تلك الطرائق أقل أماناً. ومن ثم، يكون استخدام الطرائق المعتمدة على قيم IPI فعالاً فقط في توليد سلاسل عشوائية قصيرة تعمل كمتغير عشوائي. أما بالنسبة للطرائق التي تعتمد على إشارة ECG كاملة، وعلى وجه الخصوص الطريقة المقترحة في [25]، فهي أفضل من حيث الإنتاجية، ولكنها تحتاج إلى تنفيذ عمليات التحليل المويجي وهي عمليات حسابية قد تؤدي إلى استهلاك طاقة الحساس.

3-5-1. مقارنة بين الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد ECG

يبين الجدول 3-3 مقارنة بين مخططات توليد السلاسل العشوائية بالاعتماد على إشارة ECG الواردة في الدراسات السابقة.

الجدول 3-3: مقارنة بين مخططات توليد القيم العشوائية بالاعتماد على إشارة ECG.

الدراسة	الطرق التقليدية المعتمدة على IPI	طريقة Xu وآخرون [32]	طريقة Pirbhulal وآخرون [24]	طريقة Camara وآخرون [25]
الطريقة المتبعة	تُسَخَّر البتات الأربع الدنيا من كل قيمة IPI ثم يتم تجميعها لإنتاج RBSs.	يُسَخَّر 16 bit من كل نبضة قلب باستخدام الفواصل الزمنية RR، و RQ، و RS، و RP، و RT.	جمع ثمانية قيم IPI متتالية وتطبيق التعمية وفق النمط CBC.	الاعتماد على التحليل المويجي لإشارة ECG بعد تقسيمها إلى نوافذ.
طول السلاسل التي تم اختبار العشوائية والتفرد من أجلها	128 bit	128 bit	128 bit	اختُبرت العشوائية لملفات أحجامها كبيرة، واختُبر التميز لسلاسل طولها 64 bit أو أقل.
معدل الإنتاج	4 bit/second (60 PPMs) 6.6 bit/second (100 PPMs)	16 bit/second (60 PPMs) 26.6 bit/second (100 PPMs)	16 bit/second (60 PPMs) 26.6 bit/second (100 PPMs)	184 bit/second (60 PPMs) 306 bit/second (100 PPMs)
الميزات	البساطة	أسرع من الطرق التقليدية	أسرع من الطرق التقليدية	إنتاجية أعلى من الطرق المعتمدة على IPI
السلبيات	تستغرق زمناً طويلاً جداً، حوالي 25-30 ثانية لتوليد سلاسل بطول 128 bit.	استخدام خمس فترات مختلفة يتطلب مزيداً من عمليات المعالجة اللازمة للترميز.	تعقيد أكبر من الطرائق السابقة ولا يزال الأداء منخفضاً.	معقدة، حيث تحتاج إلى العديد من عمليات التحليل المويجي.

نَلَحْظُ اعتماد معظم تلك الطرائق على قيم IPI، وأن دراسة العشوائية والتميز قد تمت فقط من أجل سلاسل عشوائية طولها يساوي 128 bit أو أقل. كما نَلَحْظُ بساطة الطرائق التقليدية وبالمقابل معدل إنتاجها المنخفض جداً. أما الطريقة التي تعتمد على قيم عينات إشارة ECG فهي ذات أداء أعلى، ولكنها معقدة، وتستهلك كثيراً من الموارد.

3-5-2. عدم الكفاية في الدراسات السابقة حول توليد السلاسل العشوائية بالاعتماد على ECG

هناك نقطتان أساسيتان يمكن ملاحظتهما من الدراسات السابقة. النقطة الأولى: تتطلب الأساليب الحالية القائمة على إشارة ECG زمناً كبيراً جداً لتوليد سلاسل عشوائية قصيرة، وذلك لا يتناسب مع تطبيقات الرعاية الصحية التي تعمل في الزمن الحقيقي. حتى الآن لم يُطَوَّر مَوْلِد سلاسل عشوائية مُعْتَمَد على إشارة ECG ذي معدل إنتاج عالٍ. أما النقطة الثانية: في الدراسات السابقة اخْتَبِرَت العشوائية والتميز من أجل سلاسل عشوائية طولها يساوي 128 bit أو أقل، علماً أن هناك عدداً من خوارزميات التعمية تحتاج إلى قيم عشوائية (على سبيل المثال، مفاتيح تعمية) أطول من 128 bit (تتراوح بين 128 bit و 2048 bit).

3-6- الدراسات السابقة حول تعمية البيانات في شبكات WBAN

لحماية شبكات WBAN يجب تحقيق عدد من المتطلبات، ومنها الحفاظ على سرية البيانات. وللحفاظ على سرية البيانات يجب أن يتم تعميتها قبل تبادلها بين الحساسات. وكما ذكرنا سابقاً، هناك نوعان أساسيان من التعمية، وهما: التعمية المتناظرة، والتعمية غير المتناظرة. تتصف خوارزميات التعمية المتناظرة ببساطة العمليات، ولكنها تعاني من الحاجة إلى تبادل المفتاح السري بشكل آمن. أما خوارزميات التعمية غير المتناظرة، فهي لا تحتاج إلى تبادل المفاتيح بشكل سري وآمن، ولكنها تعاني من التعقيد الحسابي واستهلاك الموارد. فضلاً عن ذلك تكون خوارزميات التعمية المتناظرة ذات أداء أعلى من خوارزميات التعمية غير المتناظرة، مما يجعلها أكثر ملاءمة للاستخدام في تطبيقات الرعاية الصحية التي تعمل في الزمن الحقيقي. بناءً على ذلك، يفضل استخدام التعمية المتناظرة في شبكات WBAN.

في الآونة الأخيرة، ظهر عددٌ من الأبحاث التي تُعنى بتطوير خوارزميات تسمية البيانات الطبية في شبكة WBAN، نظراً لما لحماية البيانات الطبية من أهمية. تهدف تلك الخوارزميات إلى جعل استهلاك طاقة وموارد الحساس أقل ما يمكن، مع الحفاظ على مستوى أمان عالٍ يتناسب مع الأمان المطلوب لحماية البيانات الطبية.

قدم الباحثون في [98] خوارزمية تسمية هجينة لتسمية البيانات المتبادلة بين حساسات شبكة WBAN، تأخذ في الحسبان كلاً من أمان البيانات، والقيود المختلفة مثل الطاقة المحدودة، وقدرة المعالجة المحدودة، وغيرها. تدمج هذه الخوارزمية طرائق التسمية المتناظرة مع طرائق التسمية غير المتناظرة؛ بهدف الحصول على مزايا كلٍّ منهما، وتجنب عيوب كلٍّ منهما، وبذلك يُستفاد من الفعالية العالية من حيث التكلفة لطرائق التسمية المتناظرة، ومن الحل الذي تقدمه طرائق التسمية غير المتناظرة لمسألة توزيع المفاتيح. بناءً عليه دَمَجَ الباحثون بين خوارزمية AES-128 bit المتناظرة، وخوارزمية المنحني الإهليلجي ECC-128 bit غير المتناظرة.

طَوَّرَ الباحثون في [37] خوارزمية تسمية فعالة وبسيطة التنفيذ لحماية الاتصال بين حساسات WBAN والهاتف المحمول في أنظمة العناية بالصحة. تتميز خوارزميتهم بصغر الرمز المصدري (الكود)، وباستهلاك الطاقة المنخفض، كما أنها سريعة التنفيذ بسبب اعتمادها على عمليات بسيطة مثل الجمع وعمليات XOR. تستخدم هذه الخوارزمية مفاتيح ذات أطوال متعددة وهي 128-bit، 192-bit، 256-bit، أما حجم الكتلة فيساوي 128-bit. قارن الباحثون خوارزميتهم بخوارزمية AES، فتبين أن زمن تنفيذ الخوارزمية المطورة أقل من نصف زمن تنفيذ AES.

اقترح الباحثون في [38] بنية آمنة للوصول إلى البيانات الصحية التي تُجمَعُ بوساطة WBAN. تعتمد بنيتهم على خوارزمية RSA غير المتناظرة، حيث تم تطويرها والحصول على خوارزمية ذات معدل إنتاج أعلى من معدل إنتاج RSA التقليدية كما تم أيضاً تقليل التأخير الزمني مما يقابله في RSA التقليدية.

قدم لنا الباحثون في [36] خوارزمية تسمية جديدة لتسمية البيانات في WBAN، تعتمد على عمليات بسيطة من أجل تقليل زمن التسمية وزمن فك التسمية، وزيادة الفعالية، وتقليل استهلاك الطاقة. تتألف عملية التسمية

من عشر خطوات، وعملية فك التعمية من ثماني خطوات. بعض العمليات المستخدمة في تلك الخطوات هي الاستبدال (Substitution) وتبديل المواضع (Permutation).

في IEEE 802.15.6 الخاص بشبكات WBAN، وكما ذكرنا سابقاً، تم اعتماد AES-CCM من أجل ضمان أمن المعلومات. يتكون AES-CCM من التعمية الكتلية CBC من أجل حساب MAC والنمط CTR من أجل تعمية البيانات باستخدام خوارزمية AES [99]، [100].

رغم أن بعض الباحثين في الدراسات السابقة استخدموا خوارزميات التعمية غير المتناظرة إلا أن خوارزميات التعمية المتناظرة هي أكثر ملاءمة لاعتمادها في شبكات WBAN، فهي مبنية على عمليات معالجة أبسط من تلك العمليات في خوارزميات التعمية غير المتناظرة؛ مما يجعل أداءها أفضل، واستهلاكها لطاقة الحساس أقل. وكما ذكرنا سابقاً، تُعدّ خوارزمية TEA الخوارزمية الأعلى أداءً من بين خوارزميات التعمية المتناظرة. ولكن نتيجةً لاستخدام TEA مفتاح التعمية نفسه في كافة الجولات، فهي تعاني من ضعف مناعتها ضد بعض الهجمات وهي: هجوم جمع البت، وهجوم التحليل التفاضلي، وهجوم المفاتيح المرتبطة.

اقترح الباحثون في [88] حلاً للتخلص من الهجمات المذكورة، وهو إضافة خوارزمية لتوليد مفاتيح مختلفة لدورات تنفيذ TEA. اعتمد هذا الحل على فكرة عدم إنشاء المفاتيح بشكل خطي أو متطابق من أجل دورات التنفيذ المختلفة لـ TEA. في الحالة المثالية، يجب أن يؤثر كل جزء من المفتاح على كل الجولات، وأن يؤثر على كل جولة بطريقة مختلفة. بالتالي اقترح الباحثون في [88] التعديل على طريقة توليد المفاتيح في معيار تعمية البيانات (Data Encryption Standard DES)، لتصبح مناسبة لتطبيقها من أجل توليد مفاتيح TEA. يتم توليد مفاتيح تعمية مختلفة لدورات TEA بشكل مشابه لتوليد مفاتيح تعمية DES، ولكن من أجل مفاتيح طولها 32-bit بدلاً من 48-bit. فضلاً عن ذلك، فإن عدد المفاتيح الجزئية لخوارزمية DES هو 16 مفتاحاً، ولكن تحتاج خوارزمية TEA إلى إنشاء من 16 إلى 128 مفتاحاً بحيث يتوافق مع عدد دورات تنفيذها. وبالتالي تم التعديل على خوارزمية توليد المفاتيح في DES لتلبية هذه المتطلبات. استطاع الحل المقترح زيادة أمان TEA، ولكن من الواضح أنه يؤدي إلى زيادة الأعباء الحسابية عند توليد مفاتيح دورات التنفيذ.

3-7- تحليل الدراسات السابقة في تسمية البيانات في WBAN ومناقشتها

نلاحظ من الدراسات السابقة، أن السعي نحو التوصل إلى خوارزميات تسمية خاصة بشبكة WBAN ذات استهلاك منخفض للطاقة وذات أداء عالٍ يتناسب مع تطبيقات العناية بالصحة في الزمن الحقيقي لا يزال موضع بحث. فالخوارزميات المعتمدة على التسمية غير المتناظرة معقدة، وغير متناسبة مع محدودية حساسات WBAN. أما الخوارزميات المتناظرة، فهي الأفضل بالنسبة لهذا النوع من الشبكات. تُعدّ TEA خوارزمية التسمية الأبسط على الإطلاق من بين خوارزميات التسمية الشائعة، ولكنها تحتاج إلى التحسين؛ بغية رفع مناعتها ضد بعض أنواع الهجمات مع الحفاظ على أدائها العالي.

3-8- خاتمة

من الدراسات السابقة الواردة في هذا الفصل يمكننا ملاحظة عدم الكفاية في مخططات حماية WBAN المعروفة سابقاً والمعتمدة على إشارة ECG. فلقد وضّحنا المشاكل التي لا تزال تعاني منها مخططات توليد المفاتيح السرية المصادق عليها وتبادلها بالاعتماد على ECG وأنه حتى يومنا هذا لم يتم إيجاد نماذج تحقق جميع المتطلبات اللازمة. كما وضّحنا أنه حتى الآن لم يتم إيجاد مودّل سلاسل عشوائية بالاعتماد على ECG ذو إنتاجية عالية تتوافق مع متطلبات تطبيقات الرعاية الصحية في الزمن الحقيقي. وبما يتعلق بخوارزميات التسمية، فقد بيّنا أن خوارزميات التسمية المتناظرة هي الأفضل لتسمية بيانات WBAN. كما بيّنا أن خوارزمية TEA هي خوارزمية ذات أداء عالٍ مقارنةً بالخوارزميات الأخرى الشائعة، ولكن يجب رفع مناعتها ضد الهجمات؛ لتصبح مناسبة للاستخدام في حماية الاتصالات بين حساسات WBAN.

في الفصول التالية من هذه الأطروحة، نطوّر ونصمّم نموذج جديد لتوليد وتبادل المفاتيح السرية المصادق عليها بين حساسات WBAN؛ وذلك بالاعتماد على الخصائص الزمنية والترددية لإشارة ECG، بحيث يتغلب على نقاط الضعف في الدراسات السابقة. كما نطوّر ونصمّم نموذج مودّل سلاسل عشوائية عالي الإنتاجية معتمد على إشارة ECG، يتميز ببساطة العمليات. ونقوم أيضاً بتحسين خوارزمية TEA بالاعتماد على إشارة ECG،

بطريقة تجعلها آمنة ضد الهجمات التي تتعرض لها TEA التقليدية؛ وذلك بهدف استخدامها في تعمية البيانات المتبادلة في WBAN.

الفصل الرابع

تطوير وتصميم نموذج لتوليد وتبادل المفاتيح السرية المصادق

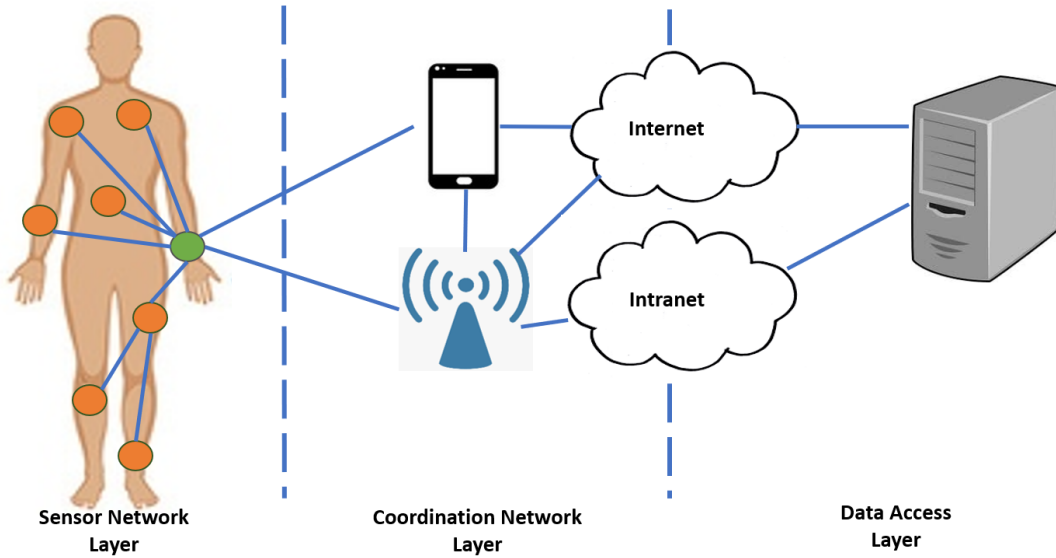
عليها بين حساسات WBAN بالاعتماد على إشارة ECG

100	1-4- تمهيد
100	2-4- البنية المعتمدة لشبكة نظام العناية الصحية الإلكترونية.....
101	3-4- أهداف تطوير نموذج جديد لتبادل المفاتيح السرية المصادق عليها في WBAN بالاعتماد على إشارة ECG.....
102	4-4- المبادئ والمفاهيم العامة لمخطط ECG-AKES.....
104	5-4- تطوير مخطط ECG-AKES وفق المبادئ والمفاهيم المقترحة.....
126	6-4- النتائج والمناقشة حول مخطط ECG-AKES المطور.....
126	1-6-4. نتائج التطبيق العملي لمخطط ECG-AKES وتحديد العتبات المثلى.....
133	2-6-4. أمان مخطط ECG-AKES.....
135	3-6-4. أداء مخطط ECG-AKES.....
136	4-6-4. ميزات مخطط ECG-AKES.....
138	7-4- خاتمة

4-1- تمهيد

من أجل التوصل إلى نظام آمن للعناية بالصحة، لا بد أن نضمن سرية البيانات المتبادلة بين حساسات شبكة WBAN من خلال تعميماتها. ولتحقيق ذلك يجب أن يكون لدى تلك الحساسات مفاتيح تعمية وفك تعمية مميزة؛ مبنية على معطيات ذات خصوصية، لكي ترفع من أمان المنظومة التي تُستخدم فيها. فضلاً عن ذلك، لا بد من استخدام آلية لتبادل تلك المفاتيح بحيث تتحقق من وصولها الآمن إلى مستخدميها. انطلاقاً من هذه الحاجة، ومن عدم الكفاية في الطرائق المقترحة في الدراسات السابقة حول توليد هذه المفاتيح وتبادلها بشكل موثوق، والتي بينهاها في الفصل السابق، نقدم في هذا الفصل نموذجاً مطوراً وجديداً لتوليد المفاتيح وتبادلها بين عقد حساسات WBAN. يعتمد النموذج المطور على إشارة ECG التي تقيسها حساسات WBAN، ويُعالج المشاكل وعدم الكفاية في النماذج المطروحة سابقاً.

4-2- البنية المعتمدة لشبكة نظام العناية الصحية الإلكترونية



الشكل 4-1: البنية المعتمدة لشبكة نظام العناية الصحية الإلكترونية.

نظراً لوجود عدة نماذج لشبكات أنظمة العناية الصحية الإلكترونية، لابد من تحديد النموذج الذي سنعتمده في دراستنا، وبالتحديد في تطوير نموذج توليد المفاتيح وتبادلها. انطلاقاً من الدراسات المرجعية، فإن النموذج الموضح

في الشكل 4-1 يُعتبر النموذج الأكثر استخداماً في أنظمة العناية الصحية الإلكترونية في وقتنا الحالي، وهو المُعتمد في بروتوكول IEEE 802.15.6.

في هذا النموذج، وبناءً على مقترحات البروتوكول IEEE 802.15.6، تكون طوبولوجيا الشبكة في طبقة WBAN هي طوبولوجيا نجمية، حيث تتصل جميع العقد بعقدة المنسق، إما بشكل مباشر وإما عن طريق عقدة أخرى تعمل كمبدل. في هذا النموذج، تُرسل جميع البيانات المحصلة إلى عقدة المنسق قبل نقلها إلى طبقة شبكة التنسيق. وتكون عقد شبكة الحساسات جميعها على تماس مباشر مع الجسم بما فيهم عقدة المنسق. تُسجل الحساسات القياسات الحيوية وترسلها إلى طبقة التنسيق ثم تُنقل هذه المعلومات إلى المخدم المركزي عبر الإنترنت أو عبر شبكة داخلية. فضلاً عما سبق، يتم افتراض أن كل شبكة WBAN ترتبط بجسم واحد فقط، وأن حساسات الشبكة جميعها محدودة جداً في الطاقة وقدرة المعالجة. ويمكن الوصول إلى البيانات الصحية للمريض فقط من قبل الأشخاص المصرح لهم بذلك.

4-3- أهداف تطوير نموذج جديد لتبادل المفاتيح السرية المصادق عليها في WBAN

بالاعتماد على إشارة ECG

نسعى في هذه الدراسة إلى تصميم مخطط لتوليد وتبادل المفاتيح السرية المتناظرة المصادق عليها بين أي حساسين في WBAN، بحيث يُعالج المشاكل في النماذج المطروحة سابقاً. نستخدم القيم الحيوية، وبالتحديد إشارة ECG لتكوين المفتاح وتبادله؛ مستفيدين من خصائصها التي وضحناها سابقاً. نطلق على المخطط المطور: مخطط تبادل المفاتيح المصادق عليها بالاعتماد على التخطيط الكهربائي للقلب (ECG-based Authenticated Key Exchange Scheme ECG-AKES).

في مخطط ECG-AKES المقترح نسعى إلى تجاوز عدم الكفاية في الدراسات السابقة وتحقيق الأهداف

التالية:

أولاً- تبادل المفاتيح بشكل آمن وتحقيق المصادقة. يقصد بالمصادقة هنا، التحقق من أن الحساسين الذين يقومان بتشكيل مفتاح سري فيما بينهما، هما حساسان شرعيان، وينتميان لشبكة WBAN نفسها.

ثانياً- بساطة العمليات المستخدمة، ومن ثمّ استهلاك أقل قدر ممكن من الموارد، والطاقة، وزمن المعالجة، وتحقيق أعلى أداء ممكن.

ثالثاً- ديناميكية المفاتيح السرية المتشكلة؛ أي إمكانية تغيير المفتاح السري المشترك دورياً مما يزيد من أمان الاتصالات بين العقد.

رابعاً- تكوين المفاتيح السرية بشكل آني من دون الحاجة إلى تحميلها أو تحميل بعض القيم السرية بشكل مسبق في الحساسات. يدعم ذلك إمكانية إضافة الحساسات إلى الشبكة بسهولة؛ وفق تقنية التوصيل والتشغيل.

خامساً- يضمن المخطط المقترح أمان الشبكة حتى في الفترة الأولية للتشغيل. أي لا تشكل الفترة الأولية لتشغيل الشبكة فترة خطر، حيث لن يتم تبادل أي بيانات سرية، ومنها المفاتيح، بشكلها الصريح عند بدء التشغيل.

سادساً- التوصل إلى نسبة FAR تساوي 0 مع نسبة FRR مقابلة تضمن فعالية المخطط.

4-4- المبادئ والمفاهيم العامة لمخطط ECG-AKES

نقدم فيما يلي المبادئ والمفاهيم التي تقود إلى النظرية العامة لمخطط ECG-AKES المطوّر. وقبل عرض المخطط المطوّر، لابد من تحديد الفرضيات اللازمة، وهي:

- عدم إمكانية أي شخص من الحصول على إشارة ECG المريض إلا إذا كان له الصلاحيات بذلك.
- حساسات WBAN متزامنة.
- لا يملك المهاجم وصولاً فيزيائياً لحساسات WBAN الموضوعّة على جسم المريض.

تتلخص فكرة المخطط المقترح بتوليد المفاتيح السرية محلياً في كل حساس بناءً على قيم مشتركة بين الحساسات والتي يتم الحصول عليها من الخصائص الترددية لإشارة ECG. لتحقيق هذه الغاية، يتم تبادل الخصائص الترددية المشتركة بين الحساسين اللذين يسعيان إلى تبادل مفتاح سري مشترك بينهما؛ باستخدام المصفوفات، وأدلة عناصر المصفوفات، وبعض العمليات عليها، كالتعمية، وتغيير المواضع. يتم في كل من

الحساسين استعادة الخصائص الترددية المشتركة بينهما، باستخدام ميزة التشابه بين قيم IPI المقاسة في كلٍ منهما بشكل متزامن. الخصائص الترددية المستخدمة، هي مجموعة مؤشرات المركبات الترددية العظمى لتحويل فورييه السريع لإشارة ECG. تُطبَّق فكرة المخطط هذه بطريقة تغطي عدم الكفاية في الأعمال السابقة؛ وفق المقترحات الآتية:

- الحصول على الخصائص المشتركة بين الحساسين ليس فقط من مؤشر المركبة الترددية العظمى لتحويل فورييه السريع لإشارة ECG؛ وإنما من مؤشرات عدد من المركبات الترددية العظمى الناتجة عن التحويل. فضلاً عن ذلك، الاستفادة من الخاصية الزمنية IPI ولكن من دون أن يُضعِف ذلك أداء المخطط، وبطريقة تساعد على تجاوز المشاكل الناتجة عن عدم تطابق قيمها لدى قياسها بشكل متزامن في حساسين مختلفين موضوعين على الجسم نفسه. بالتالي الدمج بين الخصائص الزمنية والخصائص الترددية لإشارة ECG للاستفادة من كليهما في تشكيل القيم المشتركة بين الحساسين.
- تحقيق نجاح المخطط من دون أن يكون تطابق جميع خصائص الإشارة بين الحساسين المتواصلين شرطاً لتحقيق تبادل المفاتيح بينهما. أي يمكن أن ينجح المخطط في عملية تبادل المفاتيح بالرغم من عدم تقاطع عدد لا بأس به من الخصائص بين الحساسين. في بعض الطرائق السابقة لا ينجح المخطط إلا إذا تطابقت الغالبية العظمى من الخصائص. أما في مخططنا نسعى لأن يكون من الكافي أن يتطابق عدد محدّد من الخصائص لتوليد المفتاح المشترك، ولكن من دون أن يمنعنا ذلك من تحقيق المصادقة؛ أي من دون أن يمنعنا ذلك من التحقق فيما إذا كان الحساسان المتصلان موضوعين على الجسم نفسه. كما سنسعى لتجاوز المشاكل الناتجة عن اختلاف ترتيب الخصائص المشتركة بين الحساسين.
- التخلُّص من الحاجة إلى عدد كبير من نقاط الضجيج، والتخلص من الحاجة إلى توابع تصحيح الأخطاء مثل BCH و Reed-Solomon [101]، وطرق استعادة كثير الحدود، اعتباراً من مجموعة من النقاط.
- التسامح مع ضعف التزامن بين الحساسات والتخلُّص من الحاجة إلى تزامن دقيق للغاية.

4-5- تطوير مخطط ECG-AKES وفق المبادئ والمفاهيم المقترحة

ليكن لدينا شبكة WBAN تحتوي على حساسات عدّة. يرغب الحساسان A و B، اللذان ينتميان إلى الشبكة نفسها، بتشكيل مفاتيح سرية مشتركة فيما بينهما وتبادلها. نرسم للمفتاح السري المشترك بالرمز KEY.

يبين الجدول 4-1 الرموز المستخدمة في مخطط ECG-AKES ودلالة كل منها.

الجدول 4-1: الرموز المستخدمة في مخطط تبادل المفاتيح المصادق عليها بالاعتماد على ECG (ECG-AKES) ودلالاتها.

الرمز	دلالته
ECG_B, ECG_A	إشارة ECG المحصلة في كل من الحساسين A و B
Max_F_A, Max_F_B	مجموعة مؤشرات القيم الناتجة عن تحويل فورييه السريع لإشارة ECG في كلا الحساسين A و B، مرتبة تصاعدياً.
L	عدد مؤشرات القيم المُستنتجة من معاملات تحويل فورييه السريع (عدد عناصر المجموعة Max_F والمجموعة G).
$R-R_{Bi}, R-R_{Ai}$	الفاصل الزمني بين قمتين R للنبتتين i-1 و i مقاسة في كل من الحساسين A و B بشكل متزامن.
G_B, G_A	مجموعة قيم R-R المتتالية المقاسة في كل من الحساسين A و B.
S, S_B, S_A	مجموعة القيم المشتركة بين الحساسين A و B والمولدة في كل من الحساسين A و B، حيث $S_A = S_B = S$ (وهي قيم المجموعة الناتجة عن $Max_F_A \cap Max_F_B$).
X_A	مصفوفة يتم إنشاؤها في الحساس A مكونة من 200 عنصر تُستخدَم من أجل استنتاج عناصر المجموعة S في الحساس B.
X_B	مصفوفة يتم إنشاؤها في الحساس B مكونة من 200 عنصر تُستخدَم من أجل استنتاج عناصر المجموعة S في الحساس A.
k	مفتاح تعمية خوارزمية TEA.
r	مصفوفة إعادة الترتيب ذات 10 عناصر.
R	مصفوفة إعادة الترتيب ذات 200 عنصر.
$Hash(\cdot)$	تابع البصمة.
RS	سلسلة عشوائية مُولدة بالاعتماد على إشارة ECG.
KEY	المفتاح السري المشترك بين الحساسين A و B والناتج عن تطبيق مخطط ECG-AKES.

انطلاقاً من مِيزة التشابه بين قيم IPI المقاسة بشكل متزامن في حساسين موضوعين على الجسم نفسه،

ومن الخصائص الترددية المشتركة، يمكن أن نحصل على مجموعة من القيم المساعدة لحساب المفتاح المشترك

وفقاً لما يأتي:

- تحديد عدد القيم المساعدة المستخدمة بـ L قيمة (ولكن 20 قيمة).

- إيجاد قيم IPI اعتباراً من الفاصل الزمني بين قمم R لكل نبضتين متتاليتين (R-R) لإشارة ECG المُقاسة في الحساسين A و B في الوقت نفسه، ووضع القيم الناتجة في مجموعتي القيم G_A بالنسبة للحساس A و G_B بالنسبة للحساس B. عدد عناصر كلٍّ من المجموعتين هو L عنصر.
- إيجاد مؤشرات القمم الناتجة عن تحويل فورييه السريع (FFT) لإشارة ECG المحصّلة في كلٍّ من الحساسين في الوقت نفسه، وترتيبها تصاعدياً، ووضعها في المجموعة Max_F_A بالنسبة للحساس A وفي المجموعة Max_F_B بالنسبة للحساس B بحيث يكون عدد عناصر كلٍّ منها يساوي L عنصراً.
- نظراً لتشابه قيم IPI من حيث القيمة الزمنية وتقاربها من بعضها بعضاً مع الزمن، وللاستفادة منها، لا بدّ من النظر إلى الفوارق الصغيرة الناتجة فيما بينها. بالتالي يتطلب الأمر الاحتفاظ بكسر القيمة والاستفادة من القيمة الصحيحة الناتجة؛ وذلك بكسر اعتمدَ بدقة ست خانات عشرية؛ لتجنّب الحساب بالفاصلة العائمة المسبب لأزمة حسابية كبيرة نسعى إلى تفاديها. نقوم بمقايسة القيم على مجال 10^6 فنحصل على قيم صحيحة موجبة ومتباينة.
- تشكيل مصفوفة (array) عدد عناصرها N عنصر يطابق أكبر قيمة مُحتمَل ظهورها من قيم مؤشرات القمم؛ لضمان أن تكون جميع قيم مؤشرات القمم تشير إلى إحدى عناصر هذه المصفوفة. ونظراً لأن التجربة بيّنت أن قيم مؤشرات القمم لا تتجاوز القيمة 200، حُدِدَ طول هذه المصفوفة بـ $N=200$ عنصر حيث يشير دليل المصفوفة إلى قيمة مؤشر القمة، أما قيم عناصر المصفوفة المقابلة لتلك المؤشرات، فتساوي قيم IPI بعد التقييس كما وردت.
- بما أن مؤشرات القمم الناتجة تكون متباينة وغير كافية لتغطية جميع أدلة عناصر المصفوفة، فإن بعضاً من خلايا المصفوفة ستبقى فارغة.
- نتيجة وجود خلايا فارغة في المصفوفة، كان لا بدّ من إعطاء هذه الخلايا قيمةً تساعد على زيادة أمان المفاتيح المطلوبة.

- تُملأ الخلايا الفارغة بقيم عشوائية ناتجة عن مولّد قيم عشوائية ضمن كل حساس. تُولّد هذه القيم بحيث تكون ضمن المجال المسموح فيه لخلايا المصفوفة. نرّمز لها بمجموعة القيم العشوائية RS_A و RS_B في الحساسين A و B على التوالي.

- بناءً على ما سبق، نحصل في الحساس A على سلسلة القيم للمصفوفة PX_A كما يأتي:

$$PX_A = f(RS_A, G_A, Max_F_A) \quad (1-4)$$

يربط التابع f بين قيم مؤشرات القيم وقيم IPI بالشكل الآتي:

$$PX[i] = \begin{cases} G_A[\lfloor i/(N/L) \rfloor + 1] \times 10^6 & i \in Max_F \\ RS[i] & i \notin Max_F \end{cases} \quad (2-4)$$

وعليه، وفق المعطيات المذكورة أعلاه، تصبح العلاقة بالشكل الآتي:

$$PX_A[i] = \begin{cases} G_A[\lfloor i/10 \rfloor + 1] \times 10^6 & i \in Max_F_A \\ RS_A[i] & i \notin Max_F_A \end{cases} \quad (3-4)$$

تُرسل سلسلة القيم PX_A من الحساس A إلى الحساس B من أجل استنتاج القيم المشتركة وذلك في الحساس B. ولضمان إخفاء قيم PX_A في أثناء نقلها كان لا بد من تعمية هذه السلسلة؛ وفق خوارزمية تكون ذات أداء عالٍ وحماية كافية؛ لكونها ستستخدم من أجل تعمية دفعة بيانات (burst) واحدة، وبالتالي إمكانية مهاجمتها غير متاحة. انطلاقاً من ذلك، نستخدم خوارزمية TEA بمفتاح k بالإضافة إلى خلط وتبديل مواقع عناصر المصفوفة وفق مصفوفة إعادة ترتيب محددة، ولتكن R. وعليه نحصل على:

$$X_A = Enc_{k,R}[PX_A] \quad (4-4)$$

$$X_A = Enc_{k,R}[f(RS_A, G_A, Max_F_A)] \quad (5-4)$$

- عند تلقي الحساس B للمصفوفة X_A المُعمّاة، سيستخدم قيم عناصر هذه المصفوفة مع قيم Max_F_B و G_B لاستنتاج مجموعة القيم S_B المشتركة بين Max_F_A و Max_F_B . يتم ذلك بفك تعمية قيم عناصر X_A المستلمة بعد إعادة ترتيبها من جديد وفق R ثم مقارنة القيم الناتجة والتي دليلها يساوي أحد عناصر Max_F_B مع القيم الموجودة في G_B ، فإذا كانت القيم متساوية أو ذات اختلاف مقبول Th يتم ضم دليل العنصر إلى عناصر مجموعة القيم المشتركة S_B كما هو موضح في العلاقة الآتية:

$$S_B[j] = \{i \mid i \in \text{Max_}F_B \& (\text{Dec}_{k,R}(X_A[i])/10^6 = G_B[\lfloor i/10 \rfloor + 1] \pm Th) \quad (6-4)$$

- بعد تحديد سلسلة القيم المشتركة S_B ، يجب إرسالها إلى الحساس A لاستنتاج المفتاح المطلوب؛ وذلك بتشكيل مصفوفة X_B بالاعتماد على قيم S_B و G_B و RS_B بطريقة مشابهة لتشكيل المصفوفة X_A سابقاً وذلك وفقاً لما يأتي:

$$PX_B = f(RS_B, G_B, S_B) \quad (7-4)$$

وباستخدام التابع f نفسه، نحصل على:

$$PX_B[i] = \begin{cases} G_B[\lfloor i/10 \rfloor + 1] \times 10^6 & i \in S_B \\ RS_B[i] & i \notin S_B \end{cases} \quad (8-4)$$

تُعمى قيم PX_B وفق المفتاح k نفسه ومن ثم يُعاد ترتيب القيم وفق R نفسها لنحصل على:

$$X_B = \text{Enc}_{k,R}[f(RS_B, G_B, S_B)] \quad (9-4)$$

يتم إرسال X_B إلى الحساس A.

