Effective Security Schemes for Wireless Implantable Medical Devices

A Thesis

Presented in Partial Fulfilment of the Requirements for the

Degree of Master of Science

with a

Major in Electrical and Computer Engineering

in the

College of Graduate Studies

University of Idaho

by

Taha Belkhouja

Major Professor: Sameh Sorour, Ph.D.

Committee Members: Mohamed Hefeida, Ph.D.; Yacine Chakhchoukh, Ph.D.

Department Administrator: Joseph Law, Ph.D., P.E.

May 2019

Authorization to Submit Thesis

This thesis of Taha Belkhouja, submitted for the degree of Master of Science with a major in Electrical and Computer Engineering and titled "Effective Security Schemes for Wireless Implantable Medical Devices," has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____Date_____
Sameh Sorour, Ph.D.

Committee Members: _____Date_____
Mohamed Hefeida, Ph.D.

_____Date_____
Yacine Chakhchoukh, Ph.D.

Department Administrator: _____Date_____
Joseph Law, Ph.D., P.E.

Abstract

Healthcare remote devices are recognized as a promising technology for treating health related issues. Among them are the wireless Implantable Medical Devices (IMDs): These electronic devices are manufactured to treat, monitor, support or replace defected vital organs while being implanted in the human body. Thus, they play a critical role in healing and even saving lives. Current IMDs research trends concentrate on their medical reliability. However, deploying wireless technology in such applications without considering security measures may offer adversaries an easy way to compromise them. Many malicious attacks on these devices can directly affect the patient's health in a lethal way. Using insecure wireless channels for these devices offers adversaries easy ways to steal the patient's private data and hijack these systems. On the other hand, IMDs suffer from limited resources, such as the energy supply, processing power, and storage space. This renders security schemes a critical feature for implementation. A certain balance between security and efficiency must be attained in each IMD for a satisfactory and safe functioning.

Therefore, we intend throughout our work to design effective security schemes to defend these IMDs. Our goal is to create or accommodate security approaches for the specific case of any IMD. We want to ensure for any IMD-user a high efficiency from the IMD to improve his health, while guaranteeing a safe use.

Our plans are to decrease the computational complexity of security algorithms and authentication protocols to fit on any IMD. We also want to explore biometric features for better and safer use. We investigate all the possible scenarios (regular or urgent) to guarantee for the patient a reliable device.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my major professor, Dr. Sameh Sorour for continuous support to achieve this work. His guidance helped me in all the time of research and writing of this thesis. I would like also to thank Dr. Mohamed Hefeida for his encouragements, insightful comments, and support.

I owe my profound gratitude wholeheartedly to both of them as professors and mentors for their expertise sharing and valuable guidance throughout my curriculum.

A deep appreciation goes also to Dr. Yacine Chakhcoukh for his encouragement and insightful comments.

This work was mostly achieved under the supervision of Dr. Mohsen Guizani, until he had to leave the university. Therefore, I want to thank him for the achievement of most of this work. I also want to thank him for this opportunity to gain various valuable experiences on both personal and professional levels.

Most of this work has been funded by the NPRP grant 8-408-2-172 from the Qatar National Research Fund (a member of Qatar Foundation). I also would like to acknowledge the University of Idaho, Moscow Campus, for its support to achieve the rest of the work.

Last but not least, special thanks to my wife, Syrine, my ex-labmate Elyes Balti, and my friend Amani Ben Hadj Hassan for the constant support and help to achieve this work. Other distinctive thanks to my family for all their contribution to reaching where I am today. Words will run out before I can express truly my gratitude towards them.

Dedication

In the Name of God Almighty, Most Gracious,Most Merciful, I dedicate this work to

My parents, who have supported me all along my path in life, for their love and affection for me,

My wife, for the unlimited affection and support that led me to achieve this work, for being there every day, every night, enlightening my life,

My brothers, sister and their spouses, who were always there for me, who supported me and never let me in need ,

My nephews and nieces, for letting joy a constant into my heart,

My friends, the true ones, that disregarded all the earth and oceans between me and them and held to the vows of our sacred friendship,

All the people I love and respect.

Table of Contents

List of Tables

List of Figures

CHAPTER 1

Introduction

1.1 General Introduction

Implantable and Wearable Medical Devices (IMD & WMD) are currently the new trending technologies in personal healthcare systems. They enable efficient diagnostics and easy monitoring of the patient's health status in real-time and provide more efficient and scalable healthcare by avoiding frequent visits to the healthcare provider. These devices such as cardiovascular medical devices, neurological implants and infusion function medical devices can help control a broad range of body dysfunctions, like diabetes, cardiac arrhythmia, and epilepsy.

Information security is a serious challenge to all of such devices nowadays [25]. Medical devices' security, particularly for IMDs, is of paramount importance because attacks can be fatal. They do not only steal the private medical data, but they can also affect data integrity and control. IMDs are evolving to provide patients with maximum medical efficiency and safety. The device's security and the medical records' privacy are still under development. In fact, IMDs' architectures usually have limited resources, such as the energy supply, processing power, and storage space. These may require the need of surgeries to overcome some of the limitations. For instance, if we need to resort to surgery in order to change batteries, we have to choose long-life battery types to avoid frequent surgeries. All of these disadvantages render traditional security procedures arduous to implement. Balancing security and confidentiality with the efficiency of the different components is a substantial matter for IMD technologies to advance. For this matter, similar to other systems, IMDs have the following security pillars to protect the patient against attacks:

- *Authentication:* Authentication [27] is one of the most common ways to secure two communicating devices. It ensures that both ends communicate with an authentic and legitimate device, not an impersonator. Authentication in IMDs may be directed in

two possible ways: through a *direct authentication architecture* or through an *indirect authentication architecture*. The indirect scheme introduces a proxy device used to perform authentication protocols, decreasing computation cost and communication overheads in the IMD devices. To identify the device that is requesting a communication, the IMD can use shared keys (temporary or permanent), auxiliary sensors like fingerprint scanners or other biometric signal collectors to identify the unit and to ascertain its authenticity.

- *Cryptography:* Cryptography [28, 29] relies on shared secret keys to cipher the messages within a given communication. This prevents the understanding of the communication by external eavesdropping devices. Also, cryptography secures any system from any hijacking attempts. The adversary who intercepts a message is not able to perform any significant changes like the modification of the serial number in the aim of a spoofing attack. Nevertheless, standard encrypted communications are still vulnerable to Man-In-The-Middle (MITM) or replay attacks.

- *Anomaly Detection:* This technique [30] relies on the observation and the analysis of the received value by the device over time to conclude a pattern. Accordingly, the commands received by the device are estimated to be valid or invalid. For example, in the case of infusion pumps [26], the control device monitors and analyzes the infusion rate in the human body over seven to ten days to learn the time and a dosage pattern. This learning approach helps the device to recognize any malicious abnormal command for injection. Therefore, the patient is secured from receiving lethal injections through the IMD. Fig. 1.1 shows an example of a normal injection rate of an infusion device. In the first sixteen hours, we can pinpoint an injection pattern over an eight-hour period. An adversary hijacks the device and prohibits the device from injection around 6 pm (line in red). The device can detect that this prohibition is quite different from what should be injected from the device (dotted blue line) and the anomaly detection

algorithm will likely disregard this command.

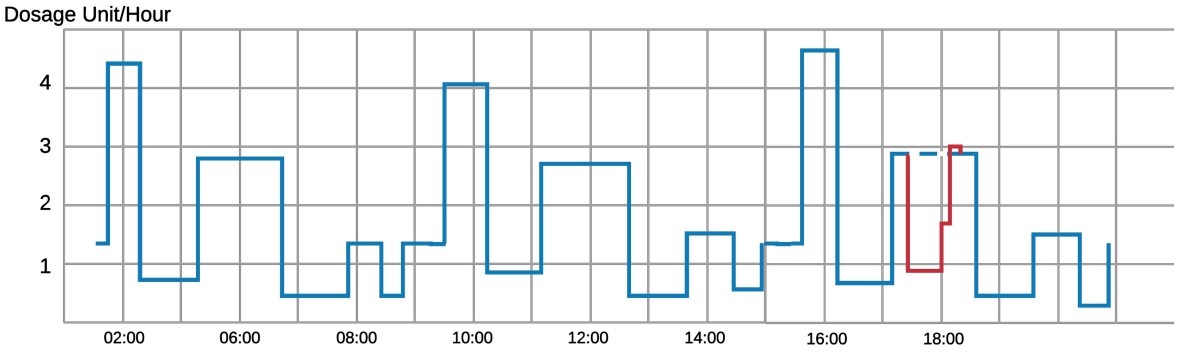


Figure 1.1: Daily Dosage Monitoring of an Infusion Device of a Patient.

- *Jamming:* Jamming attacks can be used to block any incoming packets to the IMD and block its regular work [32]. Moreover, this technique can be used to prevent other types of attacks on the device, mainly resource depletion and denial of service attacks. Attackers can blast the device with incoming messages, that can lead to a drastic drop in the battery level and overflows of memory and storage. In such scenarios, jamming techniques can be launched from the device itself or from an annexed Wearable External Device. If the device senses the existence of these messages, jamming techniques prevent the device from receiving and treating these packets.