- في الحساس A تُنفَّذ نفس الخطوات التي نُفَّذت في الحساس B عند استلام X_A وذلك للحصول على S_A كما يأتي:

$$S_A[j] = \{i \mid i \in \text{Max_}F_A \& (\text{Dec}_{k,R}(X_B[i])/10^6 = G_A[\lfloor i/10 \rfloor + 1] \pm Th) \quad (10-4)$$

وعليه ستكون $S_A = S_B$ ، وهو ما نسعى إلى تحقيقه.

بالتالي نكون قد توصلنا إلى مجموعة من القيم المشتركة بين الحساسين؛ باستخدامها يمكن استنتاج المفتاح المشترك

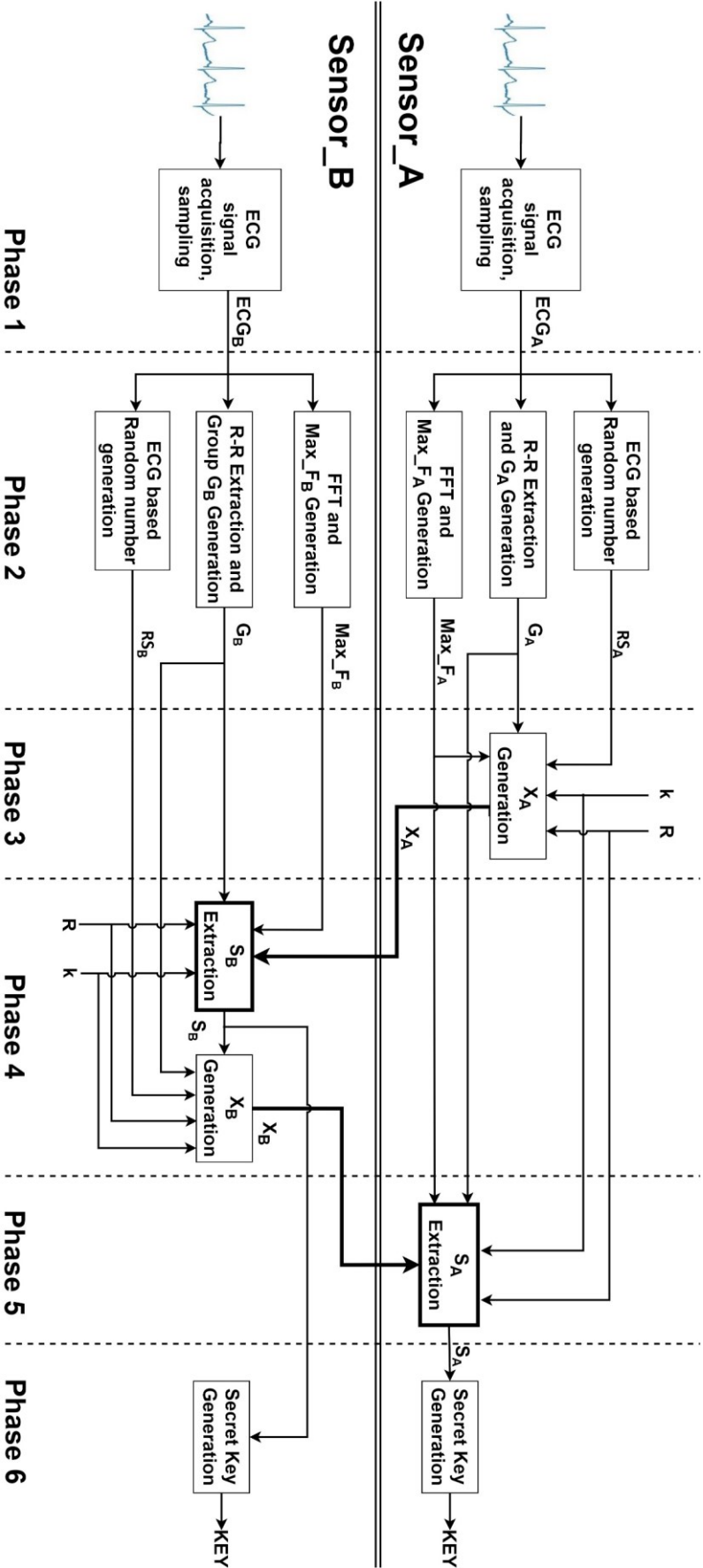
.KEY

انطلاقاً مما حُدِّد أعلاه، نستنتج المخطط المقترح ECG-AKES لتوليد المفاتيح وتبادلها. يتكون هذا

المخطط من ست مراحل كما هو موضح في الشكل 4-2. ويبين الجدول 4-1 شرحاً للرموز المستخدمة في هذا

المخطط. يمكن تكرار هذا المخطط عدداً غير محدد من دورات التنفيذ وفي كل دورة تنفيذ يتم الحصول على مفتاح

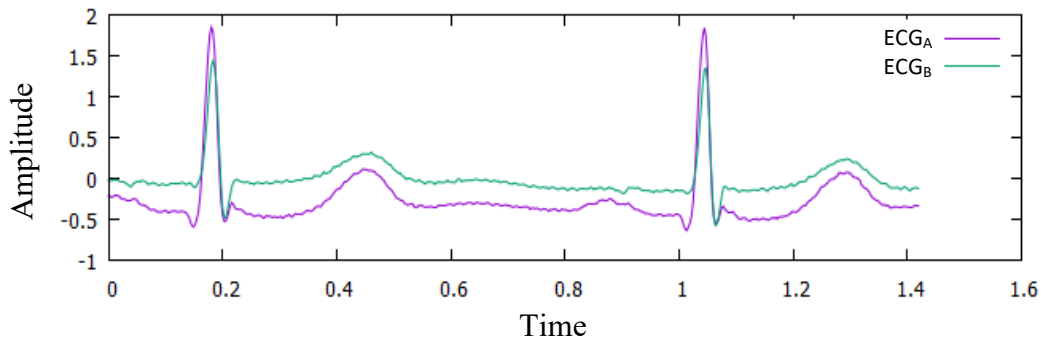
KEY جديد.



الشكل 2-4: مخطط تبادل المفاتيح المصاحبة على أساس ECG (ECG-AKES).

❖ المرحلة الأولى

في المرحلة الأولى، يتم بدايةً تحصيل إشارة ECG؛ وفق معدل اعتيان (Sampling rate) محدد ولمدة زمنية محددة، ولتكن T ثانية وبشكل متزامن في كلا الحساسين. يجب تحقيق التزامن بين الحساسين عند تحصيل الإشارة، أي يجب تحصيل الإشارة في الوقت نفسه في كلا الحساسين. لم تُحدّد في هذه الدراسة طريقة تحقيق تزامن الحساسات، وكذلك الأمر في الدراسات السابقة المعنية بمخططات توليد وتبادل المفاتيح الحيوية. ولكن يتميز مخططنا المقترح بتسامحه مع بعض الاختلافات في التزامن، أي نحن لسنا بحاجة لتحقيق تزامن دقيق للغاية بين الحساسات، وسنُثبت ذلك في فقراتٍ لاحقة.



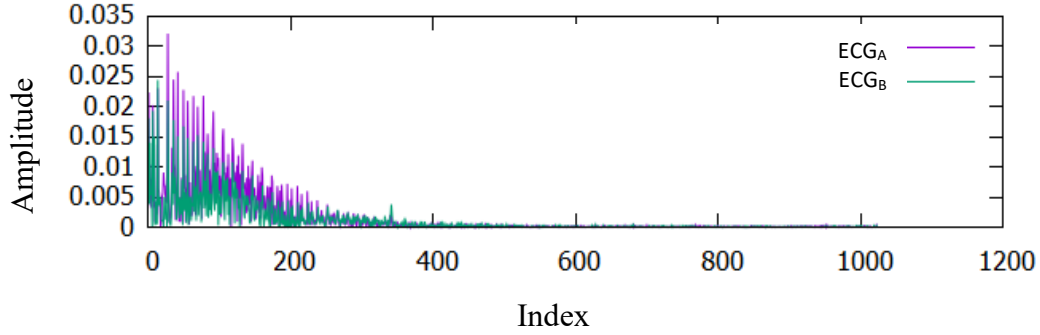
الشكل 3-4: إشارة ECG المحصلة في كل من الحساسين A و B بشكل متزامن خلال 1.4 ثانية بمعدل اعتيان يساوي 360 عينة في الثانية.

يبين الشكل 3-4 إشارة ECG المحصلة في كل من الحساسين A و B بشكل متزامن، خلال زمن تحصيل قدره 1.4 ثانية، وبمعدل اعتيان 360 عينة في الثانية.

❖ المرحلة الثانية

تتألف المرحلة الثانية من ثلاث خطوات. تُطبّق كافة الخطوات في كلا الحساسين بشكل متماثل، ولكن كلّ حسب مجموعة عينات ECG المحصلة لديه.

الخطوة الأولى: بدايةً يُطبّق كل من الحساسين A و B تحويل فورييه السريع (FFT) على الإشارة المحصلة لديه لعدد محدد من العينات، وليكن n عينة، وذلك بدءاً من العينة المقابلة للحظة زمنية محددة. يبين الشكل 4-4 مثلاً حول تحويل فورييه السريع لـ 1024 عينة من إشارة ECG المحصلة بشكل متزامن في كل من الحساسين A و B.



الشكل 4-4: تحويل فورييه السريع لـ 1024 عينة من إشارة ECG المُحصَّلة بشكل متزامن في كل من الحساسين A وB.

نلاحظُ أن المركبات الترددية العظمى لإشارة الحساس A معظمها مشترك مع المركبات الترددية العظمى لإشارة الحساس B. سنستفيد من هذه الخصائص المشتركة بين الحساسين في تشكيل المفتاح السري المشترك بينهما. لتحقيق ذلك يُستخلص في كل من الحساسين، بعد تطبيق تحويل فورييه، عددٌ محددٌ من أدلة الترددات ذات المطالات الأعلى؛ أي أدلة المركبات الترددية العظمى الناتجة، والتي نطلق عليها مؤشرات القمم، وليكن عددها L. لم نعتمد على دليل المركبة الترددية العظمى فحسب؛ وإنما على أدلة مجموعة المركبات الترددية العظمى. على سبيل المثال، في إحدى التجارب العملية التي أُجريت من أجل بيانات أحد مرضى عدم انتظام ضربات القلب، حيث كانت $L=20$ ، كانت مؤشرات القمم في الحساس A:

27, 41, 35, 13, 49, 1, 77, 63, 55, 6, 69, 91, 105, 90, 83, 104, 118, 132, 8, 33,

أما في الحساس B، فكانت:

13, 27, 6, 1, 35, 49, 69, 41, 8, 55, 63, 77, 2, 91, 83, 105, 118, 104, 132, 94,

نلاحظُ وجود عدد من القيم المشتركة (18 قيمة من أصل 20)؛ مع ملاحظة اختلاف ترتيبها، حيث نجد أن دليل المركبة الترددية العظمى في إشارة الحساس A، والذي يساوي 27، لا يتطابق مع دليل المركبة الترددية العظمى في إشارة الحساس B هو 13. بعد تشكيل مجموعة مؤشرات القمم في كل من الحساسين A وB تُرتَّب تصاعدياً ويتم تشكيل المصفوفة Max_F_A في الحساس A والمصفوفة Max_F_B في الحساس B. في مثالنا، تكون المجموعة Max_F_A كالآتي:

$Max_F_A = \{1, 6, 8, 13, 27, 33, 35, 41, 49, 55, 63, 69, 77, 83, 90, 91, 104, 105, 118, 132\}$

أما المجموعة Max_F_B فتكون كالآتي:

$Max_F_B = \{1, 2, 6, 8, 13, 27, 35, 41, 49, 55, 63, 69, 77, 83, 91, 94, 104, 105, 118, 132\}$

نلاحظ أن هناك عدداً كبيراً من النقاط المشتركة (المتقاطعة) بين المجموعتين السابقتين، وهي:

$$\text{Max_F}_A \cap \text{Max_F}_B = \{1, 6, 8, 13, 27, 35, 41, 49, 55, 63, 69, 77, 83, 91, 104, 105, 118, 132\}$$

نسعى من خلال المخطط المقترح إلى جعل كل من الحساسين قادراً على التوصل إلى أكبر عدد ممكن من مؤشرات القمم المشتركة بينهما؛ أي أكبر عدد ممكن من عناصر $\text{Max_F}_A \cap \text{Max_F}_B$. وكما ذكرنا سابقاً، نطلق على تلك المجموعة التي نسعى لإيجادها في كلا الحساسين، المجموعة S.

تختلف مؤشرات القمم من قياس لآخر بحسب اللحظة الزمنية التي تُقاس فيها الإشارة؛ وذلك لأن نبضات القلب ليست منتظمة بشكل كامل، فهي تتغير بحسب الحالة الحركية والنفسية والصحية للشخص، كما تتمتع ببعض الخصائص العشوائية.

الخطوة الثانية: استخلاص المجموعتين G_A و G_B في كل من الحساسين A و B على التوالي، حيث يكون كلٌّ منها عبارة عن مجموعة مكونة من قيم IPI (سنرمز لها بـ R-R دلالةً على الفاصل الزمني بين قمتي R لنبضتين متتاليتين) لنبضات متتالية عِدّة. وليكن عدد عناصر كل من G_A و G_B هو L عنصراً (مساوٍ لعدد عناصر المجموعة $(\text{Max_F}_A \cap \text{Max_F}_B)$). تأخذ G_A و G_B الشكل الآتي:

$$G_A = \{R-R_{A1}, R-R_{A2}, \dots, R-R_{AL}\}$$

$$G_B = \{R-R_{B1}, R-R_{B2}, \dots, R-R_{BL}\}$$

يتم ذلك في كلا الحساسين بشكل متزامن اعتباراً من لحظة محددة، حيث تكون $R-R_{Ai}$ و $R-R_{Bi}$ هي الفاصل الزمني بين النبضة i-1 والنبضة i، ولكن تم قياس $R-R_{Ai}$ في الحساس A أما $R-R_{Bi}$ فتم قياسها في الحساس B. وكما ذكرنا، تكون قيمة R-R المقاسة بشكل متزامن في حساسين مختلفين موضوعين على الجسم نفسه متقاربة جداً، ولكن غير متطابقة تماماً، وتختلف عن بعضها بعبء معينة Th. كما أن قيم R-R تختلف عشوائياً عند كل قياس؛ وذلك لأن نبضات القلب ليست منتظمة بشكل كامل وإنما تتغير بحسب عوامل عدة ولا يمكن التنبؤ بها. فيما يلي مثلاً حول عدّة قيم R-R لأحد الأشخاص، والمقاسة على التوالي:

$$1.047222, 1.030556, 1.033333, 1.041667, 1.000000, 1.025000, 1.022222, 0.994444, 0.975000, 0.969445, 0.966667, 0.991666, 0.983334$$

يمكن للخانات ذات المرتبة الأعلى أن تتشابه. أما الخانات ذات المرتبة الأدنى، فهي تختلف من قياس لآخر. سنعتمد على هذه الخصائص في تبادل قيم المجموعة S وحمايتها. من أجل قياس الفاصل الزمني R-R بأعلى دقة ممكنة تم استخدام الخوارزمية المقترحة في [102] لاكتشاف المركبة QRS ومن ثمَّ تحديد R لكل نبضة، ثم حساب الفاصل R-R بين كل نبضتين متتاليتين.

الخطوة الثالثة: توليد مجموعة من السلاسل العشوائية اعتباراً من إشارة ECG في كل من الحساسين A و B طول كلٍ منها 32 bit.

❖ المرحلة الثالثة

في هذه المرحلة يشكّل الحساس A المصفوفة X_A ، وهي مصفوفة مكونة من 200 عنصر من نمط uint32_t، تُستخدم من أجل استنتاج العناصر المشتركة بين الحساسين في الحساس B. وكما برّرنا سابقاً، جُعِلَ حجم المصفوفة 200 عنصر؛ لأنه ومن خلال التجارب نلاحظ أن الغالبية العظمى من مؤشرات القمم تكون قيمتها أقل من 200 عندما $L=20$. بالعودة إلى المثال السابق، نلاحظ أن أعلى قيمة لمؤشرات القمم هي 132. تُكوّن المصفوفة X_A وفق الخطوات الآتية:

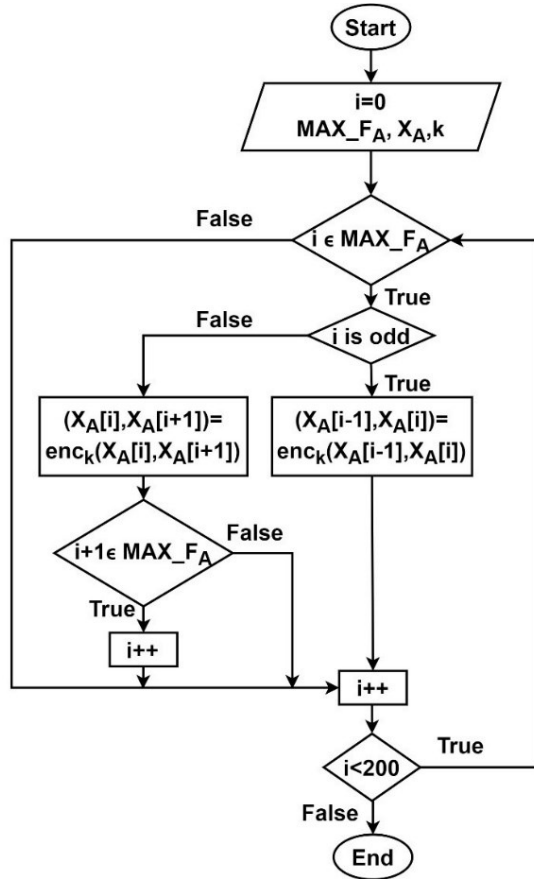
الخطوة الأولى: تُمَلَأُ عناصر المصفوفة X_A وتُعطى قيمة، وفق ما يأتي:

- تُمَلَأُ العناصر التي دليلها يساوي إحدى قيم عناصر المصفوفة Max_F_A (أي قيمة أحد مؤشرات القمم) بإحدى قيم R-R من المجموعة G_A كما في العلاقة (11-4).

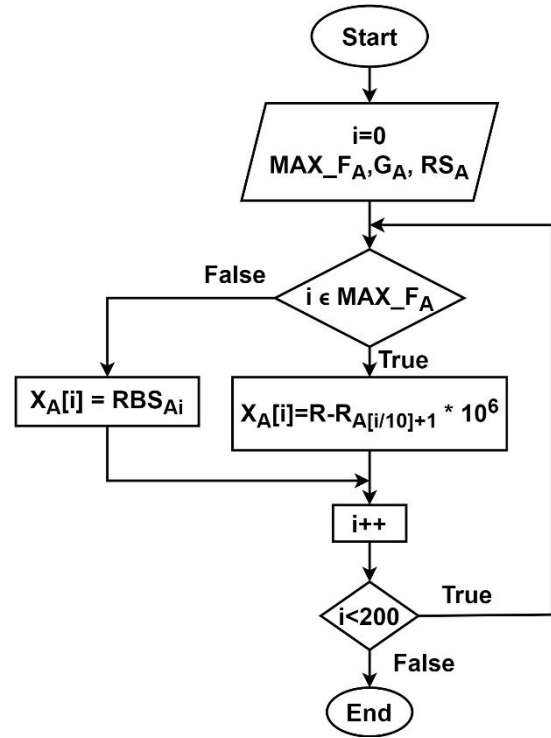
$$X_A[i] = R - R_{A[(int)(i/10)+1]} \times 10^6 \quad \text{if } i \in Max_F_A \quad (11-4)$$

حيث i هو دليل العنصر في المصفوفة X_A . ويتم ضرب قيم R- R_A المخزنة في X_A بـ 10^6 كما برّرنا سابقاً.

- تُمَلَأُ باقي العناصر بالقيم العشوائية المولدة، باستخدام مولّد أرقام عشوائية.



ب. الخوة الثانية



أ. الخوة الأولى

الشكل 4-5: تسلسل عمل الخطوتين الأولى والثانية من المرحلة الثالثة في ECG-AKES.

index	value	
0	RBS _{A0}	=179661570
1	R-R _{A1} × 10 ⁶	=836111
2	RBS _{A2}	=3884117847
3	RBS _{A3}	=3420132033
4	RBS _{A4}	=624744443
5	RBS _{A5}	=683185854
6	R-R _{A1} × 10 ⁶	=836111
7	RBS _{A7}	=2505387441
8	R-R _{A1} × 10 ⁶	=836111
9	RBS _{A9}	=2378564947
10	RBS _{A10}	=2208737343
11	RBS _{A11}	=2033245659
12	RBS _{A12}	=1262494105
13	R-R _{A2} × 10 ⁶	=844445
...	...	...
199	RBS _{A199}	=1151049111

الشكل 4-6: عناصر X_A في نهاية الخوة الأولى من المرحلة الثالثة بحسب مثالنا.

يبين الشكل 4-5 أ تسلسل عمل الخطوة الأولى من المرحلة الثالثة. بحسب مثالنا وقيم Max_F_A فيه، تكون العناصر الأولى للمصفوفة X_A عند نهاية هذه الخطوة كما هو مبين في الشكل 4-6. حيث القيم المظلمة باللون الرمادي تساوي لقيم $R-R_A$ من المجموعة G_A مضروبة بـ 10^6 ، والتي يتم اختيارها وفق المعادلة (4-11).

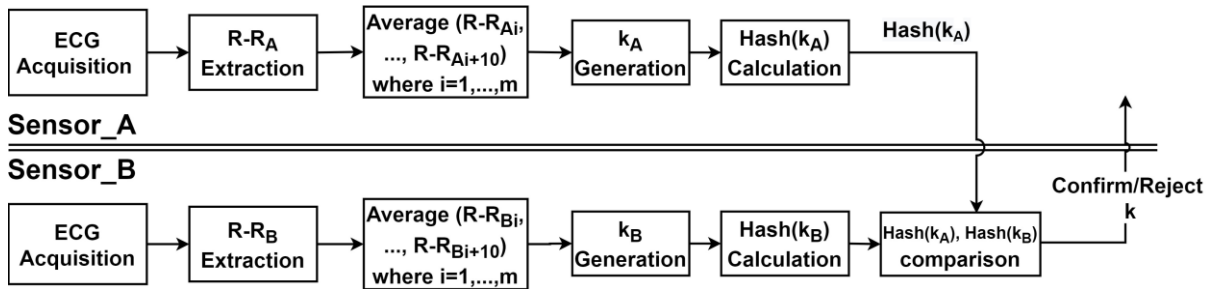
الخطوة الثانية: كما هو ملاحظ، فإن قيم عناصر المصفوفة X_A التي دليلها يساوي إحدى قيم Max_F_A في نهاية الخطوة الأولى تكون مختلفة عن القيم العشوائية بشكل ملحوظ، ويمكن تمييزها بسهولة. لحمايتها من الفضح في أثناء إرسال X_A إلى الحساس B نُعمي في هذه المرحلة عناصر المصفوفة X_A التي دليلها يساوي إحدى قيم عناصر المصفوفة Max_F_A (أي إحدى مؤشرات القيم) مع العنصر السابق أو التالي؛ باستخدام خوارزمية TEA مع المفتاح k المكون من 4 قيم من نمط uint32. تم اختيار الخوارزمية TEA؛ لأنها خوارزمية التعمية الأبسط (كما ورد سابقاً)، وهي تقوم بتعمية كتل كل منها مكون من عنصرين من نمط uint32. بالتالي لا يمكننا تعمية فقط قيم $R-R_A$ من المصفوفة X_A ، وإنما يتم تعمية هذه القيم مع عنصر سابق أو تالٍ لها. لا تُعمى جميع عناصر X_A ؛ وذلك من أجل توفير الزمن وطاقة المعالجة. بعد القيام بعملية التعمية سنلاحظ عدم إمكانية التمييز بين القيم العشوائية، والقيم الناتجة عن التعمية.

- يتم القيام بعملية التعمية باستخدام المفتاح k وفق الخطوات التالية والموضحة أيضاً في الشكل 4-5 ب:
- إذا كان دليل العنصر المراد تعميته فردياً، يُعمى مع العنصر السابق له (وهو قيمة عشوائية).
 - إذا كان دليل العنصر المراد تعميته زوجياً، يُعمى مع العنصر التالي له (وهو قيمة عشوائية).
 - إذا كان هناك عنصران متتاليان يجب تعميتهما، وكان الأول زوجياً والثاني فردياً، يُعميان معاً مرة واحدة فقط.

يجب توليد المفتاح k بحيث يكون متطابقاً في كلا الحساسين. يُنفَّذ مخطط ECG-AKES عدد غير محدد من الدورات، ويتم تبادل مفتاح سري جديد في كل دورة. كما تُحدّد قيمة k بحيث تكون أيضاً مختلفة من أجل كل دورة تنفيذ. من أجل تحديد قيمة k نميّز الحالتين الآتيتين:

الحالة الأولى: في دورة التنفيذ الأولى للمخطط ECG-AKES. يُحسب k اعتباراً من قيم R-R المسجلة كما في المخطط المبين في الشكل 4-7. يُحسب وسطي كل عشر قيم متتالية لـ R-R في كلا الحساسين والمقاسة بشكل متزامن بدءاً من لحظة زمنية معينة. ثم يُستخلص ثاني رقم بعد الفاصلة لكل من القيم الناتجة، وذلك بعد تقريب الوسطي إلى أقرب رقمين بعد الفاصلة. تُكرّر العملية m مرة وبالتالي يتم التوصل إلى m رقم، ثم تُجمّع الأرقام المستخلصة بشكلٍ متتالي وتُستخدم كمفتاح. وكما ذكرنا سابقاً، يتكون المفتاح k من أربعة مفاتيح جزئية، وعليه، تُجرى عملية التجميع بحيث تُملأ المراتب الدنيا (الآحاد) أولاً من المفاتيح الجزئية الأربعة على التتالي، ثم تُملأ المرتبة الأعلى (العشرات) من كل مفتاح جزئي على التتالي، وهكذا. على سبيل المثال، إذا كان وسطي كل عشر قيم متتالية لـ R-R بعد التقريب إلى أقرب رقمين بعد الفاصلة كما يأتي (من اليسار إلى اليمين):

$k = \{0.86, 0.88, 0.86, 0.83, 0.82, 0.85\}$ ، بالتالي يكون المفتاح الناتج $k = \{26, 58, 6, 3\}$.



الشكل 4-7: توليد المفتاح k في الدورة الأولى لتنفيذ مخطط ECG-AKES.

بناءً على التجربة العملية وبما أن الحساسين موضوعان على الجسم نفسه، تكون فرصة تطابق k بين الحساسين لا بأس بها. سنرمز للمفتاح المتشكل في الحساس A بالرمز k_A والمفتاح المتشكل في الحساس B بالرمز k_B . لكي نتحقق من أن $k_A = k_B = k$ ، يقوم الحساس A بحساب ناتج تطبيق تابع البصمة على k_A أي $\text{Hash}(k_A)$ ويُرسِل الناتج إلى الحساس B الذي بدوره يُحسب المفتاح k_B بطريقة حساب k_A نفسها، ثم يُحسب $\text{Hash}(k_B)$. إذا تحقق الشرط $\text{Hash}(k_B) = \text{Hash}(k_A)$ يُرسِل الحساس B إلى الحساس A رسالة تؤكد التطابق، ولتكن عبارة عن ثلاثة بتات ذات القيمة 1 أي (111). أما في حال عدم تحقق الشرط، فيُرسِل الحساس B إلى الحساس A رسالة تؤكد عدم التطابق، ولتكن عبارة عن ثلاثة بتات ذات القيمة 0 أي (000). في حال عدم التطابق يجب إعادة تشكّل k من جديد، واختباره مرة أخرى إلى أن يتحقق الشرط $k_A = k_B = k$.

لا يمكن استخدام طريقة تبادل المفاتيح هذه بدلاً من مخطط ECG-AKES للأسباب الآتية: أولاً، قد نضطر لتطبيق هذه الطريقة مرات عدّة إلى أن نتوصل إلى مفتاح k مشترك بين الحساسين، وذلك بسبب عدم التطابق بين قيم $R-R$ المقاسة على التزامن في الحساسين، فهي متقاربة، ولكن ليست متطابقة. يؤدي ذلك إلى استهلاك كبير للطاقة والزمن. ثانياً، تحتاج هذه الطريقة إلى زمن تحصيل إشارة كبير جداً. ثالثاً، قد تكون المفاتيح الناتجة غير عشوائية بما يكفي. ورغم نقاط الضعف المذكورة، إلا أن استخدام هذه الطريقة في سياق المخطط المقترح لن يؤدي إلى إضعافه أو تقليل أمانه.

الحالة الثانية: عند تنفيذ المخطط بدءاً من الدورة الثانية وما بعدها، نجعل قيمة k مساوية لقيمة المفتاح السري المشترك KEY المتفق عليه بين الحساسين في دورة التنفيذ السابقة. فإذا كانت دورة التنفيذ الحالية هي الدورة i ، نجعل قيمة k مساوية لقيمة KEY_{i-1} أو لجزء منه. إذا كان طول KEY المتفق عليه في الدورة السابقة أكبر من 128 bit نجعل قيمة k مساوية لجزء منه أي مساوية للقيمة الناتجة عن اقتطاع 128 bit ذات المرتبة الأعلى من KEY_{i-1} .

الخطوة الثالثة: لزيادة أمان المخطط المقترح وحمايته من هجوم الرجل في الوسط، تُنفَّذ في هذه الخطوة عملية تبديل مواضع عناصر المصفوفة X_A . بدايةً، تولّد مصفوفة إعادة الترتيب (permutation array) ذات r عشرة عناصر ثم تُكوّن مصفوفة إعادة الترتيب النهائية R ذات 200 عنصر؛ بالاعتماد على r . تُكوّن المصفوفة r بناءً على رقم دورة تنفيذ المخطط. وهنا نميز الحالتين الآتيتين:

الحالة الأولى: في الدورتين الأولى والثانية لتنفيذ ECG-AKES، تولّد r اعتباراً من قيم $R-R$ بطريقة مشابهة لتوليد k . أي يتم حساب وسطي كل عشر قيم متتالية لـ $R-R$ ثم يُؤخذ ثاني رقم بعد الفاصلة لكل من القيم الناتجة وذلك بعد تقريب الوسطي الناتج إلى أقرب رقمين بعد الفاصلة. ثم تُجمّع تلك الأرقام بشكل متتالي وتُهمل الأرقام المتكررة. في حال عدم ورود بعض القيم من 1 حتى 9 تُمأَل العناصر الفارغة بالقيم التي لم تظهر وذلك بشكل متسلسل. يتم التأكد من الحصول على المصفوفة r نفسها لدى الحساسين، باستخدام توابع البصمة بطريقة تشبه طريقة التحقق من تطابق k . كمثال حول تشكيل المصفوفة r ، بفرض لدينا 60 قيمة $R-R$ وكان ناتج حساب وسطي كل عشر

قيم، وتقريب كل ناتج إلى أقرب رقمين بعد الفاصلة كما يأتي: 0.85, 0.82, 0.83, 0.86, 0.88, 0.86. تكون المصفوفة r على الشكل الآتي: {6,8,3,2,5,0,1,4,7,9}. ويبين الشكل 4-8 توضيحاً للمثال السابق حول تشكيل r في الدورتين الأولى والثانية.

0.86	0.88	0.86	0.83	0.82	0.85
↓	↓	↓	↓	↓	↓
6	8	6	3	2	5
✓	✓	x	✓	✓	✓

$r =$

6	8	3	2	5	0	1	4	7	9
---	---	---	---	---	---	---	---	---	---

الشكل 4-8: مثال حول تشكيل المصفوفة r في الدورتين الأولى والثانية للتنفيذ.

الحالة الثانية: بدءاً من الدورة الثالثة لتنفيذ المخطط وما بعدها. تُولّد r باستخدام المفتاح السري المشترك KEY المتفق عليه بين الحواسين في الدورة قبل السابقة من دورات تنفيذ المخطط. أي إذا كان رقم الدورة الحالية هو i تُشكّل المصفوفة r اعتباراً من KEY_{i-2} ويتم ذلك وفق الخطوات الآتية وكما هو مبين في المثال الموضح في الشكل 4-9:

KEY _{i-2} =	0101	0011	1100	0001	0010	0111	0100	0000	0111	0110	1001	1000	...
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
	5	3	12	1	2	7	4	0	7	6	9	8	
	✓	✓	x	✓	✓	✓	✓	✓	x	✓	✓	✓	

$r =$

5	3	1	2	7	4	0	6	9	8
---	---	---	---	---	---	---	---	---	---

الشكل 4-9: مثال حول تشكيل المصفوفة r اعتباراً من KEY_{i-2} .

- بدايةً يُؤخذ كل أربعة بتات متتالية من KEY_{i-2} بدءاً من اليسار ويُقرأ الرقم العشري الناتج. إذا كان ضمن المجال من 0 حتى 9 ولم يظهر سابقاً، يُضاف إلى المصفوفة r . أما إذا كان أكبر من 9 أو ظهر سابقاً فيتم تجاهله. تتم الإضافة بدءاً من العنصر ذي الدليل الأدنى وحتى العنصر ذي الدليل الأعلى.
- تُكرّر العملية السابقة حتى تمتلئ المصفوفة r بقيم عشرية من 0 حتى 9 بترتيب عشوائي، أي حتى نحصل على مصفوفة إعادة ترتيب ذات عشرة عناصر. عند امتلاء العناصر العشرة للمصفوفة نتوقف عن التكرار.

- إذا انتهت قراءة جميع بتات المفتاح بالطريقة الموضحة ولم تظهر جميع القيم من 0 حتى 9، تُملأ الخانات الفارغة المتبقية بالأرقام التي لم تظهر؛ وذلك بشكلٍ متتالٍ.

خوارزمية 4-1: شبه الرماز لعملية توليد مصفوفة إعادة الترتيب R.

```

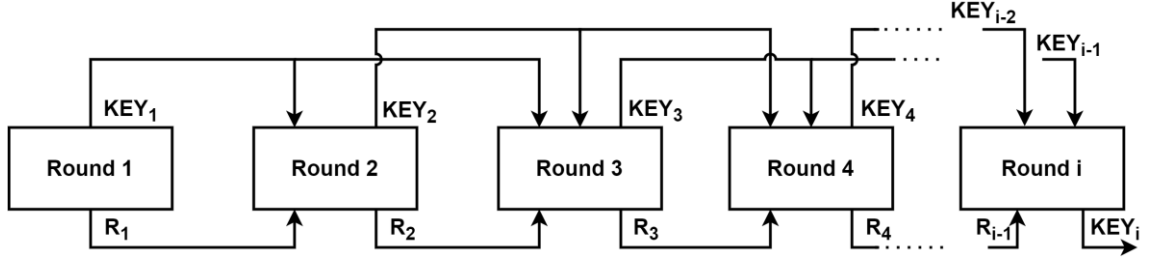
Input:
r, Ri-1, R={0,1,...,199}
Output:
permuted R

for j ← 0 to 19 do
{
    permute R[j*10] to R[j*10+9] based on r
}
for k ← 0 to 198 do
{
    x ← ((R[k] + Ri-1[k]) * R[k+1]) % 200
    swap(R[k],R[x])
}
x ← ((R[199] + Ri-1[199]) * R[k-1]) % 200
swap(R[199],R[x])

```

بعد توليد r ، تُشكّل مصفوفة إعادة الترتيب النهائية، R . أولاً، تُملأ عناصر R بالأرقام من 0 حتى 199 على التتالي، ثم تُجرى عملية إعادة الترتيب الأولية، حيث يُعاد ترتيب كل عشرة عناصر متتالية؛ باستخدام r . بعد ذلك، يُعاد ترتيب عناصر R الناتجة مرة أخرى بناءً على قيمها الحالية وقيم R في جولة التنفيذ السابقة؛ أي إذا كانت جولة التنفيذ الحالية هي i ، يُعاد ترتيب عناصر R بناءً على قيم عناصرها الحالية وعلى R_{i-1} . من أجل الجولة الأولى حيث $i=1$ تكون R_0 عبارة عن مصفوفة صفرية أي جميع عناصرها أصفار. تُوضّح خوارزمية 4-1 طريقة توليد R من خلال شبه الرماز (pseudocode) لتلك العملية.

يُوضّح الشكل 4-10 جولات تنفيذ المخطط المقترح والعلاقة بينها. كما ذكرنا للتو، من أجل توليد قيم k و R للجولة الحالية، تُستخدَم كل جولة؛ باستثناء الجولة الأولى والجولة الثانية مفاتيح KEY ناتجة عن الجولتين السابقتين، كما تُستخدَم أيضاً مصفوفة إعادة الترتيب R المؤدّة في جولة التنفيذ السابقة. بالنسبة للجولة الثانية فهي تُستخدَم المفتاح الذي تم إنشاؤه في الجولة الأولى فقط. أما بالنسبة للجولة الأولى فقد بيّنا طرق توليد قيم k و R فيها.



الشكل 4-10: دورات تنفيذ ECG-AKES والعلاقة بينها.

الخطوة الرابعة: إرسال المصفوفة X_A من الحساس A إلى الحساس B.

❖ المرحلة الرابعة

في هذه المرحلة، تُستنتج القيم المشتركة بين الحساسين في الحساس B، ومن ثم تُشكّل المجموعة S_B ، ثم تُشكّل

المصفوفة X_B وترسل إلى الحساس A. تتألف هذه المرحلة من الخطوات الآتية:

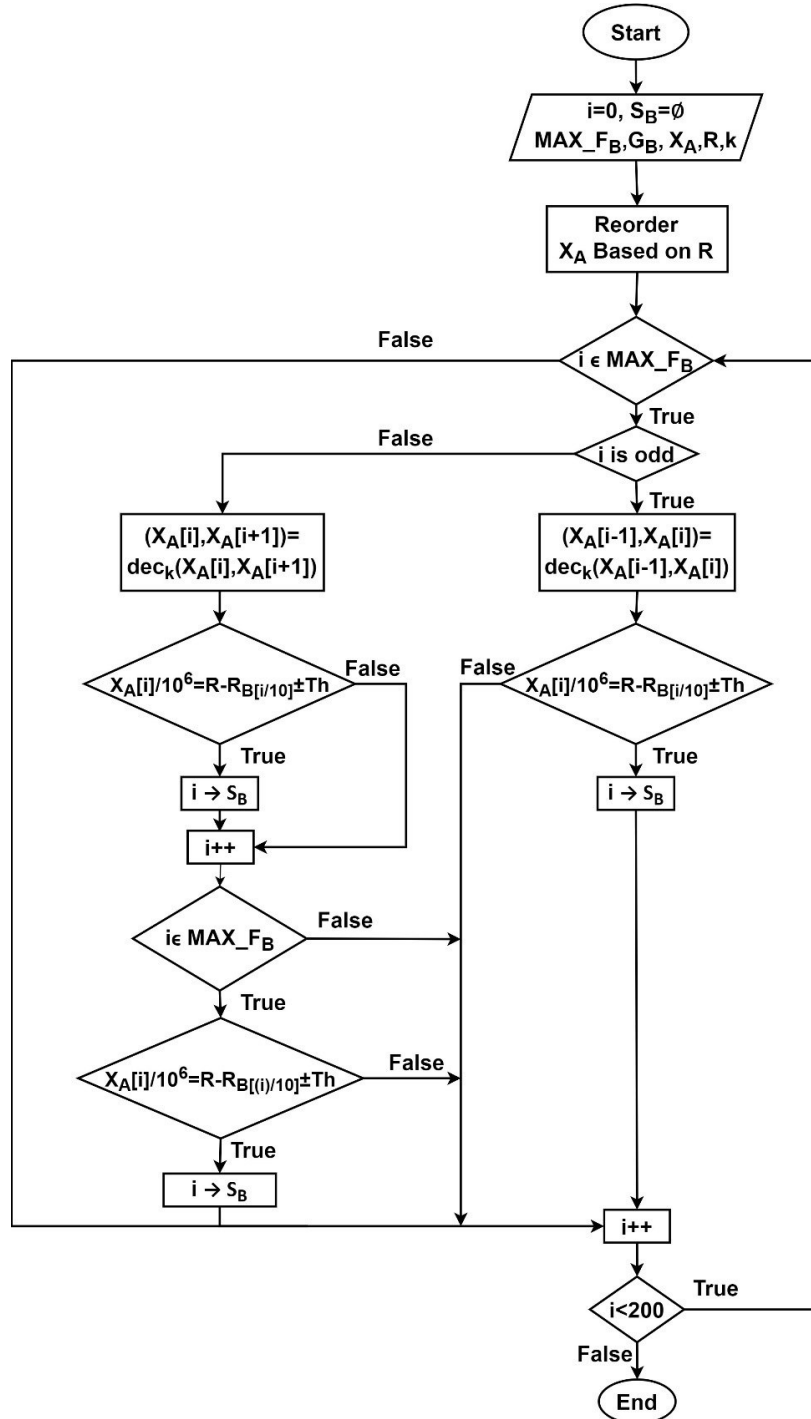
الخطوة الأولى: استنتاج مجموعة القيم المشتركة S_B في الحساس B. وذلك وفق المراحل الآتية:

- إعادة ترتيب المصفوفة X_A إلى ترتيبها الأصلي بالاعتماد على R.
- فك تعمية العناصر المُعمّاة في المصفوفة X_A ، ومقارنتها مع قيم عناصر G_B كما يأتي:
 - العنصر الذي دليله يساوي إحدى قيم عناصر المصفوفة Max_F_B (أي إحدى مؤشرات القمم المستنتجة في الحساس B) يُفكّ تعميته؛ وفق خوارزمية TEA بالمفتاح k المتفق عليه بين الحساسين. يُفكّ تعمية العنصر مع العنصر السابق أو التالي له؛ وذلك وفق ما يأتي:
 - إذا كان دليل العنصر المراد فك تعميته فردياً، يُفكّ تعميته مع العنصر السابق له.
 - إذا كان دليل العنصر المراد فك تعميته زوجياً، يُفكّ تعميته مع العنصر التالي له.
 - إذا كان هناك عنصران متتاليان يجب فك تعميتهما، وكان الأول زوجياً والثاني فردياً، يجب فك تعميتهما معاً مرة واحدة فقط.

بعدها تُقارن القيم الناتجة عن فك التعمية مع عناصر G_B كما يأتي: إذا كان دليل العنصر الذي تم فك تعميته هو

i ، تُقسّم $X_A[i]$ على 10^6 ، ومن ثم تُقارن بالعنصر $R - R_{B[(int)(i/10)+1]}$ من المجموعة G_B . إذا كان الاختلاف بينهما

أقل أو يساوي عتبة معينة نرمز لها بـ Th ، يُضاف دليل العنصر i إلى المجموعة S_B . أما إذا كان الاختلاف بينهما أكبر من العتبة Th ؛ فإن قيمة الدليل i هي ليست إحدى مؤشرات القيم المشتركة بين الطرفين، ويتم إهمالها.



الشكل 4-11: تسلسل عمل الخطوة الأولى من المرحلة الرابعة في ECG-AKES.

أي إذا كان مؤشر القمة i مشتركاً بين Max_F_B و Max_F_A ، فإن قيمة العنصر i من المصفوفة X_A بعد فك التعمية والتقسيم على 10^6 يساوي العنصر $R - R_A[(int) (i / 10) + 1]$ من G_A والذي يجب أن يكون مساوياً

لذلك، فإن Th تمثل عتبة الاختلاف المقبول بين كل عنصر في G_A والعنصر المقابل له في G_B .

مما سبق، يكون من الواضح أننا تمكنا من اكتشاف مؤشرات القيم المشتركة، وإضافتها إلى المجموعة S_B . أما باقي عناصر X_A فيتم تجاهلها. ويبين الشكل 4-11 تسلسل عمل الخطوة الأولى من المرحلة الرابعة.

في مثالنا التوضيحي، حيث قيمة Max_F_B موضحة في المثال الموجود في الخطوة الأولى من المرحلة

الأولى، تُجرى عمليات تشكيل S_B كما هو موضح في الشكل 4-12، وذلك بعد إعادة ترتيب المصفوفة X_A .

index	Value		
0	$E_K(RBS_{A0}, R-R_{A1})$	$\rightarrow D_K(X_A[0], X_A[1]) = Y[0], Y[1]$	$\rightarrow \text{Add 1 to } S_B$
1		$Y[1]/10^6 = R-R_{A1} = R-R_{B1} \pm Th$	
2	RBS_{A2}	$\rightarrow D_K(X_A[2], X_A[3]) = Y[2], Y[3]$	
3	RBS_{A3}	$Y[2]/10^6 \neq R-R_{B1} \pm Th$	
4	RBS_{A4}		
5	RBS_{A5}		
6	$E_K(R-R_{A1}, RBS_{A7})$	$\rightarrow D_K(X_A[6], X_A[7]) = Y[6], Y[7]$	$\rightarrow \text{Add 6 to } S_B$
7		$Y[6]/10^6 = R-R_{A1} = R-R_{B1} \pm Th$	
8	$E_K(R-R_{A1}, RBS_{A9})$	$\rightarrow D_K(X_A[8], X_A[9]) = Y[8], Y[9]$	$\rightarrow \text{Add 8 to } S_B$
9		$Y[8]/10^6 = R-R_{A1} = R-R_{B1} \pm Th$	
10	RBS_{A10}		
11	RBS_{A11}		
12	$E_K(RBS_{A12}, R-R_{A2})$	$\rightarrow D_K(X_A[12], X_A[13]) = Y[12], Y[13]$	$\rightarrow \text{Add 13 to } S_B$
13		$Y[13]/10^6 = R-R_{A2} = R-R_{B2} \pm Th$	
...	...	...	...
199	RBS_{A199}		

الشكل 4-12: تشكيل المجموعة S_B بعد عملية إعادة ترتيب X_A في المرحلة الرابعة بحسب مثالنا.

وعليه، تكون المجموعة S_B هي كالآتي:

$$S_B = \{1, 6, 8, 13, 27, 35, 41, 49, 55, 63, 69, 77, 83, 91, 104, 105, 118, 132\}$$

بالنسبة للعناصر ذات الدليل 2 و 94 فلن يتطابق ناتج فك تعميتهما مع قيم $R-R_B$ المقابلة، أما العناصر ذات الدليل

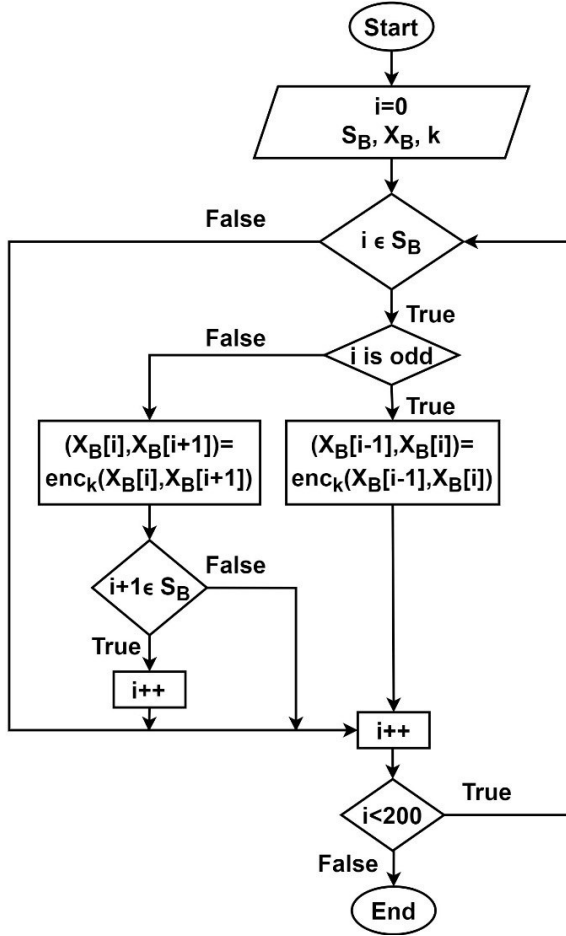
90 و 33 فلن يُفكَّ تعميتهما. من الشكل 4-12 نلاحظ أنه كي يُضاف عنصر ما إلى S_B يجب أن يتحقق الشرط

$$R-R_{A_j} = R-R_{B_j} \pm Th$$

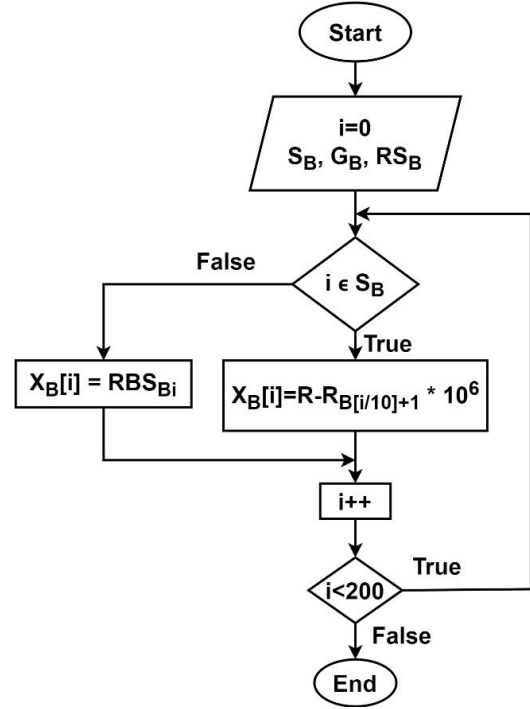
الخطوة الثانية: في هذه الخطوة، تُشكّل المصفوفة X_B في الحساس B بشكل مشابه لتشكيل المصفوفة X_A ، ولكن

بالاعتماد على المجموعة S_B ، وعلى المجموعة G_B . تتكون المصفوفة X_B أيضاً من 200 عنصر، كلّ منها عبارة

عن قيمة من نمط `uint32_t`. تُملأ عناصر المصفوفة X_B بالشكل الآتي:



ب. الخطة الثالثة



أ. الخطة الثانية

الشكل 4-13: تسلسل عمل الخطوتين الثانية والثالثة من المرحلة الرابعة في ECG-AKES.

- تُملأ العناصر التي دليلها يساوي إحدى قيم عناصر S_B بإحدى قيم R-R من المجموعة G_B ، كما في

العلاقة (4-12):

$$X_B[i] = R_{R_B[(int)(i/10)+1]} \times 10^6 \quad \text{If } i \in S_B \quad (4-12)$$

حيث i هو دليل العنصر في المصفوفة X_B .

- تُملأ باقي العناصر بقيم عشوائية.

وبين الشكل 4-13-أ تسلسل عمل الخطوة الثانية من المرحلة الرابعة. وبحسب مثالنا وقيم S_B ، تكون العناصر

الأولى للمصفوفة X_B عند نهاية هذه الخطوة، كما في الشكل 4-14.

index	value
0	RBS_{B0}
1	$R-R_{B1} \times 10^6$
2	RBS_{B2}
3	RBS_{B3}
4	RBS_{B4}
5	RBS_{B5}
6	$R-R_{B1} \times 10^6$
7	RBS_{B7}
8	$R-R_{B1} \times 10^6$
9	RBS_{B9}
10	RBS_{B10}
11	RBS_{B11}
12	RBS_{B12}
13	$R-R_{B2} \times 10^6$
...	...
200	RBS_{B199}

الشكل 4-14: عناصر X_B في نهاية الخطوة الثانية من المرحلة الرابعة بحسب مثالنا.

الخطوة الثالثة: تُعمى في هذه الخطوة عناصر المصفوفة X_B التي دليلها يساوي إحدى قيم عناصر S_B مع العنصر السابق أو التالي؛ وفق TEA؛ باستخدام المفتاح k المتفق عليه بين الحاسابين باتباع الخطوات الآتية والموضحة في الشكل 4-13-ب:

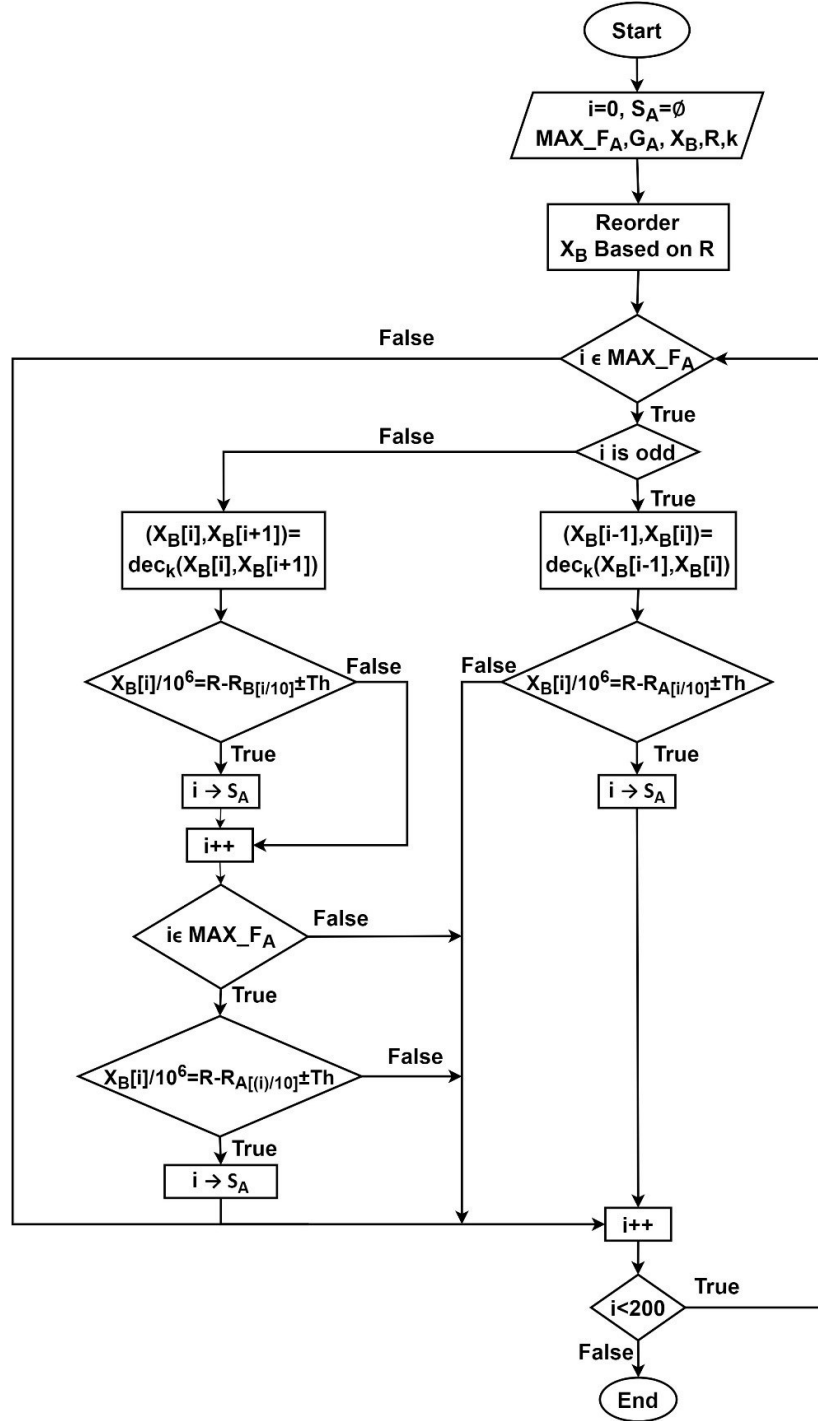
- إذا كان دليل العنصر المراد تعميته فردياً، يُعمى مع العنصر السابق له (وهو قيمة عشوائية).
- إذا كان دليل العنصر المراد تعميته زوجياً، يُعمى مع العنصر التالي له (وهو قيمة عشوائية).
- إذا كان هناك عنصران متتاليان يجب تعميتهما، وكان الأول زوجياً والثاني فردياً، يجب تعميتهما معاً مرة واحدة فقط.

الخطوة الرابعة: إعادة ترتيب المصفوفة X_B ، وفق مصفوفة إعادة الترتيب R المتفق عليها بين الحاسابين.

الخطوة الخامسة: إرسال المصفوفة X_B إلى الحساس A .

❖ المرحلة الخامسة

في هذه المرحلة، تُستنتج القيم المشتركة بين الحاسابين في الحساس A ، ومن ثم تُشكّل المجموعة S_A . وتتألف هذه المرحلة من العمليات الآتية:



الشكل 4-15: تسلسل عمل المرحلة الخامسة في ECG-AKES.

- إعادة ترتيب المصفوفة X_B إلى ترتيبها الأصلي؛ بالاعتماد على R .
- فك تعمية العناصر المُعمّاة في المصفوفة X_B ، ومقارنتها مع قيم G_A كما يأتي:
 - العنصر الذي دليله يساوي إحدى قيم عناصر المصفوفة Max_F_A يُفكّ تعميته وفق خوارزمية TEA بالمفتاح k . يُفكّ تعمية العنصر مع العنصر السابق أو التالي له؛ وذلك وفق ما يأتي:

- إذا كان دليل العنصر المراد فك تعميته فردياً، يُفك تعميته مع العنصر السابق له.
- إذا كان دليل العنصر المراد فك تعميته زوجياً، يُفك تعميته مع العنصر التالي له.
- إذا كان هناك عنصران متتاليان يجب فك تعميتهما، وكان الأول زوجياً والثاني فردياً، يجب فك تعميتهما معاً مرة واحدة فقط.

تُقارن القيمة الناتجة عن فك التعمية مع عناصر G_A كما يأتي: إذا كان دليل العنصر الذي تم فك تعميته هو i ، تُقسَّم $X_B[i]$ على 10^6 ومن ثم تُقارن بالعنصر $R-R_{A[(int)(i/10)+1]}$ من المجموعة G_A . إذا كان الاختلاف بينهما أقل أو يساوي العتبة Th ، يُضاف دليل العنصر i إلى المجموعة S_B . أما إذا كان الاختلاف بينهما أكبر من العتبة Th ، فإن قيمة الدليل i ليست إحدى مؤشرات القمم المشتركة بين الطرفين ويتم إهمالها. يبين الشكل 4-15 تسلسل عمل المرحلة الخامسة.

في مثالنا التوضيحي، حيث قيمة Max_F_A موضحة في المثال الموجود في الخطوة الأولى من المرحلة الأولى، وبعد إعادة ترتيب المصفوفة X_B ، يتم إجراء عمليات تشكيل S_A كما هو موضح في الشكل 4-16.

index	value		
0	$E_K(RBS_{B0}, R-R_{B1})$	$\rightarrow D_K(X_B[0], X_B[1]) = Y[0], Y[1]$ $Y[1] / 10^6 = R-R_{B1} = R-R_{A1} \pm Th$	$\rightarrow$ Add 0 to S_A
1			
2	RBS_{B2}		
3	RBS_{B3}		
4	RBS_{B4}		
5	RBS_{B5}		
6	$E_K(R-R_{B1}, RBS_{B7})$	$\rightarrow D_K(X_B[6], X_B[7]) = Y[6], Y[7]$ $Y[6] / 10^6 = R-R_{B1} = R-R_{A1} \pm Th$	$\rightarrow$ Add 6 to S_A
7			
8	$E_K(R-R_{B1}, RBS_{B9})$	$\rightarrow D_K(X_B[8], X_B[9]) = Y[8], Y[9]$ $Y[8] / 10^6 = R-R_{B1} = R-R_{A1} \pm Th$	$\rightarrow$ Add 8 to S_A
9			
10	RBS_{B10}		
11	RBS_{B11}		
12	$E_K(RBS_{B12}, R-R_{B2})$	$\rightarrow D_K(X_B[12], X_B[13]) = Y[12], Y[13]$ $Y[13] / 10^6 = R-R_{B2} = R-R_{A2} \pm Th$	$\rightarrow$ Add 13 to S_A
13			
...	...	...	...
199	RBS_{B199}		

الشكل 4-16: تشكيل المجموعة S_A بعد عملية إعادة ترتيب X_B في المرحلة الخامسة بحسب مثالنا.

ومن ثم تكون المجموعة S_A في مثالنا هي كالآتي:

$$S_A = \{1, 6, 8, 13, 27, 35, 41, 49, 55, 63, 69, 77, 83, 91, 104, 105, 118, 132\}$$

بالنسبة للعناصر ذات الدليل 33 و90، فلن يتطابق ناتج فك تعميتهما مع قيم $R-R_A$ المقابلة.

نلاحظ تساوي المجموعتين S_A و S_B لدى الحساسين A و B. بالتالي حصلنا على الهدف المرجو، وهو تبادل مجموعة من القيم السرية المشتركة بين الحساسين.

❖ المرحلة السادسة

في هذه المرحلة وبعد أن أصبح لدى الحساسين مجموعة من القيم المشتركة، يُولد المفتاح السري المشترك في كل من الحساسين A و B اعتباراً من S_A و S_B ؛ وذلك تبعاً لخوارزمية التعمية المستخدمة.

4-6- النتائج والمناقشة حول مخطط ECG-AKES المطور

فيما يأتي نستعرض نتائج التطبيق العملي لمخطط تبادل المفاتيح المطور، ECG-AKES والتي من خلالها تمكّننا من تحديد العتبات المثلى للتطبيق. كما ناقش أمان هذا المخطط وأدائه ونظهر ميزاته الأساسية.

4-6-1. نتائج التطبيق العملي لمخطط ECG-AKES وتحديد العتبات المثلى

بدايةً نرغب أن ننوه إلى أن جميع الاختبارات على هذا المخطط أُجريت باستخدام بيانات ECG لأشخاص يعانون من عدم انتظام ضربات القلب. استُرجعت تلك البيانات من قاعدة البيانات MIT-BIH arrhythmia database [42]. أُختيرت بيانات أشخاص يعانون من عدم انتظام ضربات القلب لاختبار هذا المخطط؛ وذلك لأن المرض من شأنه أن يجعل التوصل إلى القيم المشتركة أكثر صعوبة. فكان من الواضح في بعض السجلات عدم التماثل بين الإشارتين المقاستين في حساسين موضوعين في مكانين مختلفين على الجسم نفسه. ومن ثم فإن نجاح المخطط المقترح من أجل تلك البيانات يعني نجاحه من أجل بيانات الأشخاص السليمين.

بيّنا في الفقرة السابقة أن مخطط ECG-AKES يسمَحُ باستنتاج مجموعة من القيم المشتركة بين الحساسات اعتباراً من مؤشرات المركبات الترددية العظمى. ولكن، لا بد من إجراء تجارب عملية لتحديد عدد تلك القيم، ومدى تغير هذا العدد بتغير العتبة Th ، والتي تمثل الاختلاف المقبول بين عنصرين متقابلين من المجموعتين G_A و G_B (أي قيمتين R-R) المتشكلتين من الإشارة المحصلة بالتزامن في حساسين مختلفين موضوعين على الجسم نفسه. وأيضاً، لا بدّ من دراسة مدى تغير هذا العدد فيما لو استُخدمت بيانات غير شرعية في أحد الحساسين؛ أي إشارة

ECG محصلة من جسم مختلف عن الجسم المدروس. وبناءً على ذلك نستطيع تحديد الحد الأدنى المقبول لعدد القيم المشتركة والذي من خلاله نحكم بصحةً وشرعية عملية التبادل. فضلاً عما سبق، يجب أن ندرس أيضاً قيمة العتبة Th، ومدى تأثيرها على عدد القيم المشتركة الناتجة، من أجل تحديد القيمة المثلى لها.

وفي الفقرات السابقة، بيّنا أننا نسعى إلى أن يكون المخطط المطوّر متسامحاً مع ضعف التزامن بين الحساسات؛ بالتالي لابد من إثبات ذلك عملياً، وتحديد مدى تأثير التزامن المطلوب بقيمة العتبة Th وتأثيره على عدد القيم المشتركة الناتجة.

انطلاقاً من هذين المطلبين أُجريت التجارب على هذا المخطط في حالتين: الأولى، من أجل حساسين مرتبطتين بالجسم نفسه، والثانية من أجل حساسين مرتبطتين بجسمين مختلفين، وذلك لتوضيح قدرة المخطط المطوّر على كشف التدخلات غير الشرعية التي يمكن أن تتعرض لها شبكة WBAN. بناءً عليه نحدد متوسطات الاختبار وفق ما يأتي:

- عدد التجارب المجرّاة 360 تجربة؛ باستخدام بيانات 12 شخصاً مختلفاً، بمعدل 30 تجربة لكل شخص؛ وفق أزمنة مختلفة لبدء تحصيل الإشارة، وذلك من أجل الاختبارات التي يكون فيها الحساسان موضوعين على الجسم نفسه.

- عدد التجارب المجرّاة 396 تجربة؛ باستخدام بيانات 12 شخصاً مختلفاً، وذلك من أجل الاختبارات التي يكون فيها الحساسان موضوعين على جسمين مختلفين. أُجريت 33 تجربة من أجل بيانات كل شخص مع بيانات الأشخاص الأحد عشر المتبقين من مجموعة الاختبار؛ وفق أزمنة مختلفة لبدء تحصيل الإشارة.

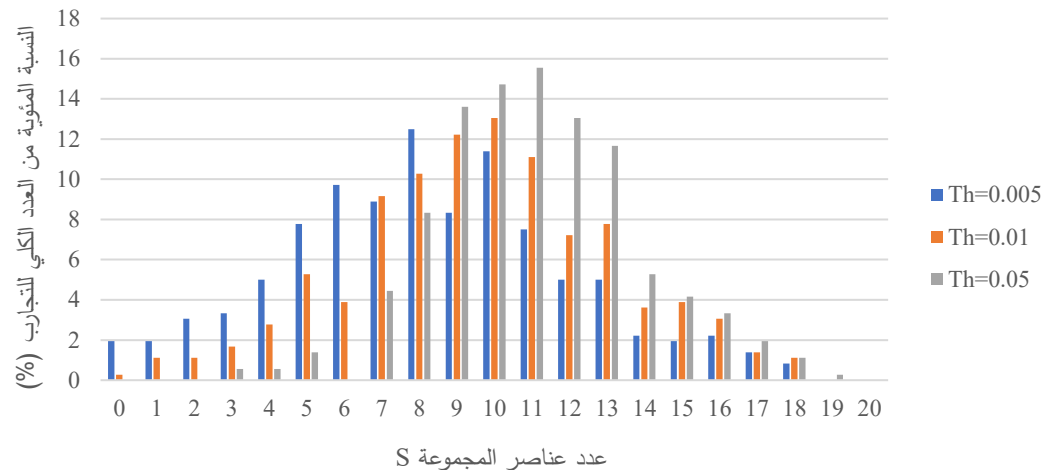
- تأخذ Th القيم 0.005، 0.01، و0.05 في جميع التجارب. أُختيرت تلك القيم لأن قيمة Th إذا كانت أصغر من 0.005 سيؤدي ذلك إلى عدم تطابق بين قيم R-R المحصلة على التزامن في حساسين مختلفين حتى ولو كانا ينتميان للجسم نفسه، وذلك مرفوض. أما إذا كانت قيمة Th أكبر من 0.05

سيؤدي ذلك إلى التطابق بين قيم R-R المحصلة في حساسين حتى ولو كان الحساسان ينتميان إلى جسمين مختلفين، وذلك مرفوضاً أيضاً.

- معدل أخذ عينات إشارة ECG في قاعدة البيانات المُستخدَمة (MIT-BIH arrhythmia database) [42] يساوي 360 عينة في الثانية.

- تطبيق FFT من أجل نافذة واحدة طولها 1024 عينة ECG للحصول على مؤشرات القمم (مؤشرات المركبات الترددية العظمى). أُختِيرَ هذا العدد من العينات؛ لأننا واعتماداً على التجربة، تبين لنا أن عدد مؤشرات القمم المشتركة بين الحساسين (عدد عناصر المجموعة S) والنتيجة عن FFT من أجل 2048 عينة يساوي إلى حد كبير عدد مؤشرات القمم المشتركة بين الحساسين والنتيجة عن FFT من أجل 1024 عينة. بالتالي لسنا بحاجة لتحصيل 2048 عينة؛ وإنما يمكننا أن نكتفي بـ 1024 عينة. أما اعتماد 512 عينة فهو غير كافٍ، حيث يجب أن نضمن وجود نبضة قلب واحدة على الأقل في الإشارة المحصلة، ولضمان ذلك يجب تحصيل العينات لمدة ثانيتين على الأقل وبالتالي الحصول على أكثر من 720 عينة. علماً أن عدد العينات في FFT يجب أن يكون من قوى العدد 2.

قبل البدء باختبار المخطط المطوّر، قمنا باختبار تطابق المركبة الترددية العظمى فقط الناتجة عن FFT من أجل 1024 عينة محصّلة بشكل متزامن في كل من الحساسين الموضوعين على الجسم نفسه، حيث اعتَمَدَت بعض الدراسات السابقة استخدام هذه القيمة فقط لتشكيل مجموعة الخصائص المشتركة بين الحساسين بدلاً من الاعتماد على مجموعة المركبات الترددية العظمى لنتائج FFT. ففي تلك الدراسات تُقسَم إشارة ECG إلى نوافذ وتُستَخْلَصُ مركبة ترددية واحدة فقط من كل نافذة، وهي المركبة الترددية العظمى، كخاصة من الخصائص المشتركة بين الحساسين. ولكن لدى تجريب ذلك عملياً، تبين أنه في 70% من التجارب المُجرّاة من أجل حساسين موضوعين على نفس الجسم، والتي عددها 360 تجربة، كانت قيمة المركبة الترددية العظمى الناتجة في أحد الحساسين مختلفة عن المركبة الترددية العظمى في الحساس الآخر.



أ- الحساسان متزانان وموضوعان على الجسم نفسه.



ب- الحساسان موضوعان على جسمين مختلفين.

الشكل 4-17: النسبة المئوية لعدد عناصر S المقاسة في حساسين مختلفين.

بدايةً ندرس عدد القيم السرية المشتركة المتشكلة بين الحساسين باستخدام مخططنا. يبين الشكل 4-17

النسب المئوية لعدد عناصر المجموعة S الناتجة حيث $S=S_A=S_B$ ، أي عدد القيم المشتركة المتشكلة بين الحساسين. في الشكل 4-17 أ تظهر النسب المئوية لعدد عناصر S في حال كان الحساسان موضوعين على الجسم نفسه. أما في الشكل 4-17 ب، فهي عندما يكون الحساسان موضوعين على جسمين مختلفين. أُجريت

التجارب من أجل كل من $Th=0.005$ ، و $Th=0.01$ ، و $Th=0.05$.

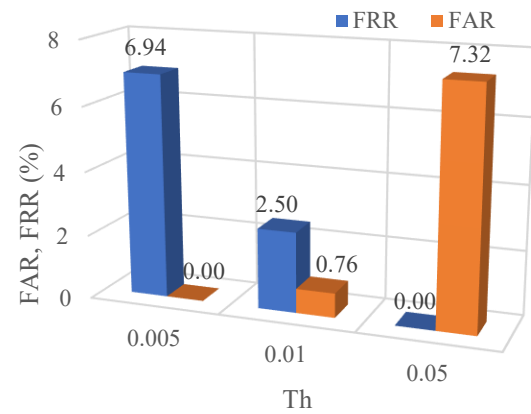
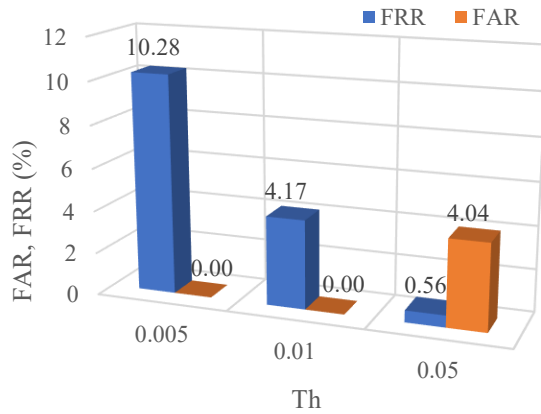
بدراسة الشكل 4-17 أ الذي يُظهر النتائج بالنسبة لحساسين موضوعين على الجسم نفسه، نلاحظ أنه

عندما $Th=0.005$ يكون عدد عناصر S صغيراً نسبياً. النسبة المئوية للتجارب التي كان فيها عدد عناصر

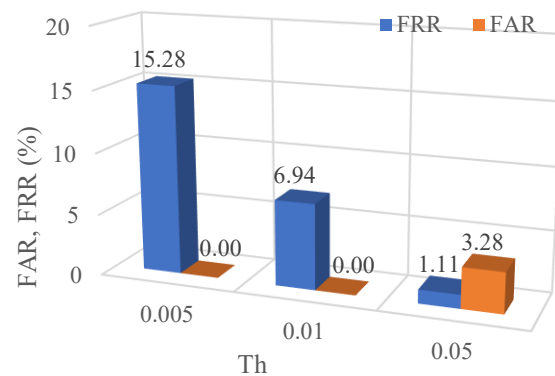
المجموعة S أقل من 3 عناصر هي 10.2% وهذه النسبة كبيرة جداً، وقد تجعل المخطط المقترح غير مجدي. من أجل $Th=0.01$ أعطت نتائج أفضل وعدد أكبر لعناصر المجموعة S. كما أن النسبة المئوية للتجارب التي فيها عدد عناصر S صغير جداً وبالتحديد أصغر من 3 عناصر هي 4.1% وذلك أفضل من النتيجة السابقة. أما بالنسبة لـ $Th=0.05$ فهي الأفضل من حيث عدد عناصر S المشتركة إذ إنها أظهرت أكبر عدد لعناصر S كما أن النسبة المئوية للتجارب التي كان فيها عدد عناصر S صغيراً جداً؛ أي أصغر من 3 هي 0.5%.