1.2 Motivation

Securing wireless medical devices is a challenging task for multiple reasons like the very limited resources in terms of energy supply, processing power, storage space... . As an IMD is embedded inside the patient's body, it usually requires surgery to change its battery. In addition, most medical devices have very limited storage. Others have fewer resources than typical wireless sensor nodes. Hence, security schemes that were designed for sensors are not suitable for most medical devices. Moreover, the existing pre-shared-key-based security schemes are not suitable for these scenarios. Even though it has been widely used for security

in wireless sensor networks, this method does not work well for medical implants. For an IMD, if it has a pre-shared key with a reader/controller, the key may be used to do security operations. However, a pre-shared key will bond a medical device to a particular reader. If the patient (e.g., is out of town and) goes to see a different doctor who does not possess the key, there is no way to authenticate not to communicate. Furthermore, the security schemes for IMD should take into accounts emergency situations. Designing secure mechanisms can, in case of emergencies, prevent the patient from having the needed care. These mechanisms will block all the urgent, unparticular interventions to save patients' lives. Access shall be provided for the needed staff to save the patient while protecting him/her at the same time from unauthorized parties. It has been thought that the best scenario is to design a backdoor to open access during emergency scenarios. But the latter may expose patients information to external unauthorized people. An attacker can exploit this open-door to block doctors' intervention and threaten the patient's survival. Due to the above challenges, traditional crypto-based security schemes may not be applied to many medical devices. Specefic efficient security schemes are needed for IMDs.

CHAPTER 2

Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control

[1] "New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control", *InGLOBECOM 2017-2017 IEEE Global Communications Conference 2017 Dec 4 (pp. 1-5). IEEE.*

2.1 Introduction

In this section, we will focus on the communication link between a wireless implantable medical device and its remote control. We will initially investigate the remote control of the Medtronic Paradigm wireless insulin pump system [5]. The remote control is operated by the patient to send basic instructions to the pump in order to stop/resume basal injection or modify the injection rate by finite steps. This work can therefore be extended to general wireless IMDs with remote controls dedicated to the patient. Halperin *et al.* [6] explained in their work how securing IMD requires a trade-off between security/privacy goals and utility/efficiency. They later analyzed the security regarding Implantable Cardioverter Defibrillator (ICD) [7]. To mitigate security vulnerabilities of these devices, some other research attempts used an external device to deal with security enforcement, without the need of modifying the original device. In this context, Gollakota *et al.* [8] explored the feasibility of protecting implantable devices using a physical layer solution which is a personal base station they called "the shield". Xu *et al.* [9] proposed "IMDGuard", that deals essentially with implantable cardiac devices. As many of the wireless devices communicate in plain text messages, which is an interesting vulnerability for eavesdroppers, Marin *et al.* [10] proposed a solution based on encrypting the communicated packet to protect the data transmitted from the eavesdropper. Li *et al.* [11] treated the problem from another perspective. They introduced a solution based on Body-coupled communication technology. This solution relies

on the fact that the devices' communication range is limited to the close surroundings of the human body. In this case, if an attacker wants to compromise such systems, he/she has to be at a close distance from the victim. Others who have studied security issues of medical devices, they tried using learning techniques like SVM models [13] [14]. These models allow the system to estimate through learning processes the standard range in which the system should operate. This range can be estimated through medical injection dosages or heartbeat rates, for example. These estimations will enable the system to decide whether any control information it receives is valid or not. The patient's mobile device may serve as an external personal system to monitor the IMD and control it with the appropriate applications. They can be linked to ensure monitoring and control with higher performance. Such measure will facilitate the use of the IMD for all the parties involved, but it will display on the other hand another access for attackers to hijack the system. So in related research, they looked for malware detection in Android [16] and mobile [17, 18] systems. Finally, other researchers focused on the creation of secure access schemes that permit any device to be authenticated as a legitimate sender by using direct authentication with fingerprints or iris [19], by using temporary keys for the authentication process generated from ECG signals [20] or many other approaches [22, 23, 24].

The motivation behind this work is to create an authentication scheme that allows the insulin pump to verify the legitimacy of a received message from a remote controller device. This scheme will avoid the use of any encryption or any physical link. Such wireless authentication gains on both energy saving and utility sides. The start point was a protocol used in the communication between the implantable wireless insulin pump and its controller as shown in Fig. 2.1. The work achieved in this section can be generalized for any other wireless implantable medical device using a remote control operated by the patient or any other simple-command device.