أما بدراسة الشكل 4-17-ب الذي يظهر النتائج بالنسبة لحساسين موضوعين على جسمين مختلفين، نلاحظ أنه عندما $Th=0.005$ فإن عدد عناصر S يكون صغيراً جداً، وفي معظم الأحيان يساوي 0 (وهو المطلوب). النسبة المئوية للتجارب التي كانت فيها المجموعة S أكبر من عنصرين هي 0%. من أجل $Th=0.01$ فأيضاً أعطت نتائج جيدة حيث كان عدد عناصر S صغيراً جداً أيضاً. كما أن النسبة المئوية للتجارب التي يكون فيها عدد عناصر S أكبر من 3 عناصر هي 0%. أما بالنسبة لـ $Th=0.05$ فهي الأسوأ حيث أظهرت أكبر عدد لعناصر S كما أن النسبة المئوية للتجارب التي كانت فيها عدد عناصر S أكبر من 3 هي 4%.

بناءً على التجارب نحدد عتبة العدد الأدنى لعناصر S المكوّنة بين الحساسين والتي من أجلها نحكم بنجاح عملية تبادل المفاتيح، والمصادقة. فإذا كان عدد عناصر S أقل من تلك العتبة؛ سيكون هناك شك في أن الحساسين موضوعان على الجسم نفسه. وكما هو واضح مما سبق أن هذه العتبة مرتبطة أيضاً بالعتبة Th . لتحديد عدد عناصر S التي تجعلنا نحكم بنجاح عملية تبادل المفاتيح، وفيما إذا كان الحساسان موضوعين على الجسم نفسه، ولتحديد العتبة Th ، سنعتمد على معيارين أساسيين، هما: معدل القبول الخاطئ FAR، ومعدل الرفض الخاطئ FRR. في مخططنا، FAR هو معدل قبول عقد خبيثة على أنها عقد شرعية في شبكة WBAN محددة، وبالتالي هو معدل تشكيل مفتاح سري مشترك مع عقد غير شرعية واعتبارها عقداً شرعيةً. FRR: وهو معدل رفض عقد شرعية من قبل عقد أخرى ضمن شبكة WBAN نفسها واعتبارها عقداً غير موثوقة، وبالتالي هو معدل رفض تشكيل مفتاح سري مشترك مع عقد شرعية.



أ- عندما يكون أصغر عدد مقبول لعناصر S هو عنصرين ب- عندما يكون أصغر عدد مقبول لعناصر S هو 3 عناصر



ت- عندما يكون أصغر عدد مقبول لعناصر S هو 4 عناصر.

الشكل 4-18: معدل القبول الخاطئ FAR ومعدل الرفض الخاطئ FRR في مخطط ECG-AKES.

يبين الشكل 4-18-أ كلاً من FAR و FRR وذلك إذا فرضنا العدد الأدنى المقبول لعناصر S الذي يدل

على أن الحساسين موضوعان على الجسم نفسه يساوي عنصرين. نلاحظ أنه عندما $Th=0.005$ ، فإن $FAR=0\%$ ،

ولكن $FRR=6.9\%$ وهذه نسبة مرتفعة. عندما $Th=0.01$ ، فإن $FAR=0.75\%$ ، ولكن $FRR=2.5\%$. أما عندما

$Th=0.05$ ، فإن $FAR=7.3\%$ و $FRR=0\%$.

يبين الشكل 4-18-ب كلاً من FAR و FRR وذلك إذا فرضنا العدد الأدنى المقبول لعناصر S الذي

يدل على أن الحساسين موضوعان على الجسم نفسه هو 3 عناصر. نلاحظ أنه عندما $Th=0.005$ ، فإن $FAR=0\%$ ،

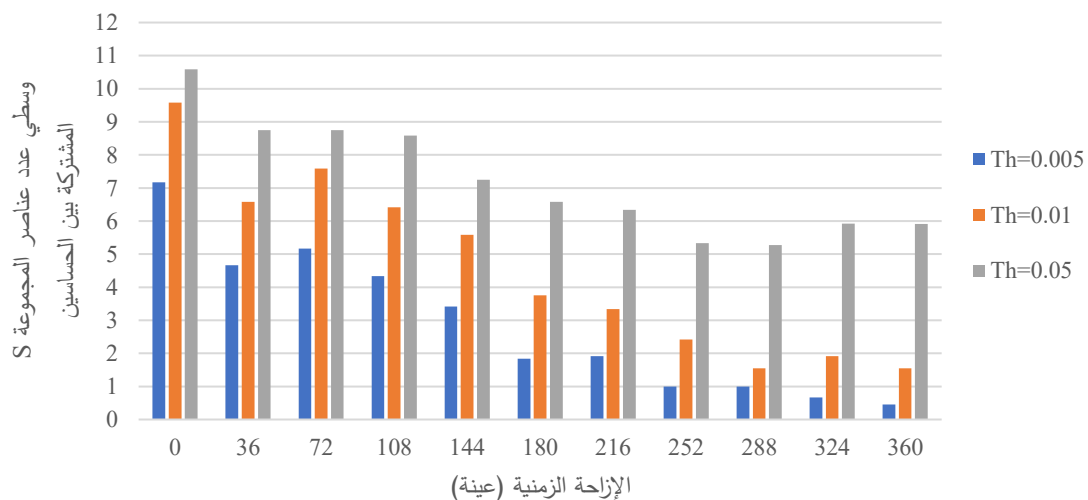
ولكن $FRR=10.2\%$ وهذه نسبة مرتفعة جداً. عندما $Th=0.01$ ، فإن $FAR=0\%$ ، ولكن $FRR=4.1\%$. أما عندما

$Th=0.05$ ، فإن $FAR=4\%$ و $FRR=0.5\%$.

يبين الشكل 4-18 ت كلاً من FAR و FRR وذلك إذا فرضنا العدد الأدنى المقبول لعناصر S الذي يدل على أن الحساسين موضوعان على الجسم نفسه هو 4 عناصر. نلاحظ أنه عندما $Th=0.005$ ، فإن $FAR=0\%$ ، ولكن $FRR=15.2\%$ ، وهذه نسبة مرتفعة جداً. عندما $Th=0.01$ ، فإن $FAR=0\%$ ، ولكن $FRR=6.9\%$. أما عندما $Th=0.05$ ، فإن $FAR=3.2\%$ و $FRR=1.1\%$.

مما سبق نلاحظ أنه كلما ازداد العدد الأدنى المقبول لعناصر S للحكم بصحة عملية تبادل المفاتيح ومصادقة الحساسات، سيكون FRR أكبر ومن ثم أسوأ. كما أننا نسعى إلى أن تكون $FAR=0\%$ ؛ لأننا لا نريد أن تُقبل حساسات غير شرعية على أنها عقد شرعية في الشبكة. بالمقابل فإن عدم قبول عقد شرعية في بعض الحالات (أي عندما $FRR > 0$)، لا يكون له الخطر نفسه، والأثر السلبي لقبول عقد غير شرعية؛ وإنما يؤدي حدوث ذلك إلى إعادة عملية تبادل المفاتيح مرة ثانية. ومن ثم نسعى إلى جعل $FAR=0\%$ ولو كان ذلك على حساب FRR. ونلاحظ أن أفضل نسبة FRR مقابل نسبة $FAR=0\%$ هي عندما $Th=0.01$ وأصغر عدد مقبول لعناصر S هو 3 عناصر.

أما بما يتعلق بالتزامن فقد درس مدى التسامح مع ضعف التزامن بين الحساسين من خلال حساب وسطي عدد قيم S الناتجة بين حساسين موضوعين على الجسم نفسه لدى كل إزاحة زمنية بينهما، كما هو مبين في الشكل 4-19.



الشكل 4-19: تسامح مخطط ECG-AKES مع ضعف التزامن بين حساسين موضوعين على الجسم نفسه.

لتحديد مدى التسامح مع ضعف التزامن أُجريت التجارب من أجل قيم Th المختلفة. عندما كان التزامن محققاً 100%، وعندما $Th=0.005$ كان وسطي عدد عناصر S هو 7، وعندما $Th=0.01$ كان وسطي عدد عناصر S هو 9.6 أما من أجل $Th=0.05$ ، فكان وسطي عدد عناصر S هو 10.6.

عندما $Th=0.005$ والعدد الأدنى لعناصر S هو 3، نلاحظ أنه وسطياً يصبح عدد عناصر S أصغر من 3؛ أي رفض تشكيل مفتاح سري بين الحساسين، عندما تكون الإزاحة الزمنية بين الحساسين أكبر من 144 عينة أي 0.4 ثانية. عندما $Th=0.01$ والعدد الأدنى لعناصر S هو 3، يبدأ الرفض اعتباراً من إزاحة زمنية أكبر من 216 عينة؛ أي أكبر من 0.6 ثانية. أما لو كانت $Th=0.05$ فحتى لو كانت الإزاحة الزمنية مساوية لثانية كاملة فسيكون عدد قيم S أكبر من 3.

الموسطات الأمثل لتطبيق مخطط ECG-AKES

من جميع التجارب السابقة نستنتج الموسطات الأمثل لتطبيق مخطط ECG-AKES، وهي: $Th=0.01$ ، والحد الأدنى المقبول لعدد عناصر S هو 3 عناصر. تؤدي هذه العتبات إلى $FAR=0\%$ و $FRR=4.1\%$ ؛ وذلك من أجل تزامن ضعيف، علماً أنه كلما ازداد التزامن كان عدد عناصر S أكبر.

4-6-2. أمان مخطط ECG-AKES

في المخطط المقترح، وكما ذكرنا سابقاً، نفترض أن حساسات WBAN متزامنة، وأن الحصول على إشارة ECG الخاصة بالمريض لا يمكن أن يتم إلا من قبل الكيانات المصرح لها بذلك. لذلك، فإن التهديدات التي تواجهها شبكة WBAN تأتي بشكل أساسي من الخصوم الذين يمكنهم التنصت على البيانات المتبادلة بين الحساسات، أو الخصوم القادرين على إقحام الرسائل أو إعادة إرسال الرسائل القديمة. وقد يحاول الخصوم أيضاً استخدام بيانات إشارة ECG التي تم تحصيلها من شخص آخر غير الشخص المُستهدف؛ وذلك بهدف كسر عملية تبادل المفاتيح. وبشكل عام، يمكن أن نستنتج أن المخطط المقترح يحقق:

- السرية: نتيجة تكوين مفتاح سري مشترك بين الطرفين.
- المصادقة: نتيجة التحقق من أن الحساسين المتصلين يقعان على الجسم نفسه.

• **الحدثة:** يمكن ضمان حداثة المفتاح، لأنه يتكون من قيم تم تحصيلها في لحظة حديثة محدّدة. فضلاً عن ذلك، لا يمكن لمهاجم يملك مفاتيح قديمة أن ينجح بالقيام بعملية التعمية أو فك التعمية باستخدامها؛ وذلك بسبب التغيير الدوري للمفتاح. لحِظنا من خلال التجارب العملية أن المفاتيح المتشكلة في الجسم نفسه ولكن في لحظتين مختلفين، تختلف اختلافاً كلياً فيما بينها (سيُبرهن ذلك في فصلٍ لاحق)؛ بسبب الاختلاف الحتمي بأكثر من قيمة من قيم عناصر S المتشكلة من بيانات الشخص نفسه، ولكن في لحظتين مختلفتين. فضلاً عن ذلك، وبسبب التباين الزمني لإشارة ECG، لن يُتاح للخصم فرصة استخدام سجلات ECG القديمة لشخص ما لتبادل مفتاح سري مع حساس شرعي للشخص نفسه.

مخطط ECG-AKES آمن ضد هجوم الرجل في الوسط (Man-in-the-middle attack)؛ وذلك بسبب عملية إعادة ترتيب عناصر X_A و X_B ، باستخدام R. لنفرض أنه تم إلغاء عملية إعادة الترتيب، من ثم إذا تمكّن المهاجم من التتصّل على X_A و X_B والتوصّل إلى k بطريقةٍ ما، ثم فك تعمية جميع عناصر X_A و X_B ، سيتمكن من العثور على عدد كبير من مؤشرات القمم المشتركة بين الحساسين. ومنه نستنتج أن عملية إعادة الترتيب تضيف أماناً لعملية التعمية باستخدام TEA، وبالمقابل زيادة أمان المخطط المقترح بأكمله.

يعتمد أمان عملية تبادل المفاتيح في مخططنا، كما ذكرنا للتوّ، على عملية التعمية وفق TEA، وعملية تبديل المواضع. طول مفتاح تعمية TEA (أي k) هو 128 bit، لذلك، فإنه يعطي مستوى أمان يعادل 128 bit. يمكن حساب مستوى الأمان المضاف بسبب تبديل مواضع عناصر المصفوفة X؛ وفق مصفوفة إعادة الترتيب R؛ باستخدام صيغة حساب الترتيب الآتية: $P(n,m)=n!/(n-m)!$. بما أن R تتكون من 200 عنصر، فإن $n=200$ و $m=200$ ويمثل $P(200,200)$ عدد المحاولات التي يحتاجها الخصم لفضح R، وهو يساوي رقماً ثنائياً من رتبة 2^{1245} . نتيجةً لذلك، تضيف عملية تبديل المواضع مستوى أمان قدره 1245 bit. نستنتج أن مستوى الأمان لعملية تبادل المفتاح السري؛ باستخدام ECG-AKES يساوي $1373 \text{ bit} = 1245 \text{ bit} + 128 \text{ bit}$.

المفاتيح السرية التي تُنشأ بواسطة ECG-AKES هي متغيرة مع الزمن، ويمكن تغييرها بشكل دوري. لإنشاء كل مفتاح سري جديد (KEY)، يُستخدَم مفتاح TEA جديد (k) ومصفوفة تبديل جديدة (R)، وهذا من شأنه أن يضيف مستوى عالٍ جداً من الأمان.

3-6-4. أداء مخطط ECG-AKES

يمكن أن يختلف زمن تنفيذ ECG-AKES؛ اعتماداً على دورة التنفيذ. بالنسبة للدورتين الأولى والثانية، يحتاج المخطط المقترح إلى تحصيل إشارة ECG لفترة زمنية كافية لتوليد k و r. تعتمد هذه الفترة على مستوى الأمان المطلوب في الدورتين الأولى والثانية من دورات تنفيذ المخطط. في الدورة الثالثة وما بعدها، يحتاج المخطط إلى تحصيل بيانات 21 نبضة لتوليد المجموعة G. لذلك، فإن زمن التحصيل اللازم يبلغ حوالي 17 ثانية، علماً أن معدل ضربات القلب الطبيعي لشخص بالغ في حالة الراحة يتراوح بين 60 و 100 نبضة في الدقيقة. كما يمكن عدّ زمن المعالجة مهماً أمام زمن التحصيل.

أما بالنسبة للطاقة المستهلكة في كل من الحساسين المتصلين، فهي تساوي الطاقة المطلوبة لإرسال واستقبال X، مضافاً إليها الطاقة المطلوبة لعمليات المعالجة، وهي بسيطة جداً مقارنة بتعقيد العمليات في الدراسات السابقة. يستخدم ECG-AKES عمليات بسيطة مثل FFT، وتعمية بضع بايتات، باستخدام خوارزمية تعمية بسيطة للغاية وهي TEA، وعمليات تبديل المواضع، وذلك بدلاً من العمليات الثقيلة مثل عمليات قفل وفك قفل Fuzzy Vault وإعادة بناء كثرات الحدود والتي تم استُخدِمت في الدراسات السابقة.

وبما يتعلّق بالتعقيد، يمكن حساب التعقيد الزمني (Time complexity) للمخطط المطوّر من خلال حساب التعقيد الزمني للوظائف الجزئية التي تُنفَّذ فيه. يتألف المخطّط من عمليات أساسية عدّة، وهي: تحويل فوريريه السريع، وعملية توليد سلاسل عشوائية، وعملية التعمية وفق TEA، وعملية تبديل المواضع. وبحساب تدوين O الكبرى (Big O Notation) نلاحظ أن التعقيد الزمني للمخطط المطوّر يساوي $O(1)$ ، وذلك لأن:

- التعقيد الزمني لتحويل فورييه السريع يساوي $O(n \log n)$ ، حيث n يساوي عدد العينات. وبما أن عدد العينات التي يُطبَّق عليها تحويل فورييه ثابت ويساوي 1024 عينة؛ بالتالي يكون التعقيد مساوياً $O(1)$.
 - سنثبت في الفصل القادم أن تعقيد عملية توليد السلاسل العشوائية المستخدمة يساوي $O(n)$ حيث n هو عدد القيم العشوائية المولدة. وبما أن عددها ثابت، بالتالي يكون تعقيد توليد القيم العشوائية مساوياً $O(1)$.
 - عملية التعمية وفق TEA هي عبارة عن خوارزمية تعمية كتلية، تعقيدها يساوي $O(1)$.
 - عملية تبديل المواضع تُجرى عدداً محدداً وثابتاً من المرات وبالتالي يكون تعقيدها مساوي $O(1)$.
- وعليه يكون التعقيد الزمني الكلي للمخطط بأكمله مساوي $O(1)$.

4-6-4. ميزات مخطط ECG-AKES

إضافةً إلى الأمان، يتمتع ECG-AKES بميزات عدّة نذكر منها:

- يمكن لأي حساس أن يتحقق من أن الحساس الآخر الذي يسعى لتشكيل اتصال آمن معه يقع على الجسم نفسه، وذلك من خلال عدد عناصر S المشتركة بينهما. فالحساس A يعتمد على عدد مؤشرات القمم المشتركة بينه وبين الحساس B ($\text{Max_F}_A \cap \text{Max_F}_B$) وعلى التشابه بين قيم $R-R$ المحصلة بشكل متزامن من أجل التحقق من شرعية الحساس B . ومع ذلك فإن عدم تطابق عدد قليل من قيم $R-R$ المتقابلة في G_A و G_B نتيجة تشوّه الإشارة في أحد الحساسين، لن يجعل المخطط يفشل في تحديد القيم المشتركة؛ وإنما سنفقد فقط بعضاً من تلك القيم. أما الاختلاف الكبير بين S_A و S_B ، فهو مؤشر على أن الحساس B ليس موثقاً وهو غير متصل بالجسم نفسه.
- يكفي أن يتشابه عدد محدد من مؤشرات القمم كي يعطي المخطط نتائج صحيحة، وليس بالضرورة أن تتشابه الغالبية العظمى منها.
- التسامح مع ضعف التزامن والذي أُثبت في فقرة سابقة.

- استُخدِمت القيم الفيزيولوجية لتحقيق الأهداف الآتية وهي: توليد المفتاح السري المشترك، وتحقيق عملية تبادل المفتاح بشكل آمن، والمصادقة.
- استفدنا من كل من الخصائص الزمنية لإشارة ECG، وهي الفاصل الزمني R-R، والخصائص الترددية لها، وهي مؤشرات قمم ناتج FFT. أُختيرت مؤشرات قمم FFT كخصائص للأسباب الآتية [13]:
 - (1) سهولة الاكتشاف مع تعقيد حسابي منخفض.
 - (2) تُميّز فيزيولوجية الشخص جيداً وبالتالي تُوفّر آلية مصادقة فعّالة وأساساً جيداً لتبادل المفاتيح.
 - (3) تتغيّر هذه الخاصة ديناميكياً مع الزمن.
- لا يشكل ترتيب الخصائص الترددية المكتشفة (مؤشرات القمم) أي عائق أمام التوصل إلى القيم المشتركة بين الحساسين.
- يعمل هذا المخطط على حساسات عدّة. ويكون المفتاح السري KEY المتشكل بين كل حساسين مختلفاً عن المفتاح السري المتشكل بين حساسين آخرين؛ وذلك بالاعتماد على اختلاف لحظة بدء قياس إشارة ECG التي يُشكّل المفاتيح اعتباراً منها.
- صُمّم هذا المخطط بطريقة تمكّننا من تغيير المفتاح السري المشترك KEY دورياً أو عند الطلب؛ مما يزيد الأمان.
- في المخطط المقترح لسنا بحاجة لتثبيت القيم في الحساسات مُسبقاً قبل تفعيل الشبكة؛ أي يعمل المخطط المقترح وفق طريقة التوصيل والتشغيل.
- لا تشكل الفترة الأولية لتكوين المفاتيح فترة خطر؛ لأن المخطط المقترح لا يفترض أن الفترة الأولية للتشغيل هي آمنة. حيث لا يتم إرسال بيانات المريض أو المفاتيح السرية، والقيم المشتركة بشكلها الصريح.
- في دراستنا اعتمدنا على قاعدة بيانات لأشخاص لديهم أمراض قلبية يعانون من عدم انتظام في ضربات القلب وبعض التشوهات في شكل إشارة ECG. وفي عددٍ من السجلات كان من الواضح عدم التطابق بين الإشارتين المقاستين من خلال حساسين موضوعين في مكانين مختلفين على الجسم نفسه. يشكل ذلك صعوبة في كشف

R-R، وفي الحصول على خصائص ترددية مشتركة. ولكن رغم ذلك استطعنا التوصل إلى النتائج المرجوة لدى تطبيق المخطط على تلك البيانات.

4-7- خاتمة

في هذا الفصل قمنا بما يأتي:

- بيّنا كيف تم استنباط وتطوير مخطط لاستنتاج مجموعة من القيم المشتركة ما بين عقدتين في شبكة WBAN، بحيث يمكن استخدام تلك القيم من قِبل خوارزميات التعمية لإنتاج المفاتيح المشتركة اللازمة.
- بيّنا أيضاً كيف تم استخدام الخصائص الترددية والزمنية لإشارة ECG من أجل الحصول على القيم المشتركة بين الحساسين من دون الحاجة إلى التزامن الدقيق في تحصيل عينات إشارة ECG.
- وضعنا المخططات المنهجية المساعدة للحصول على مجموعة القيم المذكورة أعلاه.
- أثناء استنباط وتطوير مخطط تبادل المفاتيح، ظهرت الحاجة إلى استخدام مولّد قيم عشوائية لدى كلّ حساس. ونظراً لأن مولّدات القيم العشوائية يمكن أن تكون متباينة من حيث آلية توليد القيم، ودقة العشوائية، وزمن التنفيذ، كان لا بد من التفكير في إيجاد مولّد قيم عشوائية يعتمد على القيم الحيوية ECG نفسها المُستخدمة في توليد مجموعة القيم المشتركة المستخدمة في إنشاء مفاتيح التعمية. نتج عن ذلك مادة جديدة تتطلب البحث والاستنتاج وهو ما سنقوم به في الفصل التالي.

الفصل الخامس

تطوير وتصميم نموذج مولد سلاسل عشوائية عالي الإنتاجية

مُعْتَمِد على الإشارة الحيوية ECG

140	1-5- تمهيد
140	2-5- أهداف تطوير مولّد السلاسل العشوائية المطلوب المُعْتَمِد على إشارة ECG
141	3-5- المبادئ العامّة لمولّد السلاسل العشوائية المطوّر المُعْتَمِد على إشارة ECG
142	4-5- مخطط مولّد السلاسل العشوائية المطوّر المُعْتَمِد على إشارة ECG
146	5-5- النتائج والمناقشة حول مولّد السلاسل العشوائية المطوّر المُعْتَمِد على إشارة ECG
147	1-5-5. أمان المولّد المطوّر ضد فضح إشارة ECG
149	2-5-5. اختبار العشوائية والتمييز
150	2-5-5. 1. اختبار العشوائية
154	2-5-5. 2. تحليل التميز
158	3-5-5. أداء مولّد السلاسل العشوائية المطوّر ومعدل إنتاجه
158	6-5- خاتمة

5-1-تمهيد

تُستخدَم مَوَلَّدات الأرقام شبه العشوائية لتوليد RBSs لشبكات WSN، ولكنها تعاني من الاستهلاك الكبير للموارد. أما بالنسبة لشبكات WBAN فيمكن الاستفادة من القيم الحيوية المُقاسة لتوليد RBSs ومن ثم الاستغناء عن الحاجة لتنفيذ PRNG في الحساسات. نتيجةً لذلك، يُفضَّل استخدام RBSs القائمة على القياسات الحيوية لحماية الموارد في شبكات WBAN. اعتَمَدَت العديد من الدراسات السابقة على إشارة ECG في توليد السلاسل العشوائية، وبالتحديد على قيم IPI. ولكن أُثْبِتَ أن استخدام الطرائق المُعتمَدة على قيم IPI يكون فعّالاً فقط من أجل توليد سلاسل عشوائية قصيرة تعمل كمتغير عشوائي. أما بالنسبة للطرائق التي تَعْتَمِد على قيم عِيَنات إشارة ECG، فهي أفضل من حيث الإنتاجية، ولكنها تحتاج لتنفيذ عمليات حسابية قد تؤدي إلى استهلاك طاقة الحساس. انطلاقاً من ذلك نسعى في هذا الفصل إلى تطوير وتصميم مولد سلاسل عشوائية عالي الإنتاجية بالاعتماد على إشارة ECG، يتمتع ببساطة العمليات بحيث يستهلك أقل قدر ممكن من موارد حساسات WBAN.

5-2-أهداف تطوير مَوَلَّد السلاسل العشوائية المطلوب المُعتمَد على إشارة ECG

نهدف في هذا الجزء من البحث إلى تطوير مَوَلَّد سلاسل عشوائية يعتمد على إشارة ECG في توليد RBSs ذات أطوال تتناسب مع أطوال القيم العشوائية المستخدمة في تطبيقات حماية المعلومات (أي من 128 bit وحتى 2048 bit)، على سبيل المثال، مفاتيح التعمية. يَعتَمِد المَوَلَّد المطور على قيم عِيَنات إشارة ECG لِيَسْتَغَلَّ جميع الخصائص الإنتروبية الثرية الموجودة فيها. يمكن تطبيق المَوَلَّد المطور ضمن حساسات WBAN؛ لاستخدامه في تطبيقات حماية البيانات المتبادلة عبر تلك الشبكة، ومنها مخطط توليد وتبادل المفاتيح السرية ECG-AKES المطوَّر في الفصل السابق. نسعى إلى أن يحقق المَوَلَّد المطور أعلى معدل إنتاج ممكن (توليد أكبر قدر ممكن من البتات العشوائية في الثانية) بحيث يتفوق على الدراسات السابقة، كما نسعى إلى أن نجعل العمليات الحسابية المُستخدمة لتوليد السلاسل العشوائية بسيطة؛ مما يقلل من استهلاك الطاقة المحدودة للحساسات.

5-3- المبادئ العامة لمولد السلاسل العشوائية المطور المعتمد على إشارة ECG

كما ذكرنا في الفقرة السابقة، يعتمد المولد المطور في توليد السلاسل العشوائية على قيم عينات إشارة ECG. قبل البدء بشرح مخطط مولد السلاسل العشوائية المقترح، يجب أن ننوه إلى فرضيتين أساسيتين أخذتا في الحسبان في أثناء التطوير. الأولى: هي أن إشارة ECG سرية؛ أي لا يمكن لأحد التوصل إليها ما لم يكن لديه الصلاحيات للقيام بذلك. والثانية: هي أن إشارة ECG هي إشارة ثرية بالمعلومات الإنتروبية، فهي متغيرة مع الزمن بشكل لا يمكن التنبؤ به بدقة. ولكن لا يمكن اعتبار إنتروبيتها كافية لاستخدامها مباشرة كسلاسل عشوائية لحماية المعلومات، فهي تحتوي على بعض الخصائص الدورية.

في هذه الدراسة اعتمدنا على ظاهرة أن قيم عينات ECG عند قراءتها بشكل غير متسلسل تُظهر خصائص عشوائية أفضل من الخصائص العشوائية التي تنتج عن قراءة عينات ECG بشكل متتالي. فعند قراءة العينات بشكل متتالي سيكون من الأسهل التنبؤ بقيمة العينة التالية. أما عند تغيير ترتيبها أو قراءة قيمها بشكل عشوائي غير متتالي، فسيصبح من الأصعب التنبؤ بها. فضلاً عن ذلك، لن تُستخدم قيم العينات كما هي وإنما ستُخضع لبعض العمليات الحسابية البسيطة، ومنها الجمع والطرح والضرب وباقي القسمة؛ وذلك من أجل إزالة الخصائص المميزة لها، وزيادة العشوائية.

بناءً على ما سبق، لم نعتمد في توليد السلاسل العشوائية على قيم ECG كما هي؛ وإنما من أجل توليد كل سلسلة عشوائية مكونة من 32 bit، نحصل بدايةً إشارة ECG لفترة زمنية محدّدة، ثم يتم اختيار إحدى عينات إشارة ECG المحصّلة، ويُطبّق عليها بعض العمليات الحسابية. تُستخلص من القيم الناتجة أدلة خمس عينات ECG من الإشارة المحصّلة نفسها؛ من أجل استخدامها في تكوين السلسلة العشوائية. باختصار، في المولد المقترح تُكوّن كل سلسلة عشوائية طولها 32 bit اعتباراً من قيم خمس عينات ECG متباعدة (غير متتالية) بعد إخضاعها لبعض العمليات الحسابية. يتم اختيار تلك العينات الخمس؛ بالاعتماد على قيمة إحدى عينات ECG المحصّلة.

5-4- مخطط مولد السلاسل العشوائية المطور المعتمد على إشارة ECG

يبين الشكل 5-1 مخطط مولد السلاسل العشوائية المطور المعتمد على إشارة ECG. كما يبين الجدول 5-1 قائمة بالرموز المستخدمة في هذا المخطط ودلالاتها.

الجدول 5-1: قائمة بالرموز المستخدمة في مخطط مولد السلاسل العشوائية المطور المعتمد على إشارة ECG، ودلالاتها.

الرمز	دلالته
ecg _i	إحدى عينات إشارة ECG والتي يكون دليلها i.
len	عدد عينات إشارة ECG المحصلة.
X1, X10, X100	أول، ثان، وثالث رقم بعد الفاصلة من قيمة ecg _i على التوالي؛ وذلك بفرض أن قيم العينات تتراوح بين -1 و +1.
e, d, c, b, a	قيم سرية تُستخدم في حساب f ₁ , f ₂ , f ₃ , f ₄ , f ₅ .
f ₅ , f ₄ , f ₃ , f ₂ , f ₁	خمس قيم تُحسب من أجل اختيار العينات الخمس التي ستشكل RS32 اعتباراً منها.
RS32	سلسلة بتات ثنائية عشوائية طولها 32 bit، مولدة باستخدام المولد المطور.
RS32_SET	مجموعة السلاسل RS32، المولدة باستخدام المولد المطور.
n	عدد السلاسل RS32 المولدة، أي عدد عناصر المجموعة RS32_SET.
RSL	سلسلة عشوائية طولها L-bit مكونة من دمج RS32 متعدّدة.
L	طول السلسلة العشوائية المولدة مقدراً بالـ bit. ويأخذ أحد القيم التالية: 128، 256، 512، 1024، 2048.
l	L/32
RS256, RS128, RS1024, RS512, RS2048	سلاسل بتات ثنائية عشوائية أطوالها 128، 256، 512، 1024، 2048 بت على التوالي، مكونة من الدمج RS32 متعدّدة.

لتشكيل n سلسلة عشوائية طول كل منها 32 bit، RS32_SET={RS32₁, RS32₂, ..., RS32_n}، من

خلال المخطط المقترح، نقوم بدايةً بتحصيل إشارة ECG خلال فترة زمنية محددة، والحصول على عينات الإشارة

والتي عددها len عينة، وتكوين مجموعة العينات المحصلة {ecg₁, ecg₂, ..., ecg_{len}}. تُشكّل كل سلسلة عشوائية

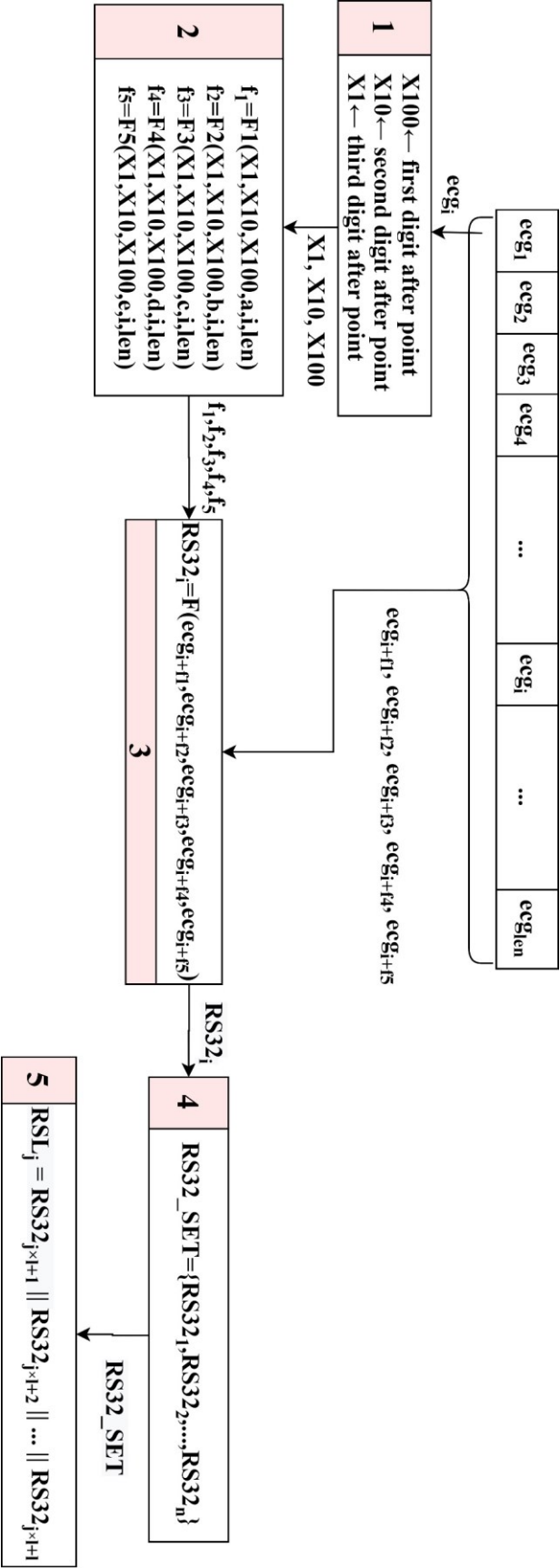
RS32_i (حيث i هي دليل السلسلة العشوائية المولدة، وتأخذ إحدى القيم من 1 إلى n) اعتماداً على خمس من

عينات ECG المحصلة والتي يتم اختيارها بناءً على قيمة i، وعلى قيمة العينة ecg_i، وقيمة len، ومجموعة من

القيم السرية المحددة مسبقاً وهي e, d, c, b, a. بالتالي لتوليد مجموعة السلاسل العشوائية RS32_i المكونة من

32 bit، أي RS32_SET، ثم استنتاج السلاسل العشوائية RS128_i المكونة من 128 bit أو سلاسل أطول من

ذلك، نقوم بالخطوات الآتية:



الشكل 5-1: مخطط مولّد السلاسل العشوائية المطور المقتصد على إشارة ECG.

- يتم بدايةً قراءة قيمة العينة ecg_i من مجموعة العينات المحصّلة. بعدها تُحسب 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 فرض أن قيم العينات، ecg_i ، تتراوح بين -1 و +1. إذا كانت قيم العينات المحصّلة خارج المجال $\{-1,1\}$ فيجب تقييسها لتصبح ضمنه.

- 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 المحصّلة)، وعلى القيم السرية a, b, c, d, e وذلك كما في المعادلات من (5-1) وحتى (5-5):

$$f_1 = F1(X1, X10, X100, a, i, len) = (i \times X100 + X10 \times a \times i + X1) \bmod (len - i) \quad (1-5)$$

$$f_2 = F2(X1, X10, X100, b, i, len) = (i \times X10 + X1 \times b \times i + X100) \bmod (len - i) \quad (2-5)$$

$$f_3 = F3(X1, X10, X100, c, i, len) = (i \times X10 + X100 \times c \times i + X1) \bmod (len - i) \quad (3-5)$$

$$f_4 = F4(X1, X10, X100, d, i, len) = (i \times X1 \times X100 + X10 \times d \times i + X100) \bmod (len - i) \quad (4-5)$$

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

حيث القيم السرية a, b, c, d, e هي أعداد صحيحة أكبر من الصفر. كلّما كانت تلك الأعداد أكبر كلّما ازداد أمان المولّد المطور ضد فضح الإشارة. ولكن تؤدي الزيادة الكبيرة جداً في حجم تلك القيم إلى زيادة زمن الحساب. في دراستنا نختار طول تلك القيم بحيث يكون مساوٍ 10 bit.

- حساب السلسلة العشوائية $RS32_i$ ، بالاعتماد على عينات إشارة ECG المحصّلة، أي $\{ecg_1, ecg_2, \dots, ecg_{len}\}$ وعلى i و f_1, f_2, f_3, f_4, f_5 كما في العلاقة (4-6).

$$RS32_i = (\text{uint32}) \left((ecg_{i+f_1} \times 10^9 + ecg_{i+f_2} \times 10^8 + ecg_{i+f_3} \times 10^6 + ecg_{i+f_4} \times 10^5 + ecg_{i+f_5} \times 10^3) \times (i) + i \right) \quad (6-5)$$

- يتم تكرار العمليات السابقة اعتباراً من $i=1$ وحتى $i=n$ ، ومن ثمّ تشكيل n سلسلة طول كل منها 32 bit.

- تشكيل سلاسل عشوائية طولها L-bit (RSL) حيث L تأخذ إحدى القيم التالية 128، 256، 512، 1024، 2048 وذلك من خلال دمج l سلسلة من مجموعة السلاسل الناتجة RS32_SET، حيث $l=L/32$ وذلك كما هو مبين في العلاقة (5-7).

$$RSL_j \leftarrow RS32_{j \times l + 1} || RS32_{j \times l + 2} || \dots || RS32_{j \times l + l} \quad (5-7)$$

حيث j تتراوح بين 1 و n/l .

خوارزمية 5-1: شبه الرمز لمخطط مولد السلاسل العشوائية المطور المعتمد على إشارة ECG.

```

Input:
ECG={ecg1, ecg2, ..., ecglen}, len, n, L
Output:
RS32_SET={RS321, RS322, ..., RS32n}, RSL

For i ← 1 to n do
    X100 ← first digit after point.
    X10 ← second digit after point.
    X1 ← third digit after point.
    f1 ← (i×X100 + X10×a×i + X1)mod(len-i)
    f2 ← (i×X10 + X1×b×i + X100)mod(len-i)
    f3 ← (i×X10 + X100×c×i + X1)mod(len-i)
    f4 ← (i×X1×X100 + X10×d×i + X100)mod(len-i)
    f5 ← (i×X1×X10 + X100×e×i + X100)mod(len-i)
    RS32i ← (uint32)((ecgi+f1×109 + ecgi+f2×108 + ecgi+f3×106 + ecgi+f4×105 +
        ecgi+f5×103)×i + i;
    add RS32i to RS32_SET
end for
select j, where j ranges from 1 to n/l and l=L/32
RSLj=RS32j×l+1 || RS32j×l+2 || ... || RS32j×l+l

```

- على سبيل المثال، يمكن توليد RS ذات طول 128 bit (أي تشكيل RS128) من خلال دمج كل 4 سلاسل عشوائية RS32_i، كما في العلاقة (5-8).

$$RS128_j \leftarrow RS32_{j \times 4 + 1} || RS32_{j \times 4 + 2} || RS32_{j \times 4 + 3} || RS32_{j \times 4 + 4} \quad (5-8)$$

- حيث تتراوح j من 1 إلى $n/4$ ، فيمكن تشكيل $n/4$ سلسلة عشوائية طول كل منها 128 bit. باستخدام المخطط المقترح، يمكن إنشاء تدفقات عشوائية أطول من 128 bit عن طريق دمج أكثر من أربع سلاسل RS32 بشكلٍ متتالٍ. ولإنشاء سلسلة عشوائية طولها 256 bit (أي تشكيل RS256)، تُدمج كل ثمانية سلاسل RS32، كما هو موضح في العلاقة (5-9)

$$RS256_j \leftarrow RS32_{j \times 8 + 1} || RS32_{j \times 8 + 2} || \dots || RS32_{j \times 8 + 8} \quad (9-5)$$

حيث j تأخذ القيم من 1 حتى $n/8$. وبشكل مشابه، يُمكن إنشاء سلاسل عشوائية أطوالها 256 bit، 512 bit، 1024 bit، 2048 bit عن طريق دمج العدد المناسب من RS32. وتبين الخوارزمية 5-1 شبه الرمز لمخطط مولّد السلاسل العشوائية المطوّر المُعتمد على إشارة ECG.

تعتمد قيمة n على عدد السلاسل المُراد تشكيلها وأطوال تلك السلاسل. ولكن كحد أقصى يمكن توليد $len/2$ سلسلة RS32. على سبيل المثال، من أجل تشكيل سلسلة عشوائية واحدة فقط طولها 128 bit بالتالي يمكن جعل $n=4$. تُختار قيمة n بحيث تكون أصغر أو تساوي $len/2$ ؛ لأن قيم f ، التي تُحدّد العينات المساهمة في تكوين RS32، تُحسب بالاعتماد على باقي القسمة على $len-i$. فإذا كانت قيمة i قريبة من n وكانت $len=n$ يكون ناتج باقي القسمة على $len-i$ ذا مجال قيم محدود جداً يجعل اختيار عينات ecg المشاركة في تكوين RS32 محدوداً أيضاً. قد يُضعف ذلك من عشوائية السلاسل الناتجة أو قد يُسهّل على المهاجم مهمة تحديد قيم ecg اعتباراً من RS32. ويجدر التنويه إلى أن العمليات الحسابية كالجمع والطرح والضرب وباقي القسمة هي عمليات طُبِّقَت من أجل الحصول على العشوائية المطلوبة وتوسيع مجال القيم التي يمكن أن تظهر في الخرج. أما استخدام القيم السرية a, b, c, d, e ، بمعدل قيمة واحدة في كل تابع من F ، فهو بهدف حماية إشارة ECG من الفضح. تزيد هذه القيم من عدد المجاهيل في المعادلات وتُبقي عدد المعادلات أكبر من عدد المجاهيل حتى لو كُشِفَت قيمة العينة التي حُسِبَت منها $X1, X10, X100$ ، حيث تُعتَبَر i سرية أيضاً. يمكن استخدام عدد أكبر من العينات في حساب RS32 ولكن ذلك يقتضي توليد وحساب عدد أكبر من F ، كما يتطلّب عدداً أكبر من القيم السرية؛ والذي بدوره يزيد من العمليات الحسابية المطلوبة.

5-5- النتائج والمناقشة حول مولّد السلاسل العشوائية المطوّر المُعتمد على إشارة ECG

فيما يلي نستعرض نتائج اختبار مولّد السلاسل العشوائية المطوّر المُعتمد على إشارة ECG. بدايةً نرغب في أن ننوّه إلى أن جميع الاختبارات أُجريت باستخدام مجموعتين من البيانات. المجموعة الأولى هي لأشخاص أصحاء، أما المجموعة الثانية فهي لأشخاص يعانون من عدم انتظام ضربات القلب. اختيرت مجموعتا البيانات السابقتان،

وبالتحديد بيانات الأشخاص الأصحاء من أجل التحقق من عشوائية السلاسل المولدة حتى في حال انتظام ضربات القلب.

5-5-1. أمان المولد المطور ضد فضح إشارة ECG

في مولدات السلاسل العشوائية يجب أن يكون مصدر الإنتروبية مقاوماً لأي هجوم يمكن أن يخفّض مستوى الإنتروبية الناتج عنه. في حالتنا مصدر الإنتروبية هو إشارة ECG، أي نبضات القلب [103]. يمكن أن تأخذ الهجمات على الإنتروبية أحد النمطين التاليين: الهجوم الفعّال والهجوم غير الفعّال. بالنسبة لمولدات الأرقام العشوائية، الهجوم الفعّال، ويمكن أن نطلق عليه أيضاً هجوم اضطراب الإشارة، هو الهجوم الذي يكون فيه المهاجم قادراً على السيطرة على مصدر الإنتروبية أو التأثير عليه بهدف التحكم بالقيم العشوائية الناتجة عنه [103]. بالنسبة للمولد المطور، لا يمكن التحكم بمصدر الإنتروبية، أي نبضات القلب، من قبل مهاجم خارجي. أما الهجوم غير الفعّال هو الهجوم الذي يسعى من خلاله المهاجم إلى توليد قيم عشوائية مماثلة أو مطابقة للقيم التي يولدها مصدر الإنتروبية ولكن باستخدام منصّة مماثلة لمصدر الإنتروبية الأصلي [103]. بالنسبة للمولد المطور تكون تلك المنصة هي إشارة ECG لشخص آخر. هذا النمط من الهجمات هو أيضاً غير مجدي في حالتنا؛ لأن إشارة ECG تختلف من شخص لآخر ومن زمن لآخر، وسيتم برهان ذلك في فقرة تالية، حيث نختبر تميز السلاسل العشوائية الناتجة عن إشارة ECG لشخص ما عن تلك الناتجة عن إشارة ECG لشخص آخر.

في مولدات السلاسل العشوائية المعتمدة على الإشارات الحيوية، يجب ألاّ يتمكّن المهاجم من التوصل إلى قيم الإشارة الحيوية بمعرفة السلسلة العشوائية الناتجة عنها. نلاحظ أن هذا الشرط محقق في المخطط المقترح. لا يمكن تحديد قيم عينات ECG اعتباراً من RS32؛ وذلك بسبب العمليات الحسابية التي تخضع لها، وبالتحديد عملية باقي القسمة، فضلاً عن سرية القيم a, b, c, d, e.

إذا افترضنا أن المهاجم استطاع معرفة قيمة i بالنسبة لسلسلة RS32_i معيّنة، وأن طول كل من a, b, c, d, e يساوي x bit، بالتالي سيحتاج معرفة f₁, f₂, f₃, f₄, f₅ وما يقابلها من أدلة العينات الخمس لإشارة ECG (وهي عينات ذات مواقع متباعدة غير متتالية) التي تم تشكيل RS32_i اعتباراً منها إلى $2^{5x+9} = (2^x)^5 * (2^3)^3$

تجربة. تمثل $(2^3)^3$ بشكل تقريبي عدد التجارب اللازمة للتوصل إلى قيم X_1 , X_{10} , X_{100} ، لأن كلاً منها هو عبارة عن رقم عشري يأخذ إحدى القيم من 0 حتى 9. وتمثل $(2^x)^5$ 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 لجميع السلاسل العشوائية الناتجة RS32_i والتوصل إلى قيمة len عينة من ecg "في أسوأ الأحوال" فهو بحاجة إلى $(2^{5x+9})^n$ تجربة. على سبيل المثال، إذا أراد المهاجم تحديد f_1, f_2, f_3, f_4, f_5 لكافة السلاسل العشوائية الناتجة عن العينات المحصّلة خلال ثانية من الوقت وكان معدل اعتيان الإشارة يساوي 360 عينة في الثانية، وكانت $n = \text{len}/2$ ، وطول كل من القيم السرية يساوي 10 bit، فسيحتاج المهاجم إلى $2^{10620} = (2^{59})^{360/2}$ تجربة. نستخدم العبارة "في أسوأ الأحوال"؛ لأنه قد يتكرّر اكتشاف قيمة العينة ecg_i نفسها من قبل المهاجم مرّات عدّة أو قد يكون هناك بعض العينات التي لم يتم استخدامها في تكوين RS32، ومن ثمّ تكون معرفة جميع قيم ecg هي السيناريو الأسوأ. في حال كان المهاجم لا يستطيع تحديد i بالنسبة لـ RS32_i؛ أي لا يستطيع معرفة العينة التي حُدّدت قيم f_1, f_2, f_3, f_4, f_5 اعتباراً منها ومن ثمّ العينات المكونة لـ RS32_i، يصبح التوصل إلى قيم ecg أكثر صعوبة. ولو افترضنا العكس، وأن المهاجم استطاع بطريقة ما التوصل إلى f_1, f_2, f_3, f_4, f_5 فهو لن يستطع التوصل إلى ecg_i؛ لأن a, b, c, d, e هي عبارة عن قيم سرية. إن عملية باقي القسمة في علاقات حساب f تزيد من صعوبة الحصول على قيمة ecg_i.

لو استطاع المهاجم بطريقة ما التوصل إلى إشارة ECG وإلى قيم RS32_i الناتجة عنها، فهو بحاجة إلى $(2^x)^5$ تجربة لتحديد قيم a, b, c, d, e .

يمكن ملاحظة أنه كلما كانت len أكبر و n أصغر، استطعنا حماية إشارة ECG من الفضح اعتباراً من السلسلة العشوائية الناتجة. كما تجدر الإشارة إلى أنّ وجود القيم السرية a, b, c, d, e لا يجعل من المولّد المقترح مولّد أرقام شبه عشوائية؛ وإنما هو مولّد أرقام عشوائية. لا يمكن فرض أن تلك القيم هي بذور لتوليد السلسلة العشوائية، وذلك لأن السلسلة العشوائية الناتجة لا تعتمد على تلك القيم فحسب وإنما تعتمد بشكل أساسي على قيم إشارة ECG المتغيرة بشكل دائم؛ ولأن تلك القيم السرية لا يتم تغييرها من أجل كلّ عملية توليد لسلسلة جديدة. فكما ذكرنا سابقاً، الهدف من القيم السرية هو فقط حماية إشارة ECG من الفضح.

2-5-5. اختبار العشوائية والتميز

لتحليل عشوائية وتميز السلاسل العشوائية الناتجة عن المولد المقترح، أجريت العديد من الاختبارات وفق ما يأتي:

- استُخدمت بيانات 50 شخصاً مقسومين إلى مجموعتين. المجموعة الأولى مكونة من بيانات 25

شخص بحالة صحية جيدة، تم الحصول عليها من قاعدة البيانات MIT-BIH Normal Sinus

Rhythm Database [43] (18 سجل)، معدّل أخذ العينات فيها يساوي 128 عينة في الثانية، ومن

قاعدة البيانات MIT-BIH Long-Term ECG Database [44] (7 سجلات)، والتي معدل أخذ

العينات فيها أيضاً يساوي 128 عينة في الثانية. أما المجموعة الثانية فهي مكونة من بيانات 25

شخصاً يعانون من عدم انتظام في ضربات القلب، تم الحصول عليها من قاعدة البيانات MIT-

BIH Arrhythmia Database [42]، معدّل أخذ العينات فيها يساوي 360 عينة في الثانية.

- أُجريت التجارب من أجل len تقابل زمن تحصيل إشارة قدره ثانية واحدة، ومن أجل len تقابل زمن

تحصيل قدره ثانيتان، ومن أجل len تقابل زمن تحصيل قدره أربع ثوانٍ. أُختير الحد الأدنى لزمن

تحصيل الإشارة بحيث يساوي ثانية واحدة على الأقل؛ لأنه من الأفضل أن تحتوي العينات التي

ستنتج عنها السلسلة العشوائية على نبضة قلب واحدة على الأقل؛ مما يؤمن عشوائية أفضل.

- أُجريت جميع التجارب من أجل الحصول على سلاسل عشوائية أطوالها 128 bit، 256 bit،

512 bit، 1024 bit، 2048 bit وهي الأطوال الأكثر شيوعاً لاستخدامها في مخططات أمن

المعلومات.

تجدر الإشارة هنا إلى أن زمن تحصيل الإشارة لا علاقة له بطول السلاسل الناتجة. فكما وصّحنا سابقاً،

وعلى سبيل المثال، إذا قمنا بتحصيل الإشارة لمدة ثانية واحدة، وكان معدل أخذ العينات يساوي 360 عينة في

الثانية، فيمكننا كأقصى حد الحصول على RS32 $= 180 = (1 \times 360)/2$ ، يمكن تجميع كل 4 منها معاً،

للحصول على سلاسل عشوائية طول كل منها 128 bit، أو تجميع كل 8 منها، وتشكيل سلاسل طول كل منها

256 bit، وهكذا.

في المولد المطور يجب التحقق من عاملين أساسيين هما: أولاً، العشوائية، من أجل تقييم جودة RBSs الحيوية المولدة. فيجب أن تكون RBSs المعتمدة على ضربات القلب عشوائية بما يكفي لتعمل كمفاتيح تسمية أو غيرها. ثانياً، التميز، فيجب أن تمتلك RBSs المولدة خصائص مميزة لضمان قيام كل فرد بتوليد RBSs مختلفة عن RBSs المولدة من أفراد آخرين.

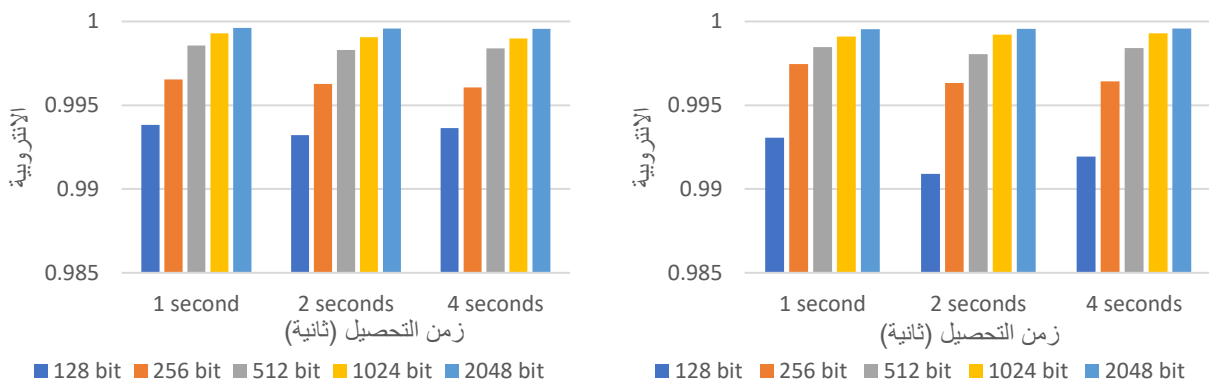
5-5-2. اختبار العشوائية

أولاً: اختبار العشوائية من خلال تحليل الإنتروبية

لاختبار عشوائية السلاسل الناتجة يجب تحليل إنتروبيتها (Entropy analysis) [104]. يتم ذلك بتطبيق علاقة Shannon Entropy المُبيّنة في المعادلة (10-5).

$$H(X) = - \sum_{j=1}^n P(x_j) \times \log_2 P(x_j) \quad (10-5)$$

يمكن أن يكون للإنتروبية قيمة قصوى تساوي 1 إذا كان التوزع موحداً؛ وذلك لأن السلاسل مكوّنة من تتالي لقيمتين هما 0 و 1. حُسِبَت الإنتروبية من أجل مجموعتي البيانات (بيانات الأشخاص الأصحاء، وبيانات المرضى) ومن أجل أزمنة تحصيل مختلفة للإشارة، وهي: ثانية واحدة، ثانيتان، وأربع ثوانٍ. كما حُسِبَت من أجل سلاسل عشوائية ذات أطوال مختلفة وهي: 128 bit، 256 bit، 512 bit، 1024 bit، 2048 bit.



ب- المرضى

أ- الأصحاء

الشكل 5-2: رسم بياني توضيحي لإنتروبية السلاسل العشوائية الناتجة عن المولد المطور.

يوضح الشكل 5-2 أ الإنتروبية الناتجة عن السلاسل العشوائية المولدة من مجموعة بيانات الأشخاص الأصحاء (25 شخصاً) من أجل أطوال مختلفة للسلاسل المولدة، ومن أجل استخدام إشارة محصلة بأزمة تحصيل مختلفة. حُسِبَ متوسط الإنتروبية لـ 75 سلسلة (3 لكل شخص) من أجل كل زمن تحصيل، ومن أجل كل طول للسلاسل العشوائية الناتجة. أما الشكل 5-2 ب فيوضح الإنتروبية الناتجة عن السلاسل العشوائية المولدة من مجموعة بيانات الأشخاص المرضى (25 شخصاً) من أجل أطوال مختلفة للسلاسل المولدة ومن أجل استخدام إشارة محصلة بأزمة تحصيل مختلفة. حُسِبَ متوسط الإنتروبية أيضاً لـ 75 سلسلة (3 لكل شخص) من أجل كل زمن تحصيل، ومن أجل كل طول للسلاسل العشوائية الناتجة.

كما هو واضح من الشكل 5-2، فإن وسطي الإنتروبية من أجل جميع الاختبارات أعلى من 0.99 أي قريب جداً من 1. ونلاحظ أن جميع النتائج متقاربة من بعضها بعضاً. كما أن إنتروبية السلاسل التي طولها 2048 bit هي الأقرب قيمةً إلى 1؛ وذلك لأن عدد البتات كبير وبالتالي يكون للاختلاف البسيط في عدد الأصفار والواحدات عن نصف إجمالي عدد البتات أثر ضئيل جداً أقل من أثر الاختلاف بالنسبة للسلاسل القصيرة. كما نلاحظ في بعض الحالات أن الإنتروبية بالنسبة للسلاسل العشوائية الناتجة عن الأشخاص المرضى هي أفضل بقليل من تلك الناتجة عن الأشخاص الأصحاء. يمكن تبرير ذلك بأن عشوائية ECG للأشخاص المرضى بعدم انتظام ضربات القلب تكون أكبر من مقابلتها للأشخاص الأصحاء مما يزيد من عشوائية السلاسل الناتجة عنها.

ثانياً: اختبار العشوائية باستخدام مجموعة الاختبار NIST

كما ذكرنا سابقاً، مجموعة NIST هي منصة ملائمة للتحقق من عشوائية السلاسل العشوائية التي تولد في تطبيقات مختلفة. تتكون من مجموعة من الاختبارات، ينتج عن كلٍ منها قيمة P. نفترض أن السلسلة عشوائية إذا كانت قيم P الناتجة عن الاختبارات أكبر من 0.01، وإلا فالسلسلة ليست عشوائية. أُجريت العديد من اختبارات NIST على RBSs المختلفة الناتجة للتحقق من عشوائيتها والتحقق فيما إذا كان بالإمكان استخدامها لأغراض حماية المعلومات. أُختيرَ هذا المعيار دون غيره؛ لأنه يُعنى باختبار عشوائية السلاسل التي تُستخدم لأغراض حماية المعلومات.

في دراستنا، حيث نسعى لتوليد سلاسل عشوائية قصيرة، أطوالها تتراوح بين 128 bit و 2048 bit، اكتفينا بإجراء 10 من اختبارات معيار NIST التي تُعنى بفحص عشوائية السلاسل ذات الأطوال القصيرة والتي تتناسب مع RBSs المولدة في المخطط المقترح. بحسب توصيات معيار NIST يجب اختبار 50 سلسلة على الأقل لإثبات أن الأرقام المولدة من قبل المولد المطور عشوائية. طُبِّقَت مجموعة الاختبار على RBSs الناتجة عن بيانات محصلة خلال ثانية واحدة، وثانيتين، وأربع ثوانٍ، من أجل مجموعتي البيانات (بيانات الأشخاص الأصحاء والمرضى)، وبالنسبة لسلاسل أطوالها 128 bit، 256 bit، 512 bit، 1024 bit، 2048 bit. اختُبرت 150 سلسلة عشوائية لكل مجموعة RBSs من المجموعات المذكورة حيث اختُبرت هذه السلاسل عشوائياً (6 سلاسل لكل شخص). يُقصد بكلمة مجموعة RBSs، مجموعة السلاسل العشوائية التي لها الطول نفسه ويتم إنشاؤها من إشارات ECG المكتسبة من مجموعة البيانات نفسها وبالنسبة لزمّن التحصيل نفسه.

الجدول 5-2: نتائج اختبارات NIST للسلاسل العشوائية ذات الأطوال المختلفة التي وُلدت من إشارة ECG المحصلة في ثانية واحدة من أشخاص أصحاء ومن مرضى عدم انتظام ضربات القلب

NIST Test	RS128		RS256		RS512		RS1024		RS2048	
	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia
Frequency test	0.4539371 (145/150)	0.466891 (149/150)	0.445182 (146/150)	0.491286 (147/150)	0.425492 (145/150)	0.488742 (148/150)	0.403181 (145/150)	0.478143 (147/150)	0.449535 (146/150)	0.506926 (149/150)
Block Frequency test	0.4861063 (150/150)	0.476131 (149/150)	0.502289 (147/150)	0.470235 (150/150)	0.465151 (149/150)	0.48316 (149/150)	0.453126 (148/150)	0.467849 (150/150)	0.466188 (149/150)	0.444678 (149/150)
Runs test	0.4894513 (149/150)	0.477067 (147/150)	0.467138 (147/150)	0.532988 (147/150)	0.453703 (150/150)	0.456062 (146/150)	0.44296 (150/150)	0.480238 (148/150)	0.478791 (149/150)	0.497732 (149/150)
Longest Run test	0.4933910 (149/150)	0.455496 (149/150)	0.471647 (150/150)	0.491179 (150/150)	0.469515 (149/150)	0.487499 (148/150)	0.503016 (150/150)	0.48583 (150/150)	0.507175 (150/150)	0.50758 (148/150)
FFT test	0.4786736 (148/150)	0.507419 (150/150)	0.445765 (148/150)	0.455913 (147/150)	0.460525 (148/150)	0.516048 (150/150)	0.471097 (148/150)	0.534245 (149/150)	0.492745 (145/150)	0.47219 (149/150)
Non-overlapping (148/148)	0.8806404 (150/150)	0.876812 (150/150)	0.693465 (150/150)	0.691438 (150/150)	0.609397 (150/150)	0.611467 (150/150)	0.595678 (150/150)	0.608489 (150/150)	0.59885 (150/150)	0.565482 (150/150)
Linear Complexity test	0.5330263 (146/150)	0.574781 (146/150)	0.501857 (148/150)	0.53163 (147/150)	0.523807 (148/150)	0.511964 (146/150)	0.517081 (149/150)	0.491068 (148/150)	0.538196 (145/150)	0.442865 (148/150)
Serial test (2/2)	0.487359 (147/150)	0.499778 (149/150)	0.514288 (148/150)	0.497818 (149/150)	0.505249 (148/150)	0.512397 (149/150)	0.508009 (147/150)	0.50701 (149/150)	0.516703 (148/150)	0.49346 (149/150)
Approximate Entropy test	0.4642176 (149/150)	0.452294 (149/150)	0.465356 (148/150)	0.504686 (149/150)	0.450087 (147/150)	0.494426 (148/150)	0.477133 (145/150)	0.48493 (148/150)	0.495937 (145/150)	0.457565 (145/150)
Cumulative Sums test (2/2)	0.4776528 (146/150)	0.484026 (149/150)	0.471015 (147/150)	0.485231 (147/150)	0.449389 (147/150)	0.475344 (149/150)	0.430528 (146/150)	0.489653 (149/150)	0.466256 (146/150)	0.506654 (149/150)

الجدول 5-3: نتائج اختبارات NIST للسلاسل العشوائية ذات الأطوال المختلفة التي وُلدت من إشارة ECG المحصلة في ثانيتين من أشخاص أصحاء ومن مرضى عدم انتظام ضربات القلب

NIST Test	RS128		RS256		RS512		RS1024		RS2048	
	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia
Frequency test	0.418237 (146/150)	0.444315 (150/150)	0.449109 (148/150)	0.474032 (148/150)	0.395032 (145/150)	0.487659 (150/150)	0.394635 (145/150)	0.502462 (147/150)	0.430471 (150/150)	0.489063 (148/150)
Block Frequency test	0.453203 (147/150)	0.518383 (149/150)	0.472918 (145/150)	0.459901 (149/150)	0.427422 (147/150)	0.470684 (150/150)	0.432275 (147/150)	0.499396 (149/150)	0.435216 (148/150)	0.476052 (148/150)
Runs test	0.461375 (147/150)	0.541177 (150/150)	0.452958 (145/150)	0.518318 (147/150)	0.467974 (146/150)	0.537438 (150/150)	0.492123 (145/150)	0.499039 (148/150)	0.517553 (146/150)	0.550426 (148/150)
Longest Run test	0.496489 (147/150)	0.484528 (149/150)	0.49682 (150/150)	0.497948 (147/150)	0.494257 (150/150)	0.477641 (150/150)	0.510431 (148/150)	0.504717 (148/150)	0.488336 (148/150)	0.493951 (147/150)
FFT test	0.484264 (147/150)	0.491878 (148/150)	0.529008 (145/150)	0.480064 (149/150)	0.478057 (147/150)	0.497503 (149/150)	0.428912 (146/150)	0.507568 (146/150)	0.460306 (145/150)	0.50516 (146/150)
Non-overlapping (148/148)	0.880055 (150/150)	0.881541 (150/150)	0.698853 (150/150)	0.70016 (150/150)	0.614562 (150/150)	0.611163 (150/150)	0.607865 (150/150)	0.604192 (150/150)	0.569852 (150/150)	0.562963 (150/150)
Linear Complexity test	0.557688 (145/150)	0.542994 (148/150)	0.51928 (146/150)	0.510974 (146/150)	0.478893 (145/150)	0.52219 (148/150)	0.495107 (148/150)	0.500315 (148/150)	0.463939 (145/150)	0.510728 (146/150)
Serial test (2/2)	0.483262 (147/150)	0.484225 (149/150)	0.509993 (147/150)	0.542076 (150/150)	0.46917 (146/150)	0.532033 (149/150)	0.46351 (150/150)	0.504178 (148/150)	0.46152 (149/150)	0.487694 (150/150)
Approximate Entropy test	0.434853 (149/150)	0.506904 (149/150)	0.428811 (146/150)	0.515209 (146/150)	0.436112 (145/150)	0.506208 (149/150)	0.472628 (145/150)	0.535284 (149/150)	0.454319 (147/150)	0.554778 (150/150)
Cumulative Sums test (2/2)	0.463168 (148/150)	0.500383 (149/150)	0.4675 (149/150)	0.467258 (148/150)	0.416593 (146/150)	0.489002 (150/150)	0.411216 (147/150)	0.507198 (147/150)	0.453467 (150/150)	0.504684 (148/150)

الجدول 5-4: نتائج اختبارات NIST للسلاسل العشوائية ذات الأطوال المختلفة التي وُلدت من إشارة ECG المحصلة في أربع ثوانٍ من أشخاص أصحاء ومن مرضى عدم انتظام ضربات القلب

NIST Test	RS128		RS256		RS512		RS1024		RS2048	
	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia	Normal	Arrhythmia
Frequency test	0.423602 (145/150)	0.496572 (148/150)	0.46244 (146/150)	0.505411 (150/150)	0.427315 (145/150)	0.489915 (149/150)	0.467806 (145/150)	0.493505 (150/150)	0.359222 (145/150)	0.498964 (149/150)
Block Frequency test	0.491905 (150/150)	0.45626 (149/150)	0.512393 (150/150)	0.500857 (147/150)	0.491971 (149/150)	0.504304 (147/150)	0.482289 (150/150)	0.485361 (148/150)	0.369335 (145/150)	0.538561 (150/150)
Runs test	0.489282 (146/150)	0.475512 (149/150)	0.445517 (149/150)	0.498767 (149/150)	0.4418 (147/150)	0.461012 (150/150)	0.397959 (149/150)	0.482889 (148/150)	0.424549 (148/150)	0.481619 (148/150)
Longest Run test	0.492095 (150/150)	0.486322 (149/150)	0.506059 (149/150)	0.556481 (150/150)	0.521922 (148/150)	0.524108 (148/150)	0.493468 (148/150)	0.469066 (150/150)	0.437641 (147/150)	0.465465 (150/150)
FFT test	0.473154 (149/150)	0.496539 (148/150)	0.492549 (149/150)	0.451194 (145/150)	0.484266 (149/150)	0.527761 (149/150)	0.467082 (150/150)	0.47951 (147/150)	0.517437 (148/150)	0.51086 (147/150)
Non-overlapping (148/148)	0.881451 (150/150)	0.883568 (150/150)	0.697464 (150/150)	0.698377 (150/150)	0.611055 (150/150)	0.61583 (150/150)	0.606604 (150/150)	0.604696 (150/150)	0.564882 (150/150)	0.564889 (150/150)
Linear Complexity test	0.532023 (145/150)	0.525388 (146/150)	0.487119 (147/150)	0.548289 (149/150)	0.513783 (146/150)	0.517785 (148/150)	0.504859 (147/150)	0.491369 (147/150)	0.540259 (145/150)	0.490268 (147/150)
Serial test (2/2)	0.494628 (150/150)	0.532958 (150/150)	0.523817 (150/150)	0.537888 (150/150)	0.481081 (147/150)	0.483329 (146/150)	0.469921 (147/150)	0.49085 (147/150)	0.478425 (148/150)	0.496623 (150/150)
Approximate Entropy test	0.455321 (146/150)	0.503039 (150/150)	0.437514 (147/150)	0.504106 (150/150)	0.451565 (147/150)	0.517057 (148/150)	0.413003 (149/150)	0.48722 (148/150)	0.44148 (148/150)	0.454336 (149/150)
Cumulative Sums test (2/2)	0.463227 (146/150)	0.511769 (147/150)	0.475655 (147/150)	0.518753 (150/150)	0.460115 (147/150)	0.518051 (149/150)	0.49223 (146/150)	0.495791 (150/150)	0.364521 (147/150)	0.515032 (149/150)

تعطي المعادلة (11-5) معدل النجاح الأدنى المطلوب لاختبارات NIST، والذي يمكن من خلاله حساب الحد الأدنى لعدد التجارب التي يجب اجتيازها لكل اختبار NIST [91]:

$$mpr = (1 - \alpha) - 3 * \text{sqrt} \left(\frac{\alpha * (1 - \alpha)}{k} \right) \quad (11-5)$$

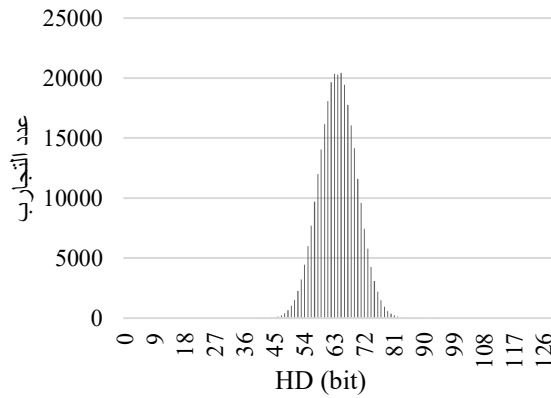
حيث $(1 - \alpha)$ هي مستوى الأهمية و k عدد السلاسل المُختَبَرَة (التجارب). في حالتنا، $\alpha = 0.01$ و $K = 150$ ، وبالنتيجة يكون معدل النجاح الأدنى هو 96.56%. أي يجب أن تتجح 145 تجربة أو أكثر اعتباراً من 150 تجربة. يوضح الجدول 2-5 متوسط قيم P وعدد التجارب التي أُجْتَبِرَتْ من أجل كلٍ من اختبارات NIST العشرة. هذه النتائج هي نتائج اختبار RBSs التي وُلِدَتْ باستخدام إشارات ECG محصّلة لمدة ثانية واحدة. وبالتالي، تم توليد واختبار 150 سلسلة لكل طول من الأطوال المدروسة ولكل مجموعة بيانات (أصحاء، مرضى). يوضح الجدول 2-5 أن RBSs التي تم توليدها اجتازت الاختبارات العشرة؛ لأن قيمة P كانت أكبر من 0.01 في أكثر من 145 تجربة بالنسبة لكل من اختبارات NIST. لذلك، يمكن افتراض عشوائية السلاسل الثنائية الناتجة عن إشارة ECG المحصلة في ثانية واحدة باستخدام المخطط المقترح. بشكل مشابه يوضح كل من الجدول 3-5 والجدول 4-5 عشوائية السلاسل الناتجة، ولكن من أجل مدة تحصيل إشارة مختلفة. بالتالي RBSs التي تم توليدها اجتازت اختبارات NIST العشرة حيث كانت قيمة P أكبر من 0.01 في 145 تجربة أو أكثر لكل من اختبارات NIST. نتيجة لذلك، فإن RBSs ذات الأطوال المختلفة التي تم توليدها باستخدام المخطط المقترح من إشارات ECG المحصلة لفترات زمنية مختلفة من مجموعتي البيانات، هي عشوائية بما يكفي لاستخدامها لأغراض التعمية وحماية المعلومات.

2.2-5-5. تحليل التميّز

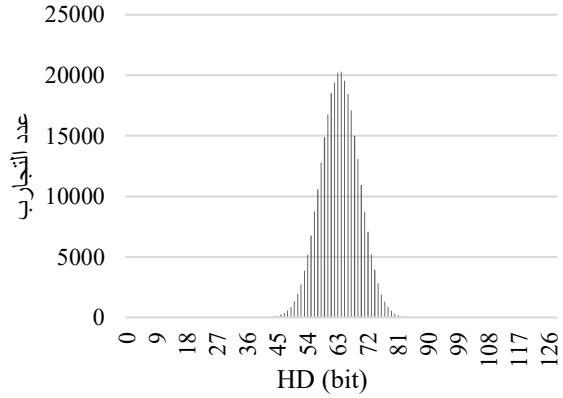
لتحليل التميّز نختبر فيما إذا كانت RBSs لأجسام مختلفة متميّزة بشكلٍ كافٍ. فإذا كانت RBSs المولّدة متميّزة، فلا يمكن للخصم استخدام بيانات فرد آخر للتنبؤ بالقيم التي يولّدها الفرد الهدف. لتقييم ذلك، ولّد ملفّ يحوي 7680 RS32 من أجل كل شخص ومن أجل كل زمن تحصيل (ثانية واحدة، ثانيتان، أربع ثوانٍ). جُمِعَتْ سلاسل RS32 في سلاسل أطوالها 128 bit، 256 bit، 512 bit، 1024 bit، 2048 bit وحُسِبَتْ مسافة هامينغ بين

السلاسل المكونة من بيانات كل شخص ومقابلاتها لكل شخص آخر ضمن المجموعة نفسها، ومن أجل زمن التحصيل نفسه. حُسِبَت مسافة هامينغ وفقاً للآتي:

- من أجل سلاسل أطوالها 128 bit حُسِبَت مسافة هامينغ بين 1920 سلسلة من كل جسم ومقابلاتها في باقي الأجسام.
- من أجل سلاسل أطوالها 256 bit حُسِبَت مسافة هامينغ بين 960 سلسلة من كل جسم ومقابلاتها في باقي الأجسام.
- من أجل سلاسل أطوالها 512 bit حُسِبَت مسافة هامينغ بين 480 سلسلة من كل جسم ومقابلاتها في باقي الأجسام.
- من أجل سلاسل أطوالها 1024 bit حُسِبَت مسافة هامينغ بين 240 سلسلة من كل جسم ومقابلاتها في باقي الأجسام.
- من أجل سلاسل أطوالها 2048 bit حُسِبَت مسافة هامينغ بين 120 سلسلة من كل جسم ومقابلاتها في باقي الأجسام.



ب- بيانات المرضى



أ- بيانات الأشخاص الأصحاء

الشكل 3-5: تَوَزُّع مسافة هامينغ للسلاسل RS128 من أجل البيانات المحصَّلة في ثانية واحدة.

يوضِّح الشكل 3-5 تَوَزُّع مسافة هامينغ من أجل RS128 مولدة من بيانات محصَّلة خلال ثانية واحدة.

نلحظ التَوَزُّع الطبيعي لمسافة هامينغ للسلاسل التي ولِّدت من بيانات الأشخاص الأصحاء وأن متوسط HDs يساوي

63.518 bit، وهو ما يقارب 50% من طول RBS كما هو موضَّح في الشكل 3-5 أ. يوضِّح الشكل 3-5 ب

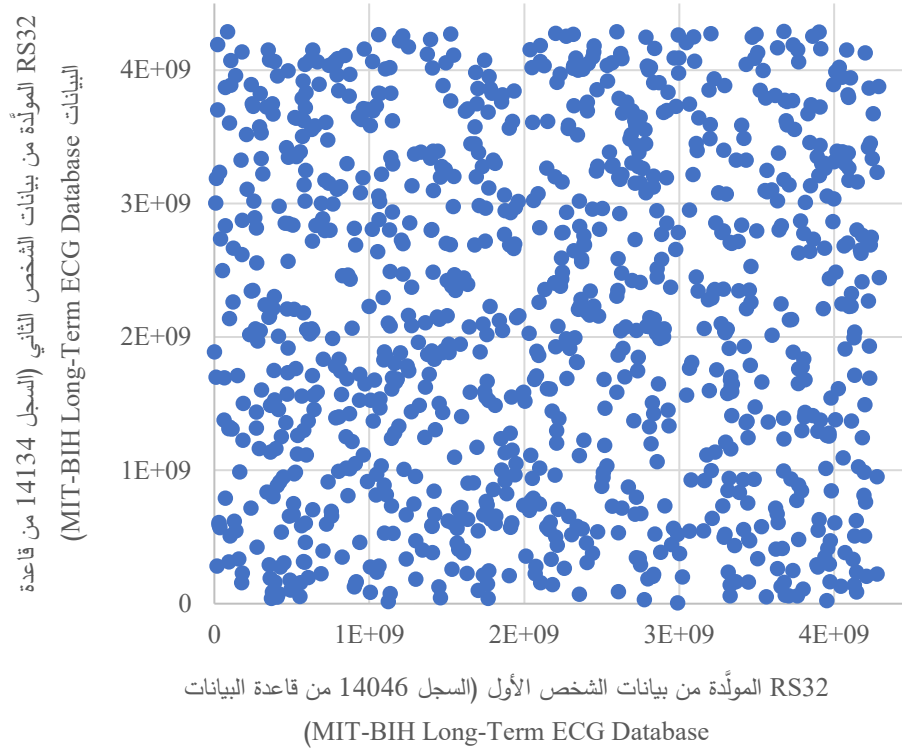
التوزع الطبيعي لمسافة هامينغ من أجل RS128 المولدة من بيانات الأشخاص الذين يعانون من عدم انتظام ضربات القلب. نلاحظ أيضاً أن قيمة هذا الوسطي تساوي 63.94 bit، وهو ما يقارب أيضاً 50% من طول RBS. وبالطريقة نفسها، يمكننا إثبات أن HD لها توزع طبيعي حتى ولو وُلدت RBS اعتباراً من بيانات الأشخاص الأصحاء أو مرضى عدم انتظام ضربات القلب، مهما كان طول RBS بين 128 bit و 2048 bit، ومهما كانت مدة تحصيل الإشارة بين ثانية وأربع ثوانٍ. يوضح الجدول 5-5 وسطى HDs بين RBSs الناتجة عن التجارب، من أجل RBSs بأطوال مختلفة، ومن أجل أزمنة تحصيل مختلفة، للأشخاص الأصحاء ومرضى عدم انتظام ضربات القلب. من الجدول 5-5، نلاحظ أن كافة قيم وسطى HDs تكون مقاربة لـ 50% من طول السلسلة، ونستنتج أن RBSs التي وُلدت من ECG تكون مميزة من شخص لآخر.

الجدول 5-5: وسطى مسافة هامينغ HD بين السلاسل العشوائية المولدة باستخدام المولد المطور.

RS2048	RS1024	RS512	RS256	RS128	مجموعة البيانات	زمن تحصيل الإشارة
1016.86	508.69	254.32	127.09	63.52	Healthy	ثانية واحدة
1023.09	511.86	256.06	127.95	63.94	Arrhythmia	
1020.96	510.26	255.09	127.54	63.75	Healthy	ثانيتان
1024.27	511.31	255.81	127.87	63.95	Arrhythmia	
1021.48	510.75	255.35	127.64	63.84	Healthy	أربع ثوانٍ
1021.30	511.09	255.70	127.96	63.97	Arrhythmia	

يمكن أيضاً تحليل التميز بين RBSs الناتجة عن أجسام مختلفة من خلال تحليل الترابط فيما بينها. لتحليل الترابط، تم دراسة وجود علاقة بين RBSs الناتجة عن إشارة ECG لشخص ما مع RBSs الناتجة عن إشارة ECG لشخص آخر من خلال التمثيل البياني. يبين الشكل 5-4 عدم وجود علاقة تربط بين قيم RS32 الناتجة عن إشارة ECG لشخص ما (بيانات السجل 14046) وقيم RS32 الناتجة عن إشارة ECG لشخص آخر (بيانات السجل 14134)، حيث يمثل المحور الأفقي القيم العشوائية الناتجة عن السجل 14046 من قاعدة البيانات MIT-BIH Long-Term ECG Database [44] ويمثل المحور العمودي القيم العشوائية الناتجة عن السجل 14134 من قاعدة البيانات نفسها، وتمثل كل نقطة العلاقة بين كل قيمة عشوائية مولدة من السجل 14046 والقيمة العشوائية المقابلة لها والمولدة من السجل 14134. دُرِس الترابط بين 1000 قيمة RS32 مولدة من كل من السجلين

(الشخصين). نلاحظ من الشكل 4-5 عدم وجود ترابط بين القيم الناتجة عن السجلين المذكورين. وبالمثل يمكن إثبات عدم وجود علاقة تربط بين القيم الناتجة عن أي سجل (شخص) والقيم الناتجة عن سجل (شخص) آخر.



الشكل 4-5: الترابط بين RS32 المولدة من إشارة ECG لشخصين مختلفين (السجلين 14046 و 14134 من قاعدة البيانات (MIT-BIH Long-Term ECG Database))

مما سبق، نستنتج أن السلاسل الناتجة عن المولّد المطوّر مميّزة من شخص لآخر ويمكن استخدامها لتطبيقات الأمان في WBANs. وبالتالي، لن يتمكن المهاجمون من تهديد شبكة WBAN لشخص معيّن باستخدام إشارة ECG لشخص آخر.

أظهرت التجارب المجراة على المخطط المقترح عدم وجود علاقة بين زمن تحصيل ECG والعشوائية الناتجة، على عكس النتائج في [24]، والتي اعتمدت العشوائية فيها على عدد نبضات القلب المحصلة. وأثبتت التجارب أيضاً أنه حتى بالنسبة لزمن تحصيل قدره ثانية واحدة فقط، فقد كان لـ RBSs الناتجة العشوائية المطلوبة.

5-3-5. أداء مولّد السلاسل العشوائية المطوّر ومعدل إنتاجه

في المخطط المقترح، وكما ذكرنا سابقاً، يمكننا توليد عدد من RS32 يساوي نصف عدد العينات المحصل كحد أقصى. فإذا كان معدّل أخذ العينات يساوي 128 عينة في الثانية، نستطيع توليد 64 سلسلة RS32 في الثانية؛ أي ما يعادل 2048 bit في الثانية. يمكن تجميعها حسب الحاجة لتشكيل سلاسل ذات أطوال مختلفة. أما إذا كان معدّل أخذ العينات يساوي 360 عينة في الثانية، فيمكننا في كل ثانية تشكيل 180 سلسلة RS32؛ أي ما يعادل 5760 bit في الثانية، يمكن تجميعها في سلاسل عشوائية ذات أطول مختلفة حسب الحاجة. بذلك نكون قد تفوقنا تقوفاً ملحوظاً على معدل توليد البتات العشوائية، أي معدل الإنتاج، في الدراسات السابقة.

وبما يتعلق باستهلاك الموارد، فيجدر بنا الإشارة إلى أن مولّد السلاسل المطوّر هو ذو استهلاك قليل للموارد؛ وذلك لأن العمليات التي ينفّذها لتوليد السلاسل العشوائية بسيطة للغاية. وأما بالنسبة للتعقيد الزمني للمولّد المطوّر، نلاحظ أنه مكوّن من حلقة واحدة يتم تنفيذها n مرة، حيث n هي عدد سلاسل RS32 المولّدة، ويتكوّن جسم الحلقة من توابع بسيطة F ، تعقيد كلّ منها يساوي $O(1)$. وبالتالي يكون التعقيد الزمني للمخطط ككل هو $O(n)$ حيث n تمثّل عدد سلاسل RS32 المولّدة.

رغم بساطة العمليّات إلا أننا استطعنا أن نثبت أن المولّد المقترح يولّد سلاسل تتمتع بالخصائص العشوائية المطلوبة لاستخدامها في حماية المعلومات. كما أن السلاسل المولّدة ليست ثابتة الطول، وإنما ذات أطوال مختلفة.

5-6- خاتمة

في هذا الفصل:

- طوّرنا مخطط لتوليد السلاسل العشوائية، انطلاقاً من الإشارة الحيوية ECG. يتميّز هذا المخطط بالبساطة الحسابية والعشوائية العالية لسلسلة القيم الناتجة، ومن ثمّ إنتاجية وأداء عالٍ في الحصول على القيم المولّدة كما هو موضّح في التقييم التجريبي.

- يتَّضح لنا أن دمج مولّد القيم العشوائية المطور في هذا الفصل، مع مخطط توليد المفاتيح المستنتج في الفصل السابق يرفع من سرّيّة مخطط توليد المفاتيح المشتركة ما بين الحساسات، ومن إمكانيّة استخدامه من أجل خوارزميات تعمية مختلفة.

الفصل السادس

تحسين خوارزمية التعمية TEA بالاعتماد على إشارة ECG

161	1-6- تمهيد
161	2-6- أهداف تطوير خوارزمية تعمية مُعتمدة على إشارة ECG لتعمية بيانات WBAN
161	3-6- المبادئ العامة لخوارزمية TEA المُحسنة المعتمدة على ECG
162	4-6- مخطط خوارزمية TEA المحسنة
167	5-6- النتائج والمناقشة حول TEA المُحسنة
167	1-5-6. أمان خوارزمية TEA المُحسنة
169	2-5-6. أداء خوارزمية TEA المُحسنة
171	6-6- خاتمة

6-1- تمهيد

من الدراسات السابقة في مجال تسمية بيانات WBAN، لَحِظْنَا أَنَّ السَّعْيَ نحو التَّوَصُّلِ إلى خوارزميات تسمية خاصة بشبكة WBAN ذات أداءٍ عالٍ يتناسب مع تطبيقات العناية بالصحة في الزمن الحقيقي، وذات استهلاك منخفض للطاقة، لا يزال موضعَ بحثٍ. كما بيَّنَّا أنَّ أفضل سيناريو يمكن تطبيقه لحماية شبكات WBAN هو استخدام خوارزميات التسمية المتناظرة مع مفاتيح حيوية، وهذا ما نتبعه في دراستنا. ودرسنا بشيءٍ من التفصيل خوارزمية التسمية مُتَناهية الصغر (TEA) والتي هي أبسط خوارزميات التسمية المتناظرة شائعة الاستخدام والأعلى أداءً، ولكنها تعاني من بعض الهجمات؛ نتيجة استخدام المفتاح نفسه في جميع جولات التنفيذ. نسعى في هذا الفصل إلى تحسين خوارزمية التسمية TEA؛ لزيادة مناعتها ضد تلك الهجمات، ورفع أدائها، من خلال الاستفادة من القيم المشتركة التي يتم التوصل إليها باستخدام مخطط ECG-AKES.

6-2- أهداف تطوير خوارزمية تسمية مُعْتَمَدَة على إشارة ECG لتسمية بيانات WBAN

نَهْدُفُ في هذه الدراسة إلى التوصل إلى خوارزمية تسمية بسيطة جداً وفعالة تَسْتَفِيدُ من القيم الحيوية المقاسة في حساسات WBAN، بحيث يكون استهلاكها لطاقة الحساس أصغر ما يمكن، وذات أداء أعلى من الطرق السابقة. نسعى لتحقيق ذلك بالاستفادة من القيم الحيوية المشتركة التي تم التوصل إليها من خلال مخطط تبادل المفاتيح المطوَّر في هذا البحث، ECG-AKES. كما نَهْدُفُ أيضاً إلى التوصل إلى خوارزمية آمنة بدرجة كافية لنقل المعلومات الطبية الحرجة الخاصة بالمرضى. فنسعى إلى ألا يكون رفع الأداء على حساب أمان عملية التسمية.

6-3- المبادئ العامة لخوارزمية TEA المُحَسَّنَة المعتمدة على ECG

نسعى في دراستنا هذه للتوصل إلى خوارزمية تسمية متناظرة لحماية البيانات المتبادلة في WBAN، تَسْتَخْدِمُ المفاتيح الحيوية والقيم الحيوية المتبادلة من خلال مخطط ECG-AKES. تعتمد خوارزمية التسمية التي نسعى إلى التوصل إليها على خوارزمية TEA كأساس لها بعد تحسينها لزيادة أمانها ورفع أدائها. تدور الفكرة الأساسية للتحسين حول زيادة أمان TEA بجعل مفاتيح جولاتها مختلفة من جولة إلى أخرى، وذلك بالاعتماد على القيم

السرية المشتركة (المجموعة S) التي توصلنا إليها باستخدام مخطط ECG-AKES، مما يساعد على إنقاص عدد الجولات المطلوب تنفيذها في TEA التقليدية، ومن ثمّ التوصل إلى أداء عالٍ جداً. وستتم عملية التعمية باستخدام مفاتيح حيوية ناتجة عن القيم السرية المتبادلة بين الحساسين.

6-4- مخطط خوارزمية TEA المحسنة

من خلال مخطط ECG-AKES، تمّ التوصل في كلا الحساسين اللذين يسعيان لتشكيل اتصال آمن فيما بينهما إلى مجموعة من القيم السرية المشتركة، وهي المجموعة S والتي يكون عدد عناصرها كحد أقصى يساوي 20 عنصراً. سيستفاد من قيم عناصر المجموعة S في جعل مقدار الإزاحة مختلف في كل جولة من جولات خوارزمية TEA المحسنة، وأيضاً في توليد المفتاح السري المشترك بين الحساسين. لتحقيق ذلك يجب بدايةً؛ أي قبل تنفيذ عملية التعمية أو عملية فك التعمية، تهيئة المفتاح السري المشترك، والقيم السرية المشتركة المستخدمة في عملية التعمية. فيما يأتي نورد شرحاً لكلٍ من مرحلة تهيئة المفاتيح ومرحلة التعمية وفك التعمية. ويبين الجدول 6-1 قائمة بالرموز المستخدمة في خوارزمية TEA المحسنة ودلالة كلٍ منها.

الجدول 6-1: قائمة بالرموز المستخدمة في خوارزمية TEA المحسنة، ودلالاتها.

الرمز	دلالته
Pr	تابع تبديل مواضع مبني على قيم المصفوفة r المؤلدة في مخطط ECG-AKES.
Pr ₂	تابع تبديل المواضع Pr ولكن عند تنفيذه من أجل كل عنصرين متتاليين معاً وكأنهما عنصر واحد.
rx	مصفوفة مكونة من 20 عنصراً مُستنتجة من المصفوفة r المؤلدة في مخطط ECG-AKES.
rx _{initial}	القيمة الابتدائية للمصفوفة rx.
rx'	ناتج تطبيق التابع Pr على المصفوفة rx _{initial} .
Prx	تابع تبديل مواضع مبني على قيم المصفوفة rx.
Sx	مصفوفة مكونة من 20 عنصراً ناتجة عن المصفوفة S بعد توسيعها، وإعادة ترتيبها باستخدام التابع Prx.

❖ مرحلة تهيئة المفاتيح

يمكن عدّ هذه المرحلة على أنها المرحلة السادسة في خوارزمية تبادل المفاتيح والتي سينتج في نهايتها المفتاح السري المشترك KEY، والقيم السرية المشتركة التي سنستخدمها في عملية التعمية. تتكوّن مرحلة التهيئة من الخطوات الآتية:

الخطوة الأولى: يُستنتج في هذه المرحلة مصفوفة تبديل المواضع الموسعة rx . وهي مصفوفة ناتجة عن توسيع المصفوفة r المولدة في مخطط ECG-AKES من أجل تشكيل مصفوفة تبديل مواضع ذات 20 عنصر؛ تُستخدم في تغيير ترتيب عناصر S . نحن بحاجة إلى مصفوفة تبديل مواضع ذات 20 عنصر لأن أكبر عدد لعناصر S هو 20. تُستنتج المصفوفة rx من المصفوفة r وفق الخطوات الجزئية الآتية:

- بدايةً يُستنتج التابع Pr انطلاقاً من r ، وهو عبارة عن تابع تبديل مواضع (Permutation function) مبني على قيم r ، كما هو مبين في المثال الموضح في الشكل 6-1-أ.
- ثملاً عناصر المصفوفة rx بالقيم الابتدائية وهي من 0 حتى 19 على التوالي، ونرمز لها بـ $rx_{initial}$.

- تُجرى عملية تبديل مواضع عناصر $rx_{initial}$ بالاعتماد على r ، أي باستخدام التابع Pr ، ولكن من أجل كل عنصرين متتاليين معاً وكأنهما عنصر واحد كما هو مبين في الشكل 6-1-ب؛ وذلك للاستفادة من التابع Pr الناتج عن المصفوفة r ذات العناصر العشرة. يُرمز لتلك العملية بـ Pr_2 ويُرمز للمصفوفة الناتجة عنها بـ rx' .

- من أجل زيادة عشوائية ترتيب العناصر، يُعاد ترتيب العناصر العشرة الأولى من عناصر rx' (بدءاً من العنصر الأول وحتى العنصر العاشر) باستخدام Pr ، ثم تُكرّر العملية بالنسبة لثاني عشرة عناصر (أي بدءاً من العنصر الحادي عشر وحتى العنصر العشرين) كما في الشكل 6-1-ب. يُرمز لهذه العملية بـ $Pr(rx'_{0-9}) || Pr(rx'_{10-19})$. عند انتهاء تنفيذ هذه الخطوة يتم التوصل إلى مصفوفة إعادة الترتيب rx المطلوبة. وبما أن $rx_{initial}$ تم ملؤها بالقيم من 0 حتى 19 على التوالي، وبناءً على قيم r في المثال الموضح في الشكل 6-1-أ، تكون قيم rx الناتجة كما هو مبين في الشكل 6-1-ج.

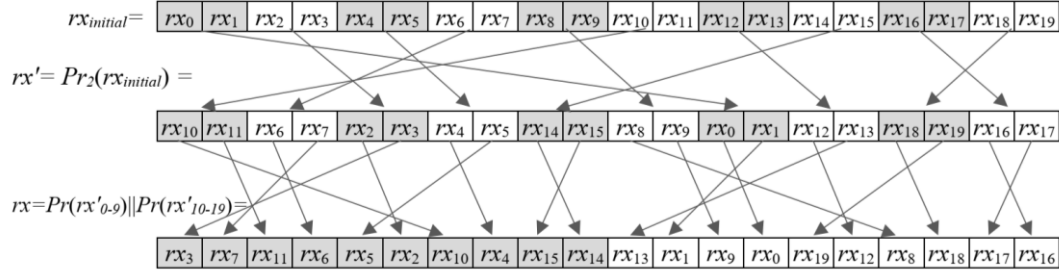
ويُبين الشكل 6-1-د تابع تبديل المواضع وفق rx الناتجة بحسب مثالنا، والذي يُرمز له بـ Prx .

$$r = \begin{bmatrix} 5 & 3 & 1 & 2 & 7 & 4 & 0 & 6 & 9 & 8 \end{bmatrix}$$

$$X = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 \end{bmatrix}$$

$$Pr(X) = \begin{bmatrix} x_5 & x_3 & x_1 & x_2 & x_7 & x_4 & x_0 & x_6 & x_9 & x_8 \end{bmatrix}$$

(أ)



(ب)

$$rx_{initial} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 \end{bmatrix}$$

$$rx = \begin{bmatrix} 3 & 7 & 11 & 6 & 5 & 2 & 10 & 4 & 15 & 14 & 13 & 1 & 9 & 0 & 19 & 12 & 8 & 18 & 17 & 16 \end{bmatrix}$$

(ج)

$$X = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_9 & x_{10} & x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & x_{16} & x_{17} & x_{18} & x_{19} \end{bmatrix}$$

$$Pr(X) = \begin{bmatrix} x_3 & x_7 & x_{11} & x_6 & x_5 & x_2 & x_{10} & x_4 & x_{15} & x_{14} & x_{13} & x_1 & x_9 & x_0 & x_{19} & x_{12} & x_8 & x_{18} & x_{17} & x_{16} \end{bmatrix}$$

(د)

الشكل 6-1: تشكيل المصفوفة rx والتابع Prx اعتباراً من r خلال مرحلة التهيئة في خوارزمية TEA المحسنة.

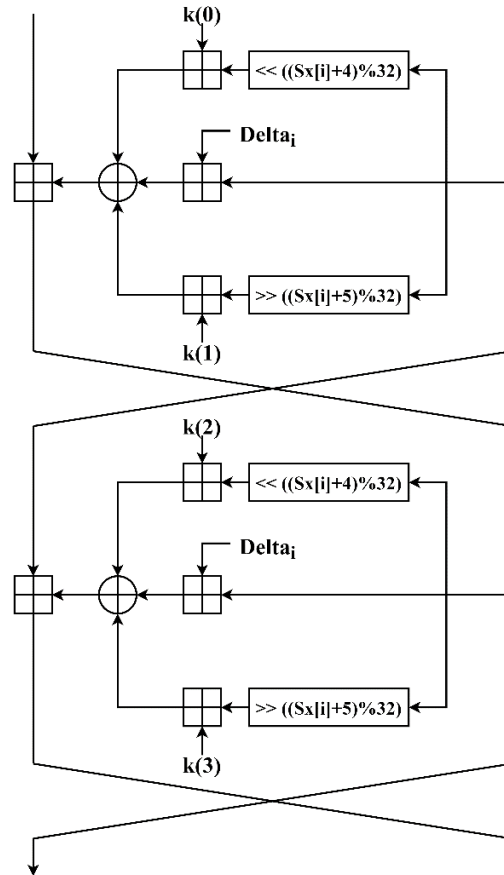
الخطوة الثانية: توسيع المجموعة S إلى 20 عنصراً وإعادة ترتيبها وفق rx أي باستخدام تابع التبديل Prx . في هذه المرحلة إذا كان عدد عناصر S الناتجة أقل من 20 عنصراً، وهو الاحتمال الأرجح، تُملأ أولاً العناصر المتبقية بالقيمة 0. ثم يتم تبديل مواضع عناصر S وتشكيل Sx ؛ بالاعتماد على التابع Prx الناتج عن rx . تُستخدَم المجموعة الناتجة Sx في تشكيل المفتاح السري المشترك KEY، كما تُستخدَم عناصرها لتحديد الإزاحة في كل جولة من جولات TEA المُحسَّنة.

الخطوة الثالثة: توليد مفتاح التعمية KEY ذي طول 128 bit؛ وذلك من خلال تطبيق تابع البصمة على المصفوفة Sx ؛ أي تطبيق تابع البصمة على النص المكوّن من عناصر Sx المتتالية. تابع البصمة هو عبارة عن تابع ذو اتجاه واحد، يحوّل دخل محدّد من الأرقام والحروف إلى خرج مُعَمّى ذو طول ثابت. من غير الممكن معرفة قيم

الدخل بمعرفة الخرج الناتج عن التابع، كما أن أي تغيير في دخل تابع البصمة مهما كان طفيفاً يؤدي حتماً إلى تغيير كبير في خرجه. بناءً على ذلك، تم استخدامه في توليد المفتاح KEY اعتباراً من S_x . ومن الأمثلة حول توابع البصمة الأكثر استخداماً والتي يمكن تطبيقها في هذا المخطط: التابع XOR، MD5، SHA، وغيرها.

تهدف عملية تغيير ترتيب عناصر S التي أُجريت في مرحلة التهيئة إلى زيادة عشوائية هذه المجموعة وتقليل احتمال تطابقها في دورتي تنفيذ مختلفتين من دورات توليد المفاتيح؛ وذلك لأن كل ترتيب مختلف لعناصر S ينتج عنه مفتاح KEY جديد، كما ينتج عنه قيم مختلفة للإزاحة في جولات TEA المعدلة. وبالتالي حتى ولو حدث احتمال تطابق S في دورتي تنفيذ مختلفتين، لن تتطابق بعد تغيير ترتيب عناصرها؛ وبناءً على ذلك لن يتطابق المفتاح السري KEY الناتج، ولن تتطابق قيم الإزاحة في جولات TEA المعدلة.

❖ مرحلة التعمية وفك التعمية



الشكل 6-2: عملية التعمية وفق خوارزمية TEA المُحسَّنة. حيث i هو رقم الجولة، k تُمثِّل المفاتيح الجزئية من المفتاح KEY، Δ_{tai} تُمثِّل أحد مضاعفات الثابت السحري، $S_x[i]$ العنصر i من المصفوفة S_x .

في هذه المرحلة تُستخدَم خوارزمية TEA للقيام بعملية التعمية وفق المفتاح KEY، ولكن بعد تعديل عمليتي الإزاحة نحو اليمين ونحو اليسار المستخدمتين في الخوارزمية الأصلية. يتم ذلك بتغيير قيمة الإزاحة من أجل كل جولة، وجعلها تساوي إحدى قيم S_x ؛ أي لن يبقى مقدار الإزاحة نحو اليسار ثابتاً، ويساوي 4 bit ومقدار الإزاحة نحو اليمين ثابتاً ويساوي 5 bit؛ وإنما سيصبح مقدار الإزاحة متغيراً من أجل كل جولة بحسب قيمة أحد عناصر S_x . وبيّن الشكل 2-6 خوارزمية TEA المحسّنة، وفيه يتّضح أن الإزاحة نحو اليسار أصبحت بمقدار $(S_x[i]+4)\%32$ bit والإزاحة نحو اليمين أصبحت بمقدار $(S_x[i]+5)\%32$ bit. استُخدمت عملية باقي القسمة على 32 لكي تتوافق الإزاحة مع طول الكلمة المُعمّاة. تُمثّل i رقم الجولة، وتمثّل Δ_i أحد مضاعفات الثابت السحري.

بما أنه قد تم تعديل عملية الإزاحة والتي أصبحت متغيرة من أجل كل جولة، فقد أصبح من الممكن الاكتفاء بتنفيذ 16 جولة (32 دورة فيستل) فقط؛ لأن تعديل الإزاحة في كل جولة وفقاً لقيم سرية مشتركة بين الحساسين سيؤدي إلى زيادة أمان الخوارزمية إلى حد كبير. وبالتالي ستُستخدم العناصر الست عشر الأولى فقط من S_x . أما بالنسبة لعملية فك التعمية، فستتغير الإزاحة لتصبح موافقة للإزاحة في عملية التعمية وبالتالي تُستخدَم عناصر S_x بترتيب معاكس لترتيب استخدامها في عملية التعمية. أي تكون الإزاحة نحو اليسار بمقدار $(S_x[16-i]+4)\%32$ bit والإزاحة نحو اليمين بمقدار $(S_x[16-i]+5)\%32$ bit. وتبيّن الخوارزمية 1-6 شبه الرماز لعملية التعمية وفق TEA المُحسّنة. أما الخوارزمية 2-6 فتبيّن شبه الرماز لعملية فك التعمية وفق TEA المُحسّنة.

خوارزمية 1-6: شبه الرماز لعملية التعمية وفق خوارزمية TEA المحسّنة.

```

Input:
v[2], k[4], delta=2654435769
Output:
v[2] // After encryption

sum ← 0, v0 ← v[0], v1 ← v[1]
for i ← 0 to 16 do
{
    sum += delta;
    v0 += ((v1 << ((Sx[i]+4)%32)) + k[0]) ^ (v1 + sum) ^ ((v1 >> ((Sx[i]+5)%32)) + k[1])
    v1 += ((v0 << ((Sx[i]+4)%32)) + k[2]) ^ (v0 + sum) ^ ((v0 >> ((Sx[i]+5)%32)) + k[3])
}
v[0]=v0; v[1]=v1;

```

خوارزمية 6-2: شبه الرماز لعملية فك التعمية وفق خوارزمية TEA المحسنة.

```

Input:
v[2], k[4], delta=2654435769
Output:
v[2] // After decryption

sum ← 0, v0 ← v[0], v1 ← v[1]
for i ← 0 to 16 do
{
    v1 -= ((v1<<((Sx[16-i]+4)%32))+k[0])^(v1+sum)^(v1>>((Sx[16-i]+5)%32))+k[1])
    v0 -= ((v0<<((Sx[16-i]+4)%32))+k[2])^(v0+sum)^(v0>>((Sx[16-i]+5)%32))+k[3])
    sum -= delta;
}
v[0]=v0; v[1]=v1;

```

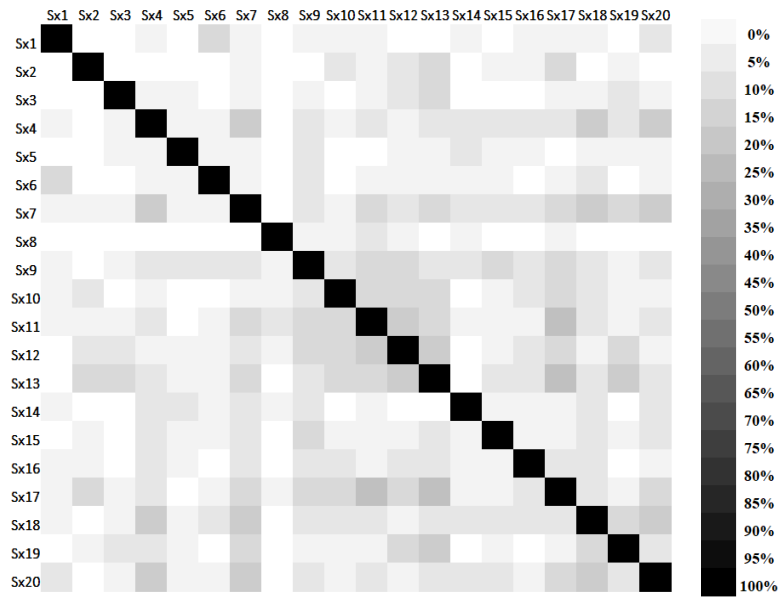
6-5- النتائج والمناقشة حول TEA المحسنة

فيما يلي نستعرض نتائج تطبيق خوارزمية TEA المحسنة. بدايةً نرغب أن ننوّه إلى أن جميع الاختبارات أُجريت باستخدام نتائج تطبيق مخطط تبادل المفاتيح ECG-AKES؛ أي طُبِّقَت التجارب، باستخدام قيم S و r و k الناتجة عن اختبار مخطط تبادل المفاتيح المطوّر في هذه الدراسة.

6-5-1. أمان خوارزمية TEA المُحسّنة

يُتيح مخطط تبادل المفاتيح المطوّر ديناميكية المفتاح، أي يمكن تغييره دورياً. فمن أجل كل قياس لنبضات القلب يُولّد مفتاح جديد، وبالتالي S جديدة والتي ينتُج عنها Sx جديدة و KEY جديد. للتحقق من مدى اختلاف مفاتيح TEA المُحسّنة الناتجة عن إشارة ECG للشخص نفسه والمكوّنة من أجل أزمنة بدء تحصيل إشارة مختلفة، تم إجراء قياس لمدى التشابه بين عشرين مصفوفة Sx للشخص نفسه، ولكن من أجل لحظات عشوائية لبدء تحصيل إشارة ECG.

يبين الشكل 6-3 مصفوفة التشابه (Similarity Matrix) بين عشرين مصفوفة Sx مختلفة للشخص نفسه. نلاحظ أن تلك المصفوفات غير متشابهة، وأن التشابه فيما بينها طفيف جداً. وبالتالي مقدار الإزاحة في أثناء تطبيق خوارزمية TEA المُحسّنة لا يمكن معرفته بمعرفة قيمة Sx سابقة للشخص نفسه. كما أنه من الملاحظ أن اختلاف Sx حتى ولو كان بقيمة واحدة فقط، سيؤدي إلى حتمية الحصول على مفتاح KEY مختلف عن المفاتيح السابقة. فهو ينتج عن تطبيق تابع البصمة على المجموعة Sx التي أثبت أنها تختلف من أجل كل قياس.



الشكل 6-3: مصفوفة التشابه بين عشرين مصفوفة Sx ناتجة عن إشارة ECG للشخص نفسه من أجل أزمنة بدء تحصيل مختلفة، حيث يمثل اللون الأبيض عدم تطابق أي عنصرين متقابلين من عناصر مصفوفتي Sx التي يتم مقارنتهما (تشابه بنسبة 0%)، ويمثل اللون الأسود تطابق كافة العناصر (تشابه بنسبة 100%).

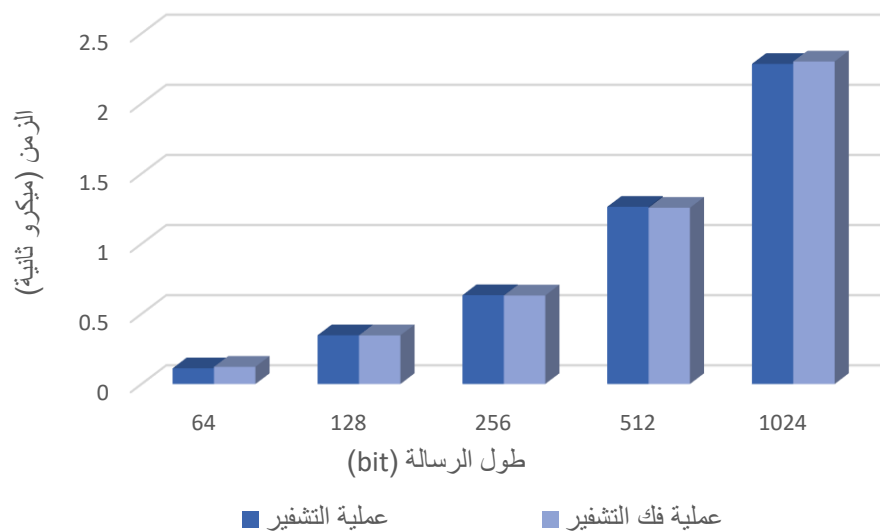
أما بما يتعلّق بأمان خوارزمية TEA المحسّنة، فيمكن ملاحظة أن التعديل الذي أُجري على بنية الخوارزمية بجعل الإزاحة متغيرة في كل جولة بمقدارٍ سرّي، سيُلغي تأثير الهجمات المشروحة في الدراسة المرجعة، وسيجعلها غير قابلة للتطبيق. فمن المُلاحَظ أن جميع الهجمات على خوارزمية TEA ترتبط بمفاتيح التعمية، وباستخدام المفتاح نفسه في جميع الجولات. وقد اقترح بعضُ الباحثين كما في [88] أن تكون مفاتيح التعمية مختلفة في كلّ جولة تنفيذ لنفاذي الهجمات. كذلك الأمر في خوارزمية TEA المُحسّنة المقترحة في هذه الدراسة، يُعدّ تغيير الإزاحة بمقدارٍ سرّي في كل جولة هو بمثابة استخدام مفتاح مختلف من أجل كل جولة.

نتيجةً لزيادة أمان خوارزمية TEA المُحسّنة عن أمان خوارزمية TEA التقليدية، نقترح أن نكتفي بعدد من جولات التنفيذ يساوي 16 جولة. فإذا اعتمدنا هذا العدد من الجولات سنلحَظ أن مقدار الأمان المضاف لهذه الخوارزمية سيكون مساوياً لـ 5 بتّات في كل جولة. فإذا نُفِدت الخوارزمية من أجل 16 جولة، سيكون مقدار الحماية المضاف يعادل 80 bit؛ أي يكون مستوى أمان TEA المُحسّنة يعادل التعمية بمفتاح طوله $128+80=208$ bit.

2-5-6. أداء خوارزمية TEA المُحسَّنة

لتقييم أداء TEA المُحسَّنة، قُورِنَ أدائها بأداء خوارزمية AES الأكثر شيوعاً والمُستخدمة في المعيار IEEE 802.15.6 الخاص بشبكات WBAN. اختُبِرَت TEA المُحسَّنة، باستخدام بيانات 12 شخصاً كما في اختبار ECG-AKES، وذلك بتشكيل 20 مفتاحاً مختلفاً من إشارة ECG لكل شخص. عُيِّنَت رسائل متعدِّدة الأطوال بدءاً من 64 bit وحتى 1024 bit. ثم حُسِبَ وسطي الأزمنة الناتجة. كُرِّرَت كل تجربة 10^5 مرة من أجل كل مفتاح، وكل رسالة، وذلك لكي نستطيع التوصل إلى نتائج دقيقة. أما بالنسبة لخوارزمية AES فتم تعمية البيانات نفسها باستخدام المفتاح KEY نفسه ذي 128 bit، وأيضاً كُرِّرَت كل تجربة 10^5 مرة من أجل كل مفتاح، وكل رسالة.

يبين الشكل 4-6 زمن التعمية وزمن فك التعمية، باستخدام خوارزمية TEA المُحسَّنة، وذلك من أجل أطوال مختلفة للرسائل. نلاحظ أنَّ زمن التعمية مساوٍ تقريباً لزمن فك التعمية، وهذا الأمر طبيعي؛ لأن خوارزمية التعمية هي نفسها خوارزمية فك التعمية.

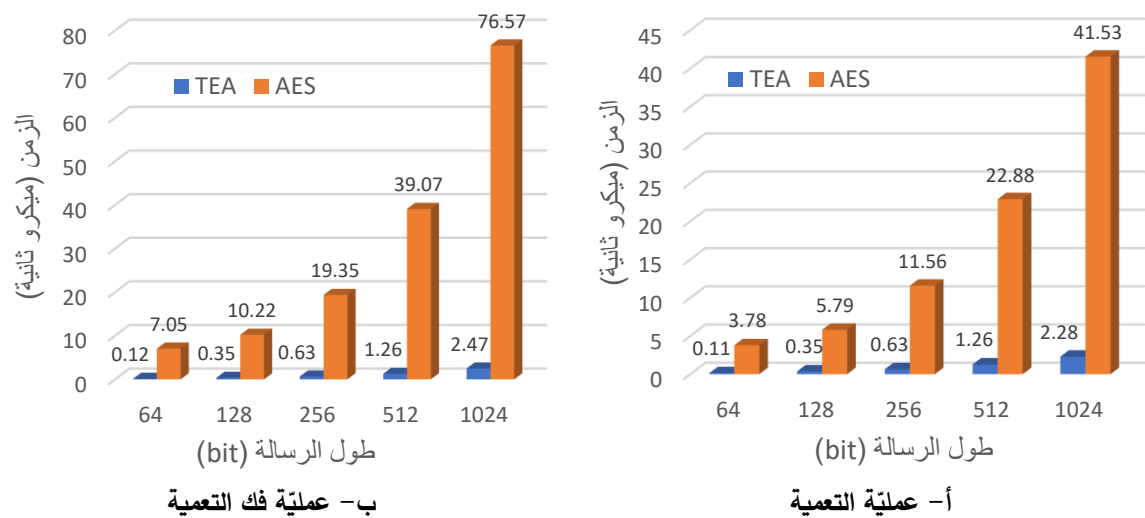


الشكل 4-6: زمن تنفيذ عملية التعمية وعملية فك التعمية باستخدام خوارزمية TEA المُحسَّنة.

يبين الشكل 5-6 أ مقارنَةً لأداء عملية التعمية باستخدام TEA المُحسَّنة مع أداء عملية التعمية باستخدام

AES، من أجل رسائل ذات أطوال مختلفة. ويبين الشكل 5-6 ب مقارنَةً أداء عملية فك التعمية باستخدام TEA

المُحسَّنة مع عمليّة فك التعمية باستخدام AES؛ وذلك أيضاً من أجل رسائل ذات أطوال مختلفة. نلاحظ أن خوارزمية TEA المُحسَّنة أسرع بكثير من خوارزمية AES. تُظهر النتائج التجريبية أن عملية التعمية باستخدام خوارزمية TEA المُحسَّنة، أسرع بحوالي 16 مرة من عمليّة التعمية باستخدام خوارزمية AES. أما عمليّة فك التعمية، فهي أسرع بحوالي 30 مرة. سبب الاختلاف بين زمن تنفيذ عمليّة التعمية، وعمليّة فك التعمية في خوارزمية AES هو طريقة تنجيزها. ولكن مهما كانت طريقة التّجيز تبقى خوارزمية TEA المُحسَّنة أسرع بكثير من خوارزمية AES، فعمليات المعالجة التي تحتاجها أبسط بكثير.



الشكل 5-6: مقارنة بين زمن تنفيذ خوارزمية TEA المُحسَّنة وزمن تنفيذ AES.

اختُبِرَت الخوارزمية وأُجريت عمليات التعمية، وفك التعمية، باستخدام الحاسب، وهو ذو أداء أعلى بكثير من أداء حساسات شبكة WBAN؛ مما قد يجعل تطبيق هذه الخوارزمية ضمن حساسات WBAN ذات نتائج مختلفة من حيث زمن التنفيذ المُستغرق. ولكن ستبقى النسبة بين زمن تنفيذ TEA المُحسَّنة وزمن تنفيذ AES هي نفسها مهما كانت المنصّة التي ستُطبّق الخوارزميات ضمنها، وستبقى خوارزمية TEA المُحسَّنة متفوقة عليها بحوالي ست عشرة مرة على أقل تقدير.

6-6- خاتمة

في هذا الفصل، حَسَّنَا خوارزمية TEA، وذلك بجعل الإزاحة فيها متغيرة من جولة إلى أخرى، بهدف زيادة مناعتها ضد الهجمات الناتجة عن استخدام المفتاح نفسه في جميع جولات تنفيذ الخوارزمية. حُسِّنَت الخوارزمية من خلال الاستفادة من القيم السريّة المشتركة المتبادلة باستخدام مخطط ECG-AKES؛ وذلك بطريقة تضمن تعديل مقدار الإزاحة في كل جولة. بفضل التحسينات المجراة، تمكَّنّا من التوصل إلى خوارزمية آمنة، وعالية الأداء، ومناسبة لحماية البيانات الطبيّة الحرجة، كما أنها مناسبة للعمل في الزمن الحقيقي.

الفصل السابع

المساهمة العلمية والمناقشة

173	1-7- تمهيد
173	2-7- مقارنة بين مخطط ECG-AKES المطور والدراسات السابقة
177	3-7- مقارنة بين مخطط توليد السلاسل العشوائية المطور والدراسات السابقة
179	4-7- مقارنة بين خوارزمية TEA المحسنة والدراسات السابقة
180	5-7- الحادثة والمساهمة التي توصل إليها البحث
183	6-7- مقارنة بين المخططات المطورة وأساليب الحماية في تقانات الاتصال في WBAN
184	7-7- خاتمة

7-1-تمهيد

في هذا الفصل، نُقارن المخططات المطوّرة في هذا البحث مع مخططات حماية WBAN الواردة في الدراسات السابقة، ونبيّن ميزاتّها. كما نسلط الضوء على الحداثة والمساهمة التي قدمناها في مجال حماية شبكات WBAN من خلال بحثنا هذا. وختاماً، نُقارن بين المخططات المطوّرة وطرق الحماية في تقانات الاتصال المُستخدمة في WBAN.

7-2-مقارنة بين مخطط ECG-AKES المطوّر والدراسات السابقة

فيما يلي نُقارن بين مخطط ECG-AKES المطوّر ومخططات تبادل المفاتيح بالاعتماد على إشارة ECG المقترحة في الدراسات السابقة، وذلك من نواحي عدّة.

أ. **خصائص الإشارة المُستخدمة لتوليد و/أو تبادل المفاتيح:** اعتمدَ المخطط المطوّر في هذه الدراسة على كلّ من الخصائص الترددية والخصائص الزمنية لإشارة ECG. أما في [20] استُخدمت الخصائص الزمنية فقط، وهي IPI. في PSKA [13] و ECG-IJS [23] و [5] استُخدمت الخصائص الترددية، وهي دليل المركبة الترددية العظمى لنتائج تطبيق FFT على إشارة ECG لعدد محدّد من العينات، لنافذة واحدة، أو لعدّة نوافذ. ولكن، أثبتنا في دراستنا أنه في معظم الأحيان لا يتطابق دليل المركبة الترددية العظمى المُستنتج في الحساس الأول مع دليل المركبة الترددية العظمى المُستنتج في الحساس الثاني، وهذا ما دفعنا إلى استخدام مجموعة أدلة المركبات الترددية العظمى (مؤشرات القمم) لنتائج تطبيق FFT على إشارة ECG في مخططنا المطوّر. أما في [22] استُخدمت قيم عينات ECG؛ وذلك يؤدي إلى صعوبة بالغة في التوصل إلى مفتاح سري مشترك بين الحساسين.

ب. **استخدام القيم الحيويّة:** في المخطط المطوّر يُستفاد من القيم الحيويّة في توليد المفتاح وفي تبادله. وكذلك الأمر بالنسبة لمخطط الإدارة القائمة للمفتاح متعددة النقاط [20] و [22] و [5]. أما في PSKA [13]

و ECG-IJS [23] تُستخدَم القيم الحيويّة فقط في تبادل المفتاح وليس في توليده، حيث يُؤلّد باستخدام مولّد أرقام عشوائية.

ت. استخدام رماز تصحيح الأخطاء: في المخطط المطوّر ليس هنالك حاجة لاستخدام رماز تصحيح الأخطاء مما يقلل من العبء الحسابي، وكذلك الأمر في [5]. أما في [20] استُخدِم من أجل تجاوز مشكلة اختلاف قيم ECG المقاسة في اللحظة نفسها في حساسين مختلفين موضوعين على الجسم نفسه. في PSKA [13] يُستخدَم رماز تصحيح الأخطاء من أجل تكوين vault، بالاعتماد على طريقة Fuzzy Vault. في ECG-IJS [23] يُستخدَم رماز تصحيح الأخطاء من أجل تكوين كثير الحدود الذي يجب أن يتطابق بين الحساسين. أما في [22] يُستخدَم من أجل تصحيح الاختلاف بين المفتاح المكوّن لدى كلّ من الحساس الأب والحساس الابن، كما يُستخدَم من أجل تشكيل المفتاح بين الابنين.

ث. الحمل الناتج عن الاتصالات اللاّزمة: يحتاج المخطط المطوّر إلى إرسال X_A من الحساس A إلى الحساس B وإرسال X_B من الحساس B إلى الحساس A. حجم كل من X_A و X_B يساوي 800 Byte. في مخطط الإدارة القائمة للمفتاح متعددة النقاط [20] يُرسل المفتاح بعد إخضاعه لتابع البصمة؛ بالإضافة إلى جزء آخر من خرج تطبيق تابع البصمة، يعتمد طولها على الأمان المطلوب. يحتاج مخطط PSKA [13] إلى نقل حجم كبير جداً من البيانات، فهو يحتاج إلى نقل بيانات تحوي نقاط ضجيج يتراوح عددها بين 0 و 2^{13} نقطة، حجم كلّ منها 36 bit؛ وذلك لأن أمان المخطط يعتمد على عدد تلك النقاط. في ECG-IJS [23] يُرسل عددٌ محدّد من معاملات كثير الحدود بالإضافة إلى MAC الرسالة المُعمّاة. أما في [22] يُرسل 136 bit من كلّ من العقدتين إلى العقدة الأب الذي يقوم بدوره بإرسال 128 bit إلى كلّ من الابنين. أما في [5] فحجم البيانات المتبادلة من أجل تشكيل المفتاح هو 129 bit.

ج. زمن تحصيل الإشارة: يحتاج المخطط المطوّر بدءاً من الدورة الثالثة للتنفيذ إلى تحصيل 20 نبضة قلب. بينما في مخطط الإدارة القائمة للمفتاح متعددة النقاط [20]، يُنشأ المفتاح اعتباراً من قيم IPI بطريقة تَسْتَعْرِق كحد أدنى 54 ثانية للحصول على مفتاح طوله 128 bit. وإذا لم تكن القيم الناتجة بدرجة كافية

من العشوائية فسيحتاج المخطط إلى زمن تحصيل أكبر. لحل تلك المشكلة اقترح تقسيم المفتاح إلى قسمين، القسم الأول يُشكّل اعتباراً من قيم IPI، أما القسم الثاني فيُشكّل باستخدام مولّد أرقام عشوائية. قد يُقلّل ذلك زمن تشكيل المفتاح بشكل بسيط، ولكنه يزيد التعقيد الحسابي بشكل كبير. أما بالنسبة ل PSKA [13] و ECG-IJS [23] و [5] فهي تحتاج إلى تحصيل إشارة لمدة 4 ثوانٍ، وهو الزمن الكافي لضمان وجود نبضة واحد على الأقل في الإشارة المحصّلة. أما في [22] فلم يُحدّد الزمن المطلوب لتحصيل الإشارة اللازمة.

ح. FAR و FRR: في المخطط المطوّر، وبالنسبة للعتبات المُعتَمَدة، أي عندما تكون $Th=0.01$ وأصغر قيمة مقبولة لعدد عناصر S هي 3، يكون FAR=0% و FRR=4.1%. في مخطط الإدارة العائمة للمفتاح متعددة النقاط [20] فقد يصل FRR إلى 17% أما FAR يصل إلى 0.04%. في PSKA [13] عندما يكون ترتيب كثير الحدود يساوي 15، تكون FAR مساوية لـ 0% ولكن تصل FRR إلى 80%. في ECG-IJS [23] عندما تكون درجة كثير الحدود مساوية لـ 8 ومقدار الأخطاء التي يمكن تصحيحها $t=1$ يكون FAR=0% و FRR=0.027%، أما عندما $t=5$ يكون FAR=0.0156% و FRR=0.01%. في [5] تكون FAR و FRR أكبر من الصفر. أما بالنسبة للمخطط الوارد في [22] فتكون فيه FAR و FRR مساوية لـ 0%.

خ. التسامح مع ضعف التزامن بين الحساسات: يُعدّ المخطط المطوّر متسامحاً مع ضعف التزامن، حيث أثبت ذلك سابقاً. لم يُدرّس التسامح مع ضعف التزامن في كلّ من [20] و ECG-IJS [23]. بالنسبة إلى PSKA [13] فهو متسامح مع إزاحة زمنية تصل إلى ثانية. أما [22] و [5] ليست متسامحة أبداً مع ضعف التزامن.

يبين الجدول 1-7، وهو تكملة الجدول 1-3، مقارنة بين مخطط ECG-AKES المطوّر والدراسات السابقة من حيث النواحي التي تم شرحها.

الجدول 7-1: مقارنة بين مخطط ECG-AKES المطور والدراسات السابقة

ECG-AKES	المخطط المقترح في [5]	المخطط المقترح في [22]	ECG-IJS [23]	PSKA [13]	Multipoint fuzzy key management [20]	
المجال الزمني والمجال الترددي	المجال الترددي	المجال الزمني	المجال الترددي	المجال الترددي	المجال الزمني	مجال استخراج خصائص ECG
في توليد المفاتيح وتبادلها	في توليد المفاتيح وتبادلها	في توليد المفاتيح وتبادلها	في تبادل المفاتيح	في تبادل المفاتيح	في توليد المفاتيح	الاستفادة من خصائص ECG
متوسط 800 bytes	متوسط 129 bytes	صغير (عشرات البايتات)	صغير (عشرات البايتات)	كبير جداً، 2^{13} نقطة، حجم كل منها عدة بايتات	صغير (عشرات البايتات)	الحمل الناتج عن الاتصالات اللازمة
20 نبضة قلب ≈ 17 ثانية	4 ثوانٍ	–	4 ثوانٍ	4 ثوانٍ	أكثر من 54 ثانية	زمن التحصيل
كافة الأطوال	كافة الأطوال	128 bit	–	128 bit	–	طول المفتاح المولد
غير مستخدم	غير مستخدم	BCH	Reed– Solomon	يستخدم في Fuzzy-vault	BCH	استخدام توابع تصحيح الأخطاء
متسامح مع التزامن الضعيف	صارمة	صارمة	–	متسامح مع التزامن الضعيف	–	درجة التزامن المطلوبة
FAR=0%, FRR=4.1%	$> 0\%, > 0\%$	0%, 0%	$> 0\%, > 0\%$ تعتمد على درجة كثير الحدود	$> 0\%, > 0\%$ تعتمد على درجة كثير الحدود	$> 0\%, > 0\%$ تعتمد على معاملات BCH	FRR و FAR

يستفيد مخطط ECG-AKES من خصائص ECG لتوليد وتبادل المفاتيح السرية. على عكس الدراسات السابقة، فإنه يستخدم خصائص ECG في كلٍّ من المجال الزمني والمجال الترددي. إنه يستفيد من خصائص المجال الزمني من دون الوقوع في عيوبه مثل التأخير الزمني الكبير جداً. من الجدول 7-1، يتضح أنه على الرغم من أن مخطط الإدارة القائمة للمفتاح متعددة النقاط [20] يتطلب نقل رسائل أقصر، إلا أن مخططنا يتفوق عليه بزمان تحصيل الإشارة المطلوبة، واستخدام القيم الحيوية ليس فقط من أجل تبادل المفاتيح السرية، وإنما من أجل توليدها أيضاً. بالنسبة لمخطط PSKA [13]، تكون مدة تحصيل الإشارة المطلوبة أقل من المدة المطلوبة للمخطط المطور. ولكن من ناحية أخرى، يحتاج PSKA إلى نقل كمية كبيرة جداً من البيانات؛ كما أنه يحتاج أيضاً إلى عمليات معالجة معقدة لإتمام عملية فك التعمية؛ مما يجعله مستهلكاً لموارد الحساس بشكل كبير، على عكس

ECG-AKES الذي يعتمد على عمليات حسابية بسيطة جداً، ويحتاج إلى نقل كمية أقل من البيانات. مقارنةً بمخططنا المطور، يتطلب ECG-IJS [23] مدةً تحصيل إشارة أقل وتبادل حجم أقل من البيانات، ولكن تكون فيه FAR أكبر من الصفر (مع ملاحظة أن FAR في مخططنا تساوي الصفر)، مما يجعل حدوث الاختراقات أكثر احتمالاً؛ فضلاً عن الحاجة إلى بعض العمليات المعقدة من أجل البحث عن كثير حدود يلتقي بنقاط محددة. في المخطط المقترح في [22]، تكون كمية البيانات المرسلّة أقل من كمية البيانات المرسلّة في ECG-AKES، ولكن على عكس ECG-AKES، فهو يعاني من الحاجة إلى دقة كبيرة في التزامن، ويعاني أيضاً من الحاجة إلى ثلاثة كيانات لتبادل المفاتيح السرية؛ مما يؤدي بدوره إلى زيادة التعقيد واستهلاك الطاقة. علاوةً على ذلك، يعتمد المخطط المقترح في [22] على قيم عينات إشارة ECG، وهو أمر غير عملي؛ نظراً لأن قيم عينات ECG تختلف اختلافاً كبيراً عند قياسها في حساسين مختلفين. أخيراً، تكون تكلفة الاتصال في المخطط المقترح في [5] أقل ومدةً تحصل الإشارة أقصر، ولكنه يعاني من الحاجة إلى دقة كبيرة في التزامن المطلوب، وتكون فيه FAR لا تساوي الصفر، في حين أن ECG-AKES متسامح مع ضعف التزامن و FAR فيه تكون مساويةً للصفر.

7-3- مقارنة بين مخطط توليد السلاسل العشوائية المطور والدراسات السابقة

في دراستنا هذه، استطعنا التوصل إلى مولّد سلاسل عشوائية يُولّد عدداً كبيراً من السلاسل العشوائية بفترة زمنية محدودة جداً على عكس باقي المولّدات المعتمدة على إشارة ECG المطوّرة في الدراسات السابقة.

الجدول 7-2: معدّل إنتاج مولد السلاسل العشوائية المطور مقارنةً بمعدلات إنتاج المولّدات المقترحة في الدراسات السابقة.

الطريقة	معدل الإنتاج
طريقة Xu وآخرون [32]	16 bit/second (60 PPMs)
	26.6 bit/second (100 PPMs)
طريقة Pirbhulal وآخرين [24]	16 bit/second (60 PPMs)
	26.6 bit/second (100 PPMs)
طريقة Camara وآخرين [25]	184 bit/second (60 PPMs)
	306 bit/second (100 PPMs)
مولد السلاسل العشوائية المقترح	2048 bit/second (sampling rate 128 sample/ second)
	5760 bit/second (sampling rate 360 sample/ second)

يبين الجدول 2-7 معدل إنتاج مولّد السلاسل العشوائية المقترح مقارنةً بمعدل إنتاج الطرائق السابقة. نلاحظ تفوقاً كبيراً لمولّد السلاسل العشوائية المطوّر في هذه الدراسة على باقي مولّدات السلاسل العشوائية المعتمدة على إشارة ECG. كما نلاحظ ارتباط الإنتاجية بمعدل أخذ العينات على خلاف الطرائق السابقة التي تعتمد فيها الإنتاجية على عدد نبضات القلب في الدقيقة (PPMs). ولكن حتى بالنسبة لمعدل اعتيان منخفض (وهو 128 عينة / الثانية) يبقى المولّد المطوّر ذو إنتاجية أعلى من جميع المولّدات السابقة.

يتميّز مولّد السلاسل العشوائية المطوّر في دراستنا كما في [25] بعدم الاعتماد على قيم IPI؛ وإنما تُستخدم قيم عينات إشارة ECG لاستخراج العشوائية. طريقتنا هي من الطرائق القليلة لمولّدات السلاسل العشوائية المعتمدة على نبضات القلب التي لم تعتمد على IPI، وهي ليست الوحيدة. ولكن ما يميّزها عن غيرها هو الإنتاجية التي استطعنا التوصل إليها؛ حيث يتجاوز المولّد المقترح أسلافه من حيث الإنتاجية بحوالي عشرات أو مئات المرات. فضلاً عن ذلك، لا يحتاج المولّد المطوّر إلى عمليات تعمية أو إلى تحليل طيفي أو توابع البصمة أو غيرها من العمليات التي قد تستهلك طاقة الحساسات، فهو يميّز ببساطة العمليات، مما يؤدي إلى توفير عمليات المعالجة، وتقليل استهلاك طاقة حساسات WBAN.

من أجل اختبار عشوائية وتمييز السلاسل الناتجة عن المولّد المطوّر، أُجريت الاختبارات العمليّة للعشوائية والتمييز على مجموعتين من البيانات، وهي بيانات أشخاص أصحاء، وبيانات أشخاص مرضى بعدم انتظام ضربات القلب. كان بالإمكان الاكتفاء باختبار المولّد المطوّر باستخدام بيانات أشخاص أصحاء وهو أسوأ السيناريوهات، لأن المرض نفسه من شأنه أن يُضيف المزيد من الإنتروبية إلى إشارة ECG. ولكن مع ذلك اختبرنا المولّد باستخدام بيانات مرضى عدم انتظام ضربات القلب للتحقق بشكل عملي من عشوائية السلاسل الناتجة عنها.

هناك جانب آخر مهم بالنسبة للمولّد المطوّر، ألا وهو اختبار ما إذا كان لدى الخصم إمكانية التنبؤ بالقيم العشوائية للمستخدم المستهدف باستخدام إشارة ECG لمستخدم آخر. بيّنا سابقاً أن التجارب التي أُجريت تشير إلى عدم وجود فرصة للمهاجم في النجاح بذلك. علاوةً على ذلك، وعلى عكس الطرق القائمة على IPI، فإن استخدام قيم عينات إشارة ECG في توليد السلاسل العشوائية يَمْنَعُ الهجمات التي يتم فيها التنصّت على إشارة القلب من

مسافة بعيدة، كمرقبة تغيّر لون البشرة بواسطة الكاميرات. كما أثبت أن التوصل إلى إشارة ECG من قبل المهاجم، بالاعتماد على السلاسل العشوائية الناتجة، هي عملية غير مجدية زمنياً، في حين لم يُثبت ذلك في الدراسات السابقة.

يبين الجدول 3-7 مقارنة بين المولد المطور والدراسات السابقة، من حيث النقاط الأساسية المذكورة للتو.

الجدول 3-7: مقارنة بين مولّد السلاسل العشوائية المطوّر والدراسات السابقة

الدراسة	طريقة Xu وآخرين [32]	طريقة Pirbhulal وآخرين [24]	طريقة Camara وآخرين [25]	مولّد السلاسل العشوائية المطوّر
معدل الإنتاج	منخفض	منخفض	مرتفع	مرتفع جداً
طول السلاسل التي اختُبرت العشوائية والتفرد من أجلها	128 bit	128 bit	اختبار العشوائية لملفات ذات أحجام كبيرة، واختبار التميز لسلاسل طولها 64 bit أو أقل.	128 bit، 256 bit، 512 bit، 1024 bit، 2048 bit
بساطة عمليات المعالجة	بسيطة	معقدة	معقدة	بسيطة
أمن الخوارزمية ضد فضح إشارة ECG اعتباراً من القيم العشوائية الناتجة	لم تُدرس	لم تُدرس	لم تُدرس	آمنة

7-4- مقارنة بين خوارزمية TEA المُحسّنة والدراسات السابقة

بالعودة إلى الخوارزميات الواردة في الدراسة المرجعية، نلاحظ أن خوارزمية TEA المُحسّنة هي الأفضل. في [98] و [38] اعتُمدت التعمية غير المتناظرة بشكل كامل أو كجزء من عملية التعمية. ولكن مهما كانت التعديلات المجراة على خوارزميات التعمية غير المتناظرة لتحسين أدائها، تبقى ذات أداء أخفض بكثير من خوارزميات التعمية المتناظرة، وبالتحديد من خوارزمية TEA المُحسّنة؛ لأنها تعتمد على توابع رياضية معقدة تحتاج إلى زمن كبير لتنفيذها. أما بالنسبة للخوارزمية المقترحة في [37] فأثبت الباحثون أن زمن تنفيذها أقل من نصف زمن تنفيذ AES، أما خوارزمية TEA المُحسّنة فزمن تنفيذها أقل بست عشرة مرة أو أكثر من زمن AES. وبالعودة إلى [6] نلاحظ أن الخوارزمية المطروحة أكثر تعقيداً من خوارزمية TEA المُحسّنة، فهي تتألف من عدد أكبر من الخطوات

(10 خطوات لعملية التعمية و8 لعملية فك التعمية)، كما أنها تحوي على S-Boxes وغيرها من العمليات التي تجعلها أبسطاً من خوارزمية TEA المُحسَّنة. بالنسبة للمعيار IEEE 802.15.6 [63] المُعتمد في شبكات WBAN فهو يَستخدم خوارزمية AES لتعمية البيانات والتي أثبتنا انخفاض أدائها مقارنةً بخوارزمية TEA المُحسَّنة.

7-5- الحادثة والمساهمة التي توصل إليها البحث

نقدم فيما يلي الحادثة والمساهمة التي يقدمها هذا البحث وذلك من أجل كافة المخططات المطوّرة.

أ. الحادثة والمساهمة بالنسبة لمخطط ECG-AKES

في هذا البحث، وبالنسبة لمخطط ECG-AKES المطوّر، تكمن مساهمتنا في استخدام خصائص ECG المستخرجة في المجالين الزمني والترددي معاً من أجل إنشاء المفتاح السري وتبادلته ضمن مخطط جديد يلغي الحاجة إلى استخدام أرمزة تصحيح الخطأ وفي الوقت نفسه يفي بالمتطلبات اللازمة. يوضح الجدول 4-7، وهو ملحق الجدول 2-3، أن ECG-AKES يلبي جميع المتطلبات الأساسية لمخطط تبادل المفاتيح المصادق عليها في شبكة WBAN.

الجدول 4-7: ملحق الجدول 2-3، المتطلبات الواجب تحقيقها في مخطط تبادل المفاتيح المُعتمد على القيم الحيوية، ومدى تلبية تلك المتطلبات في مخطط ECG-AKES.

ECG-AKES	المتطلبات الواجب تحقيقها في مخططات تبادل المفاتيح المعتمدة على القيم الحيوية
✓	بساطة عمليات المعالجة
✓	عدم الحاجة لتدخل كيان ثالث من أجل توليد المفاتيح وتبادلها
✓	حجم البيانات المتبادلة مقبول
✓	زمن مقبول لإتمام عملية توليد المفاتيح
✓	التسامح مع ضعف التزامن
✓	FAR يساوي الصفر
✓	ديناميكية المفتاح (أي المفتاح متغير مع الزمن)
✓	العمل وفق تقنية Plug-and-Play
✓	ضمان أمان شبكة WBAN في أثناء إقلاعها

ب. الحداثة والمساهمة بالنسبة لمخطط مولّد السلاسل العشوائية بالاعتماد على إشارة ECG

فيما يتعلق بتوليد القيم العشوائية اعتباراً من إشارة ECG، يُنشئ المولّد المطوّر سلاسل ثنائية عشوائية يمكن استخدامها لأغراض التعمية في WBAN ذات الموارد المحدودة للغاية. استطعنا إيجاد مولّد سلاسل عشوائية عالي الإنتاجية مُعتمد على ECG ومناسب لتطبيقات الرعاية الصحية في الزمن الحقيقي. تكمن مساهمتنا في هذا المجال فيما يأتي:

- يتمّتع المولّد المطوّر بإنتاجية عالية جداً تتراوح من 2048 إلى 5760 بتاً في الثانية وفقاً لمعدل أخذ عينات ECG. في حين أن إنتاجية مولّدات الأرقام العشوائية المُعتمدة على ECG والمُقدّحة في الدراسات السابقة، لا تتجاوز 306 بتاً في الثانية.

- يجمع المولّد المطوّر بين بساطة العمليات ومعدل الإنتاج المرتفع، فهو يولّد RBSs باستخدام عمليّات بسيطة جداً (الجمع والطرح والضرب وباقي القسمة)، ولا يحتاج إلى عمليّات ترميز أو تحويلات مويجية أو توابع البصمة أو غيرها؛ مما يجعله مناسباً للتطبيق في حساسات WBAN. تتميز الطرق البسيطة في الدراسات السابقة بإنتاجية منخفضة جداً. وتستخدم الطريقة المقترحة في [25]، والتي تتمتع بإنتاجية أعلى من الدراسات السابقة الأخرى، التحليل المويجي الذي يحتاج إلى عمليات معقدة غير مناسبة للتطبيق في حساسات WBAN.

- أثبتت عشوائية RBSs الناتجة عن المولّد المطوّر وتميّزها، وذلك من أجل السلاسل التي تتراوح أطوالها بين 128 bit و 2048 bit، وأُثبت أنه يمكن استخدامها لأغراض التعمية (على سبيل المثال، مفاتيح التعمية). في الدراسات سابقة، أثبت الباحثون عشوائية وتميّز سلاسل أطوالها 128 bit أو أقصر، علماً أن هناك عدداً من خوارزميات التعمية التي تستخدم قيماً عشوائية (مفاتيح) أطول من 128 bit (تتراوح من 128 bit إلى 2048 bit).

- أُثبِتَ أن الخصم لا يمكنه كشف إشارة ECG اعتماداً على RBSs الناتجة عن المولد المطوّر، ولكن لم تُثبِت هذه الميزة في الدراسات السابقة.

- على عكس مولّدات الأرقام العشوائية الأخرى، يولّد المولد المطوّر عدداً كبيراً من RBSs في وقتٍ محدود. غالباً ما يكون لمولّدات الأرقام العشوائية إنتاجية منخفضة نتيجة لاعتمادها على الظواهر الطبيعية، لذلك فإنها عادةً ما تولّد سلاسل عشوائية قصيرة خلال فترة زمنية طويلة نسبياً. تُستخدَم مولّدات الأرقام شبه العشوائية عند الحاجة إلى توليد العديد من السلاسل العشوائية في وقتٍ قصير. على الرغم من أن المولد المطوّر يصنّف تحت مولّدات الأرقام العشوائية، إلا أنه يتغلّب على الإنتاجية المنخفضة لذلك الصنف.

ت. الحداثة والمساهمة بالنسبة لخوارزمية TEA المحسّنة

بما يتعلق بخوارزمية التعمية المطوّرة في هذه الدراسة، تم تحسين خوارزمية TEA للحصول على خوارزمية تعمية خاصّة بشبكات WBAN، تراعي محدوديّة الموارد وسرعة معالجة البيانات المطلوبة في تطبيقات العناية بالصحة في الزمن الحقيقي. أدى اختيار خوارزمية TEA وتحسينها بطريقة تسمح باستخدام قيم إزاحة مختلفة في كل دورة إلى زيادة أمان TEA وبالتالي قابلية استخدامها لحماية WBAN. تغلّبت TEA المحسّنة على كافة الهجمات التي تعاني منها TEA التقليدية. إضافةً إلى ذلك، أُثبِتَ أن التعديل الذي قمنا به جعل أمانها يعادل التعمية بمفتاح طوله 208 bit بدلاً من 128 bit. كما أدى هذا التعديل إلى رفع الأداء من خلال الاكتفاء بتنفيذ 16 جولة فقط من TEA المحسّنة. إن TEA المحسّنة تُستخدَم عمليات حسابية أبسط من جميع الخوارزميات في الدراسات السابقة. كما أُثبِتَت التجارب أن TEA المحسّنة أسرع بست عشرة مرة من AES المستخدمة في معيار IEEE 802.15.6 على أقل تقدير. يمكننا القول إننا تمكّنّا من التوصل إلى خوارزمية تعمية سريعة جداً ومناسبة للاستخدام في شبكات WBAN، وهي ذات أداء أعلى واستهلاك موارد أقل من الخوارزميات السابقة، وتحقق الأمان المطلوب لحماية البيانات الطبية.

7-6- مقارنة بين المخططات المطوّرة وأساليب الحماية في تقانات الاتصال في WBAN

بالعودة إلى الفصل الأول من الأطروحة، حيث تم شرح التقانات المُستخدمة في WBAN وأساليب الحماية فيها، نُقارن بين نظام الحماية المطوّر في بحثنا وأساليب الحماية المتّبعة في تلك التقانات.

بالنسبة لعملية تبادل المفاتيح، نلحظ في BLE الحاجة لوجود طرف ثالث لإتمام العملية، بالإضافة إلى الحاجة إلى مفاتيح قصيرة الأمد من أجل تنفيذ عملية تبادل مفاتيح طويلة الأمد. وفي مستوى الأمان الرابع يتم تبادل المفاتيح وفق خوارزمية ECDH غير المتناظرة. أما في IEEE 802.15.4 و Zigbee فتحتاج عملية تبادل المفاتيح إلى التثبيت المسبق للمفاتيح الرئيسة MK، كما أنها تحتاج لعقدة ثابتة موثوقة مسؤولة عن عملية تبادل مفتاح الشبكة. وفي معيار IEEE 802.15.6 يتم تبادل المفاتيح وفق طريقة Diffie-Hellman التي تستخدم مبادئ التعمية غير المتناظرة. أما في مخطط تبادل المفاتيح المطوّر في دراستنا هذه، ECG-AKES، يتم تبادل المفاتيح بالاعتماد على القيم الحيوية وعلى عمليات بسيطة، دون الحاجة إلى استخدام خوارزميات التعمية غير المتناظرة أو الاعتماد على طرف موثوق يقوم بإدارة عملية التبادل والإشراف عليها. كما أن المخطط المطوّر لا يحتاج إلى التثبيت المسبق للمفاتيح في حساسات WBAN وبالتالي يتوافق مع العمل وفق نمط التوصيل والتشغيل. وعليه فإن مخطط ECG-AKES يتفوّق على طرق تبادل المفاتيح المستخدمة في تقانات الاتصال بين حساسات WBAN.

في أساليب الحماية المتبعة في تقانات الاتصال في WBAN، تُولّد القيم العشوائية كمفاتيح التعمية وغيرها باستخدام مولّدات الأرقام العشوائية التقليدية، دون الاعتماد على القيم الحيوية، مما يجعل تلك العمليات مكلفة ومُستهلكة لطاقة الحساسات.

أما بالنسبة لعملية التعمية، وكما بيّنا سابقاً، فإن جميع التقانات المدروسة تستخدم خوارزمية AES في عمليات التعمية وذلك وفق أنماط عدّة مثل: CCM، وCTR، وCBC. ولكن كما برهنا سابقاً، فإن خوارزمية TEA المُحسّنة أسرع بكثير من خوارزمية AES وأبسط منها بكثير، وهي آمنة أيضاً، مما يجعلها أفضل من AES المستخدمة في التقانات المدروسة.

7-7- خاتمة

في هذا الفصل من الأطروحة، قارنًا المخططات المطوّرة في هذا البحث مع الدراسات السابقة. وتبيّن من المقارنة أن مخطط ECG-AKES يَحَقِّق جميع المتطلبات اللازمة، كما أنه يتفوق على الدراسات السابقة في نقاط عدّة تتفاوت بحسب الدراسة. كما استنتجنا أن مولّد السلاسل العشوائية المطوّر ذو أداء أعلى بكثير من مولّدات السلاسل العشوائية المُعتمَدة على ECG والمطوّرة في الدراسات السابقة. وعلى خلاف الدراسات السابقة، أثبتنا العشوائية والتميُّز من أجل السلاسل التي تتراوح أطوالها من 128 bit إلى 2048 bit. أما خوارزمية TEA المُحسّنة فقد أثبتنا أنها آمنة وأن أداءها أعلى بحوالي ست عشر مرة من أداء خوارزمية AES المُستخدَمة في حماية شبكات WBAN.

الخاتمة

في هذه الأطروحة، ونظراً لأهمية حماية البيانات الصحية في أنظمة التطبيق عن بُعد، درسنا طرائق حماية تلك البيانات وبالتحديد في شبكة WBAN. تجلّت مشكلة البحث التي سعينا نحو إيجاد حلول لها في عدم قابلية تطبيق آليات الحماية التقليدية في حساسات WBAN، نظراً لمحدودية طاقتها وقدرتها على المعالجة، ونظراً لتعقيد تلك الآليات. درسنا العديد من الأبحاث السابقة التي تسعى لحل مشكلة البحث، وبالتحديد تلك الدراسات التي اعتمدت على إشارة ECG في توليد مفاتيح التعمية السريّة وتبادلها، وفي توليد السلاسل العشوائية. ولكن أثبتنا عدم كفاية الطرائق المطروحة، وأن إيجاد خوارزميات تعمية، ومخططات تبادل مفاتيح، ومولّدات سلاسل عشوائية تتناسب مع متطلبات ومحدودية WBAN هو أمر لا يزال قيد البحث. وبالتالي انقسمت دراستنا إلى ثلاثة أقسام رئيسية: القسم الأول، تطوير وتصميم مخطط جديد لتوليد وتبادل المفاتيح السريّة المصادق عليها بالاعتماد على إشارة ECG. القسم الثاني، تطوير وتصميم مولّد سلاسل عشوائية ذو معدل إنتاج عالٍ مُعتمد على إشارة ECG. القسم الثالث، تحسين خوارزمية TEA أيضاً بالاعتماد على إشارة ECG.

تمكّنّا في دراستنا من التوصل إلى مخطط جديد لتبادل المفاتيح السريّة المصادق عليها بالاعتماد على خصائص إشارة ECG في كلّ من المجال الزمني والمجال الترددي. يفي هذا المخطط (ECG-AKES) بجميع المواصفات المطلوبة للعمل على النحو الأمثل ضمن شبكة WBAN، كما أنه يَسْتخدِم عمليات معالجة بسيطة، وهو قادر على إنشاء مفاتيح سريّة متغيرة مع الزمن. يعمل ECG-AKES من خلال طريقة التوصيل والتشغيل، ويضمن أمان WBAN في الفترة الأولى لتشغيل الشبكة. لقد أثبتنا أن المخطط المطوّر مقاوم لضعف التزامن والاختلاف الطفيف في الإشارة المقاسة بوساطة حساسات مختلفة موضوعة على الجسم نفسه. باختصار، يضمن ECG-AKES جودة وأمن وكفاءة عمليّة تبادل المفاتيح، ويتغلب على العديد من سلبيات الدراسات السابقة.

توصّلنا أيضاً من خلال دراستنا إلى مولّد سلاسل عشوائية جديد مُعتمد على القياسات الحيوية، يَسْتخدِم قيم عينات إشارة ECG بدلاً من قيم IPI لتوليد السلاسل العشوائية، يَتَمَنع بمعدّل إنتاج عالٍ أفضل من معدل إنتاج

الدراسات السابقة بعشرات أو مئات المرات، ويؤدّ سلاسل بأطوال مختلفة مناسبة لتطبيقات أمن المعلومات. فضلاً عن ذلك، لا يحتاج المودّ المطوّر إلى عمليات الترميز أو التحويل الموجي أو توابع البصمة أو غيرها من العمليات التي قد تستهلك طاقة الحساسات، ويتميّز ببساطة العمليات مما يؤدي إلى انخفاض استهلاك الطاقة. كما يتمتّع بميزة أخرى مهمة، ألا وهي عدم قدرة الخصم على التنبؤ بالقيم العشوائية المولّدة من بيانات شخص ما، باستخدام بيانات شخص آخر. وهو منيع ضدّ التنصّت، فلقد أظهر بعض الباحثين كيفية التنصّت على قيم IPI باستخدام الكاميرا، ولكن، هذا النهج من التنصّت غير مجدي مع المودّ المطوّر في هذا البحث، حيث استُخدِمَت قيم عينات إشارة ECG، ولا توجد طريقة لالتقاطها من مسافة بعيدة. لقد تبيّن أيضاً أن الخصم لا يمكنه كشف إشارة ECG اعتماداً على السلاسل الناتجة. وللتحقّق من عشوائية السلاسل الناتجة، لم يتم اختبارها من أجل بيانات أشخاص أصحاء فحسب، وإنما تم اختبارها أيضاً باستخدام بيانات أشخاص يعانون من عدم انتظام ضربات القلب؛ للتحقق تجريبياً من عشوائية السلاسل الناتجة. لقد أثبتت التجارب أن السلاسل ذات الأطوال المختلفة الناتجة عن المخطط المقترح عشوائية بما يكفي لاستخدامها في أغراض التعمية وحماية المعلومات.

في دراستنا هذه، قمنا أيضاً بتحسين خوارزمية TEA للحصول على خوارزمية تعمية خاصة بشبكات WBAN تراعي محدودية الموارد وسرعة معالجة البيانات المطلوبة في تطبيقات العناية بالصحة في الزمن الحقيقي. كان لتعديل TEA وجعل الإزاحة متغيّرة من أجل كل دورة تنفيذ وفق قيم مستنتجة من القيم الحيويّة المقاسة الأثر الأكبر في زيادة أمانها، وبالتالي قابلية استخدامها لحماية WBAN. إضافةً إلى ذلك، أثبتنا أن التعديل الذي قمنا به جعل أمانها يعادل التعمية بمفتاح طوله 208 bit بدلاً من 128 bit. كما أدى هذا التعديل إلى رفع الأداء من خلال الاكتفاء بتنفيذ 16 جولة فقط من TEA المُحسّنة. إن TEA المُحسّنة ذات عمليات حسابية أبسط من جميع الخوارزميات في الدراسات السابقة. كما أثبتت التجارب أن TEA المُحسّنة أسرع بست عشرة مرة من AES المستخدمة في معيار IEEE 802.15.6 على أقل تقدير. يمكننا القول إننا تمكّنّا من التوصل إلى خوارزمية تعمية سريعة جداً، ومناسبة للاستخدام في شبكات WBAN، ذات أداء أعلى، واستهلاك موارد أقل من الخوارزميات السابقة التي استُخدِمَت وطوّرت لحماية شبكات WBAN، وتُحقّق الأمان المطلوب لحماية البيانات الطبية.

في الختام، وبعد أن بيّنا أهمية المخططات المطوّرة في هذا البحث، وقدرتها على حل المشاكل التي تعاني منها طرائق حماية شبكات WBAN، نوصي بتطبيق تلك المخططات بشكلٍ فعليّ في أنظمة التطبيب عن بعد المعتمدة على شبكات WBAN؛ من أجل حماية المعلومات الطبيّة المُتبادلة عبرها. ونقترح أيضاً الاستفادة من القيم المشتركة بين الحساسات التي يُمكن توليدها باستخدام مخطّط ECG-AKES من أجل توليد مفاتيح تسمية لخوارزميات أخرى إلى جانب خوارزمية TEA المحسّنة، مثل خوارزمية AES، أو DES، أو أيّ خوارزمية تسمية متناظرة. كما نوصي بتطبيق مولّد السلاسل العشوائية المطوّر في هذا البحث، ليس ضمن حساسات WBAN فحسب، وإنما أيضاً لتوليد السلاسل العشوائية في أي جهاز إلكتروني قادر على قياس إشارة ECG والاستفادة منها، مثل الساعة الرقمية وغيرها؛ مما يوفر من عمليات المعالجة اللازمة لتطبيق مولدات الأرقام العشوائية التقليدية في تلك الأجهزة. ونوصي أيضاً بمتابعة البحث لتعزيز نتائجه من حيث أمان الخوارزميات المطوّرة، وذلك من خلال محاولة إيجاد الثغرات الأمنية فيها بهدف سد تلك الثغرات إن وجدت. كما نوصي بمتابعة البحث لتغطية جميع متطلبات حماية المعلومات في أنظمة التطبيب عن بعد المعتمدة على WBAN، في جميع طبقات تلك الأنظمة، وذلك بالاعتماد على المخططات المطوّرة في هذا البحث.

قائمة المراجع

- [1] H. Wang, M. S. Mahmud, H. Fang and C. Wang, *Wireless Health*, Berlin, Germany: Springer, 2016.
- [2] A. Rangarajan, "Emerging trends in healthcare adoption of wireless body area networks," *Biomedical instrumentation & technology*, vol. 50, no. 4, pp. 264-276, 2016.
- [3] M. A. Simplicio, L. H. Iwaya, B. M. Barros, T. C. Carvalho and M. Naslund, "SecourHealth: a delay-tolerant security framework for mobile health data collection," *IEEE journal of biomedical and health informatics*, vol. 19, no. 2, pp. 761-772, 2014.
- [4] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 113-122, 2017.
- [5] Y. Al-Saeed, E. Eldaydamony, A. Atwan, M. Elmogy and O. Ouda, "Efficient Key Agreement Algorithm for Wireless Body Area Networks Using Reusable ECG-Based Features," *Electronics*, vol. 10, no. 4, p. 404, 2021.
- [6] T. Jabeen, H. Ashraf and A. Ullah, "A survey on healthcare data security in wireless body area networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-14, 2021.
- [7] M. Masdari, S. Ahmadzadeh and M. Bidaki, "Key management in wireless Body Area Network: Challenges and issues," *Journal of Network and Computer Applications*, vol. 91, pp. 36-51, 2017.
- [8] N. Mahmoud, S. El-Sappagh, H. El-Bakry and S. Abdelrazek, "A Real-time Framework for Patient Monitoring Systems based on a Wireless Body Area Network," *Int. J. Comput. Appl*, vol. 176, pp. 12-21, 2020.
- [9] D. P. Tobón, T. H. Falk and M. Maier, "Context awareness in WBANs: a survey on medical and non-medical applications," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 30-37, 2013.
- [10] Z. Guan, T. Yang and X. Du, "Achieving secure and efficient data access control for cloud-integrated body sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, p. 101287, 2015.
- [11] H. A. Maw, H. Xiao and B. Christianson, "An adaptive access control model for medical data in wireless sensor networks," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, IEEE, 2013, pp. 303-309.
- [12] M. Barua, X. Liang, R. Lu and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," in *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2011, pp. 970-975.
- [13] K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60-68, 2009.

- [14] H. Zhao, C. Chen, J. Hu and J. Qin, "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*, vol. 11, no. 8, p. 764919, 2015.
- [15] M. S. Hajar, M. O. Al-Kadri and H. K. Kalutarage, "A survey on wireless body area networks: architecture, security challenges and research opportunities," *Computers & Security*, p. 102211, 2021.
- [16] S. Amini, R. Verhoeven, J. Lukkien and S. Chen, "Toward a security model for a body sensor platform," in *2011 IEEE International Conference on Consumer Electronics (ICCE)*, IEEE, 2011, pp. 143-144.
- [17] W. Stallings, *Cryptography and Network Security Principles and Practice, Fifth Edition* ed, Prentice Hall, 2011.
- [18] S. Hussain and M. Kumar, "Secured Key Agreement Schemes in Wireless Body Area Network—A Review," *Indian Journal of Science and Technology*, vol. 14, no. 24, pp. 2005-2033, 2021.
- [19] S. M. K.-u.-R. Raazi, H. Lee, S. Lee and Y.-K. Lee, "BARI+: a biometric based distributed key management approach for wireless body area networks," *Sensors*, vol. 10, no. 4, pp. 3911-3933, 2010.
- [20] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, pp. 1-16, 2007.
- [21] P. Kumari and T. Anjali, "Symmetric-key generation protocol (SGenP) for body sensor network," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, 2018, pp. 1-6.
- [22] A. Sammoud, O. Hamdi, M. A. Chalouf and A. Bouallegue, "A new protocol for an efficient and green biometric-based security key establishment in WBAN's," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, 2018, pp. 762-767.
- [23] Z. Zhang, H. Wang, A. V. Vasilakos and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 6, pp. 1070-1078, 2012.
- [24] S. Pirbhulal, H. Zhang, W. Wu, S. C. Mukhopadhyay and Y.-T. Zhang, "Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks," *IEEE Transactions on Biomedical Engineering*, vol. 65, no. 12, pp. 2751-2759, 2018.
- [25] C. Camara, P. Peris-Lopez, H. Martin, M. Aldalaien and others, "ECG-RNG: A random number generator based on ECG signals and suitable for securing wireless sensor networks," *Sensors*, vol. 18, no. 9, p. 2747, 2018.
- [26] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, J. Zhou, L. Qiao and K. Saleem, "Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks," *IEEE journal of biomedical and health informatics*, vol. 21, no. 3, pp. 655-663, 2016.

- [27] G.-H. Zhang, C. C. Poon and Y.-T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 1, pp. 176-182, 2011.
- [28] M. S. A. Malik, M. Ahmed, T. Abdullah, N. Kousar, M. N. Shumaila and M. Awais, "Wireless body area network security and privacy issue in e-healthcare," *Int. J. Adv. Comput. Sci. Appl*, vol. 9, no. 4, pp. 209-215, 2018.
- [29] S. R. Moosavi, E. Nigussie, S. Virtanen and J. Isoaho, "Cryptographic key generation using ECG signal," in *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, 2017, pp. 1024--1031.
- [30] L. E. Bassham III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks and others, "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards & Technology, 2010.
- [31] G. Lo Re, F. Milazzo and M. Ortolani, "Secure random number generation in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 15, pp. 3842-3862, 2015.
- [32] F. Xu, Z. Qin, C. C. Tan, B. Wang and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *2011 Proceedings IEEE INFOCOM*, IEEE, 2011, pp. 1862-1870.
- [33] G. Chen, "Are electroencephalogram (EEG) signals pseudo-random number generators?," *Journal of Computational and Applied Mathematics*, vol. 268, pp. 1-4, 2014.
- [34] D. Nguyen, D. Tran, W. Ma and K. Nguyen, "EEG-Based random number generators," in *International Conference on Network and System Security*, Springer, 2017, pp. 248-256.
- [35] T. Linciya and K. Anandkumar, "Enhanced three tier security architecture for WSN against mobile sink replication attacks using mutual authentication scheme," *International Journal of Wireless & Mobile Networks*, vol. 5, no. 2, p. 81, 2013.
- [36] T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band and A. Mosavi, "A lightweight genetic based algorithm for data security in wireless body area networks," *IEEE Access*, vol. 8, pp. 183460-183469, 2020.
- [37] A. Z. Alshamsi and E. S. Barka, "Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks," in *2017 International Conference on Informatics, Health & Technology (ICIHT)*, IEEE, 2017, pp. 1-7.
- [38] R. Nidhya, S. Shanthi and M. Kumar, "A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm," in *Intelligent System Design*, Springer, 2021, pp. 255-263.
- [39] J. Wang, Z. Zhang, K. Xu, Y. Yin and P. Guo, "A research on security and privacy issues for patient related data in medical organization system," *International Journal of Security and Its Applications*, vol. 7, no. 4, pp. 287-298, 2013.

- [40] J. P. Singh and N. Bilandi, "Analysis of biometric-based security in wireless body area network (WBAN)," in *Proceedings of the International Conference on Information Technology and Computer Science, Liverpool, UK*, 2019, pp. 26-28.
- [41] S. Peter, B. Pratap Reddy, F. Momtaz and T. Givargis, "Design of secure ECG-based biometric authentication in body area sensor networks," *Sensors*, vol. 16, no. 4, p. 570, 2016.
- [42] MIT-BIH, "MIT-BIH arrhythmia database," [Online]. Available: <http://physionet.org/physiobank/database/mitdb/>. [Accessed 2021].
- [43] MIT-BIH, "MIT-BIH Normal Sinus Rhythm Database," [Online]. Available: <https://physionet.org/content/nsrdb/1.0.0/>. [Accessed 2021].
- [44] MIT-BIH, "MIT-BIH Long-Term ECG Database," [Online]. Available: <https://physionet.org/content/ltadb/1.0.0/>.
- [45] R. Negra, I. Jemili and A. Belghith, "Wireless body area networks: Applications and technologies," *Procedia Computer Science*, vol. 83, pp. 1274-1281, 2016.
- [46] K. Yazdandoost and K. Sayrafian, "Channel model for body area network (BAN). IEEE p802. 15-08-0780-09-0006," IEEE 802.15 Working Group Document, 2009.
- [47] A. Fragopoulos, J. Gialelis and D. Serpanos, "Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures," in *The 12th IEEE International Conference on e-Health Networking, Applications and Services*, IEEE, 2010, pp. 127--134.
- [48] D. M. Barakah and M. Ammad-uddin, "A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture," in *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, IEEE, 2012, pp. 214-219.
- [49] X. H. Le, M. Khalid, R. Sankar and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *Journal of Networks*, vol. 6, no. 3, pp. 355-364, 2011.
- [50] A. Rasheed and R. N. Mahapatra, "The three-tier security scheme in wireless sensor networks with mobile sinks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 5, pp. 958-965, 2010.
- [51] M. Usman, M. R. Asghar, I. S. Ansari and M. Qaraqe, "Security in wireless body area networks: From in-body to off-body communications," *IEEE Access*, vol. 6, pp. 58064-58074, 2018.
- [52] A. R. Ansari and S. Cho, "Human body: The future communication channel for WBAN," in *The 18th IEEE international symposium on consumer electronics (ISCE 2014)*, IEEE, 2014, pp. 1-3.
- [53] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *Journal of Systems Architecture*, vol. 113, p. 101883, 2021.
- [54] M. Conti, *Secure wireless sensor networks*, New York: Springer, 2015.

- [55] A. Boukerche and Y. Ren, "A secure mobile healthcare system using trust-based multicast scheme," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 387-399, 2009.
- [56] D. N. Gupta and R. Kumar, "Lightweight Cryptography: an IoT Perspective," *Trivium*, vol. 80, no. 1, p. 2580, 2019.
- [57] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd and T. Hayajneh, "Security vulnerabilities in Bluetooth technology as used in IoT," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 28, 2018.
- [58] K. Scarfone, "Guide to bluetooth security: Recommendations of the National Institute of Standards and Technology," DIANE Publishing, 2009.
- [59] S. Sevier and A. Tekeoglu, "Analyzing the security of Bluetooth low energy," in *2019 International Conference on Electronics, Information, and Communication (ICEIC)*, IEEE, 2019, pp. 1-5.
- [60] G. Kwon, J. Kim, J. Noh and S. Cho, "Bluetooth low energy security vulnerability and improvement method," in *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, IEEE, 2016, pp. 1-4.
- [61] "MICROCHIP," Microchip Technology, Inc, [Online]. Available: <https://microchipdeveloper.com/wireless:ble-gap-security>. [Accessed 2021].
- [62] X. Fan, F. Susan, W. Long and S. Li, "Security analysis of zigbee," *MWR InfoSecurity*, pp. 1-18, 2017.
- [63] A. Astrin, "IEEE Standard for Local and metropolitan area networks part 15.6: Wireless Body Area Networks," IEEE Std 802.15.6, 2012.
- [64] K. S. Kwak, S. Ullah and N. Ullah, "An overview of IEEE 802.15. 6 standard," in *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, IEEE, 2010, pp. 1-6.
- [65] S. Ullah, M. Mohaisen and M. A. Alnuem, "A review of IEEE 802.15. 6 MAC, PHY, and security specifications," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, p. 950704, 2013.
- [66] M. Toorani, "Security analysis of the IEEE 802.15. 6 standard," *International Journal of Communication Systems*, vol. 29, no. 17, pp. 2471-2489, 2016.
- [67] F. Hu, M. Jiang, M. Wagner and D.-C. Dong, "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign," *IEEE Transactions on Information Technology in Biomedicine*, vol. 11, no. 6, pp. 619-627, 2007.
- [68] Y.-M. Huang, M.-Y. Hsieh, H.-C. Chao, S.-H. Hung and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE journal on selected areas in communications*, vol. 27, no. 4, pp. 400-411, 2009.

- [69] P. Kumar, Y.-D. Lee and H. Lee, "Secure health monitoring using medical wireless sensor networks," in *The 6th International Conference on Networked Computing and Advanced Information Management*, IEEE, 2010, pp. 491-494.
- [70] Y. S. Lee, E. Alasaarela and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," in *The International Conference on Information Networking 2014 (ICOIN2014)*, IEEE, 2014, pp. 453-457.
- [71] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "Sage: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE journal on selected areas in communications*, vol. 27, no. 4, pp. 365-378, 2009.
- [72] M. M. Haque, A.-S. K. Pathan and C. S. Hong, "Securing U-healthcare sensor networks using public key based scheme," in *Haque, Md Mokammel and Pathan, Al-Sakib Khan and Hong, Choong Seon*, vol. 2, IEEE, 2008, pp. 1108-1111.
- [73] M. Marković, Z. Savić and B. Kovačević, "Secure mobile health systems: Principles and solutions," in *M-Health*, Springer, 2006, pp. 81-106.
- [74] V. Anusuya Devi and V. Kalaivani, "Hybrid cryptosystem in wireless body area networks using message authentication code and modified and enhanced lattice-based cryptography (MAC-MELBC) in healthcare applications," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 9, p. e6132, 2021.
- [75] T. Falck, H. Baldus, J. Espina and K. Klabunde, "Plug 'n play simplicity for wireless medical body sensors," *Mobile Networks and Applications*, vol. 12, no. 2, pp. 143-153, 2007.
- [76] A. Rashkovska, M. Depolli, I. Tomašić, V. Avbelj and R. Trobec, Medical-grade ECG sensor for long-term monitoring, vol. 20, Multidisciplinary Digital Publishing Institute, 2020, p. 1695.
- [77] F. Sufi, I. Khalil and J. Hu, "ECG-based authentication," in *Sufi, Fahim and Khalil, Ibrahim and Hu, Jiankun*, Berlin, Heidelberg, Springer, 2010, pp. 309-331.
- [78] S. Sanei, D. Jarchi and A. G. Constantinides, Body sensor networking, design and algorithms, John Wiley & Sons, 2020.
- [79] "Acquisition and Analysis of an ECG (electrocardiography) Signal," *JoVE Science Education Database. Biomedical Engineering.*, vol. MA, 2022.
- [80] A. Abdou and S. Krishnan, "Horizons in Single-Lead ECG Analysis From Devices to Data," *Frontiers in Signal Processing*, p. 27, 2022.
- [81] R. Pan, D. Chua, J. S. Pathmasuntharam and Y. P. Xu, "A WBAN based cableless ECG acquisition system," in *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, IEEE, 2014, pp. 910-913.
- [82] S. Bruce, Applied cryptography: protocols, algorithms, and source code in C, Wiley, 1996.
- [83] S. J. Shepherd, "The tiny encryption algorithm," *Cryptologia*, vol. 31, no. 3, pp. 233-245, 2007.

- [84] M. Ebrahim, S. Khan and U. B. Khalid, "Symmetric algorithm survey: a comparative analysis," *arXiv preprint arXiv:1405.0398*, 2014.
- [85] S. Rajesh, V. Paul, V. G. Menon and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019.
- [86] J. Tian and X. Gao, "A Bitsum Attack research based on TEA," in *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, IEEE, 2016, pp. 1721-1724.
- [87] S. Hong, D. Hong, Y. Ko, D. Chang, W. Lee and S. Lee, "Differential Cryptanalysis of TEA and XTEA," in *International Conference on Information Security and Cryptology*, Springer, 2003, pp. 402-417.
- [88] S. A. Klyokta, N. I. Chesnokov, I. A. Pilipenko, A. I. Zhukov, L. V. Cherckesova, O. A. Safaryan, A. G. Lobodenko and V. M. Porksheyen, "Development of Modified Block Cipher Algorithm TEA, Free from Vulnerability of "Connected Keys Attack"," in *2019 IEEE East-West Design & Test Symposium (EWDTS)*, IEEE, 2019, pp. 1-6.
- [89] C. D. de Saint Guilhem, M. Fischlin and B. Warinschi, "Authentication in key-exchange: Definitions, relations and composition," in *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, IEEE, 2020, pp. 288-303.
- [90] J. Walker, "ENT A Pseudorandom Number Sequence Test Program," 18 January 2008. [Online]. Available: <https://www.fourmilab.ch/random/>. [Accessed 2021].
- [91] C. Camara, H. Martin, P. Peris-Lopez and M. Aldalaien, "Design and analysis of a true random number generator based on GSR signals for body sensor networks," *Sensors*, vol. 19, no. 9, p. 2033, 2019.
- [92] R. G. Brown, D. Eddelbuettel and D. Bauer, "Dieharder: A Random Number Test Suite," [Online]. Available: <https://webhome.phy.duke.edu/~rgb/General/dieharder.php>. [Accessed 2021].
- [93] M. Mana, M. Feham and B. A. Bensaber, "Trust key management scheme for wireless body area networks," *Int. J. Netw. Secur.*, vol. 12, no. 2, pp. 75-83, 2011.
- [94] W. Tang, K. Zhang, J. Ren, Y. Zhang and X. Shen, "Flexible and efficient authenticated key agreement scheme for BANs based on physiological features," *IEEE Transactions on Mobile Computing*, vol. 18, no. 4, pp. 845-856, 2018.
- [95] A. Ali and F. A. Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1-19, 2013.
- [96] N. Karimian, Z. Guo, M. Tehranipoor and D. Forte, "Highly reliable key generation from electrocardiogram (ECG)," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 6, pp. 1400-1411, 2016.

- [97] A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237-257, 2006.
- [98] S. Farooq, D. Prashar and K. Jyoti, "Hybrid encryption algorithm in wireless body area networks (WBAN)," in *Intelligent communication, control and devices*, Springer, 2018, pp. 401-410.
- [99] I. Choi and J.-H. Kim, "Area-Optimized Multi-Standard AES-CCM Security Engine for IEEE 802.15.4/802.15.6," *JSTS: Journal of Semiconductor Technology and Science*, vol. 16, no. 3, pp. 293-299, 2016.
- [100] Ö. Hasan Yavuz, E. Hakan, K. Temel and Y. I. K. Ali Özgür, "Wireless body area network studies for telemedicine applications using IEEE 802.15.6 standard," in *CMBEBIH 2017*, Springer, 2017, pp. 666-670.
- [101] R. H. Morelos-Zaragoza, *The art of error correcting coding*, John Wiley & Sons, 2006.
- [102] X. Lu, M. Pan and Y. Yu, "QRS detection based on improved adaptive threshold," *Journal of healthcare engineering*, vol. 2018, 2018.
- [103] F. R. R. C. S. t.-D. E. M. Răstoceanu, "Sensor-based entropy source analysis and validation for use in IoT environments," *Electronics*, vol. 10, no. 10, p. 1173, 2021.
- [104] J. Gärtner, *Analysis of Entropy Usage in Random Number Generators*, 2017.

Abstract

Telemedicine systems, also called electronic health care systems (E-healthcare systems), are systems that monitor the patient's health status at anytime and anywhere, without restricting his motion and his daily activities. In these systems, Wireless Body Area Networks (WBANs) are used, which are a group of wirelessly connected medical sensors designed to collect and transmit various biometrics of the human body. Maintaining the security of health information in these systems is critical due to the negative effects of security attacks that threaten the patient's life. However, due to the limited resources of WBAN sensors, traditional security mechanisms cannot be applied, as they consume a lot of energy and resources. To reduce resource consumption, researchers have developed encryption algorithms and authentication mechanisms based on biometrics, most commonly the electrocardiogram (ECG) signal. But their methods suffer from some problems. For ECG-based key generation, the developed methods suffer from time delay, strict synchronization, non-zero False Acceptance Rate (FAR), etc. The same for the generation of random sequences based on ECG, which suffers from low throughput that is unsuitable for the requirements of real-time healthcare. In this thesis, we have developed new schemes to secure WBAN by profiting from the ECG signal. The novelty and contribution of this research can be summarized in three main contributions. **First:** Developing and designing a new model to generate and exchange authenticated secret keys between WBAN sensors based on extracted features of the ECG signal in the time domain and the frequency domain. The developed model overcomes the weaknesses of previous studies. It is also characterized by the simplicity of operations, time-varying key generation, FAR equal to zero, and the tolerance with poor synchronization between sensors. **Second:** Developing and designing a high-throughput random string generator model based on the ECG signal. The developed generator is characterized by the simplicity of operations and is used by the developed key exchange scheme. **Third:** Improving the Tiny Encryption Algorithm (TEA)

based on the ECG signal in a way that increases its performance and makes it secure against attacks on traditional TEA, to be used for encrypting the data exchanged within WBAN. The improved TEA uses the secret values and keys generated by the developed key exchange scheme. The developed models are built and tested, and the security and performance of each one are studied. It was proven that the resulting random strings, whatever their length is between 128 and 2048 bits, are suitable for information security applications, and the throughput of their generation is tens or hundreds of times greater than in previous studies. The key exchange model was also validated, its security was proven, its performance was studied, and it was compared with the models proposed in previous studies. Enhanced TEA has also been demonstrated to be approximately sixteen times faster than the Advanced Encryption Standard AES used in the IEEE 802.15.6 standard for WBANs.

Key Words: Wireless Body Area Network (WBAN), Electrocardiogram (ECG) Signal, Biometric Key, Secret Key Exchange Scheme, Random Bit Strings (RBS), Tiny Encryption Algorithm (TEA).

Syrian Arab Republic

Damascus University

Faculty of Mechanical and Electrical Engineering

Department of Computer and Automation Engineering



Developing Algorithms to Protect Information Acquired via Wireless Body Area Networks in Telemedicine Systems

**A dissertation submitted in fulfillment of the
requirements for the degree of Ph.D. in
Computer and Networks Engineering**

By

Eng. Christine Youssef Zenieh

Supervisors

Dr. Eng. Mohamed Mazen Al-Mahairi

Dr. Eng. Moufid Haddad

2022