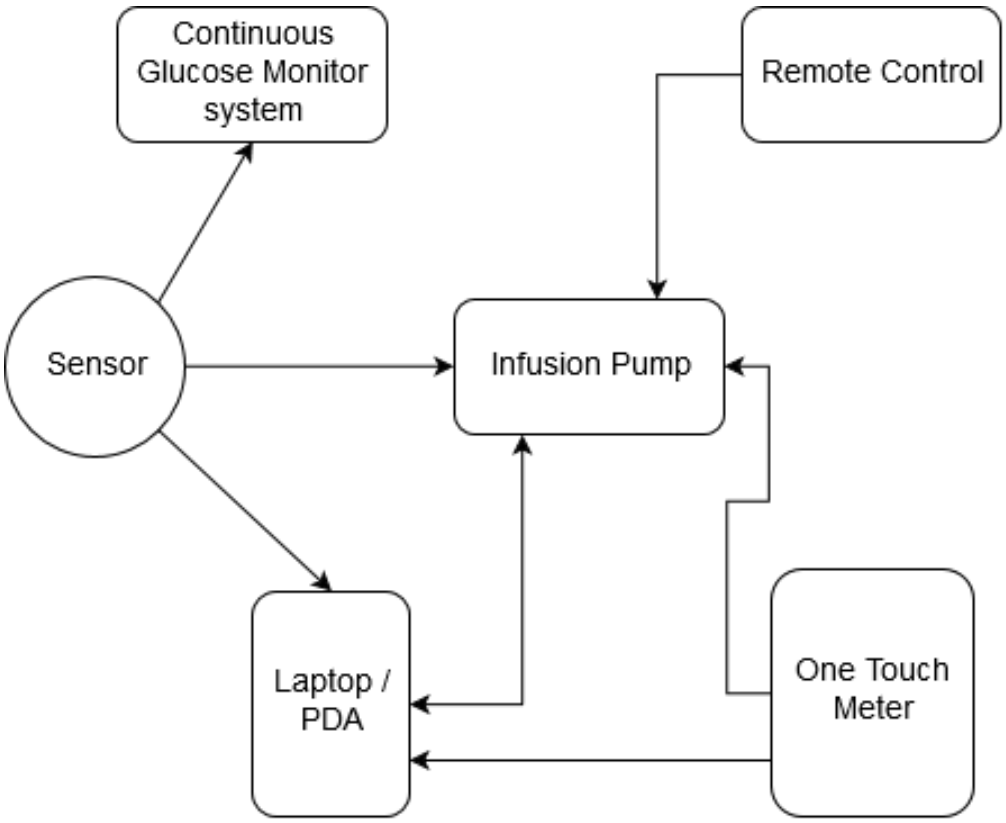
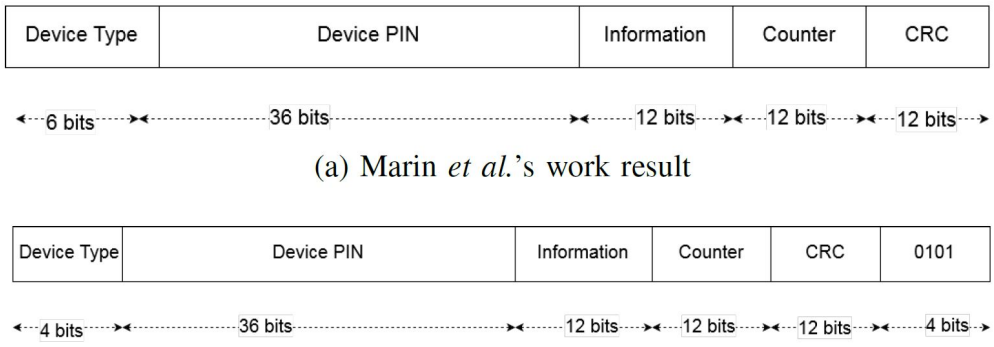


Figure 2.1: Illustration of the Communication Links in the Medtronic Insulin Pump System.

2.2 The Insulin Pump Device

2.2.1 The insulin pump

The Medtronic Insulin Pump is composed of 6 different devices as shown in Fig. 2.1, two of them are attached to the patient's body (Infusion Pump and Sensor). The infusion pump injects the insulin into the patient's circulatory system. The second is the sensor that measures the glucose level in the interstitial fluid of the body. The other devices of the insulin pump system communicate with each other wirelessly as shown in Fig. 2.1: The OneTouch meter measures the blood glucose (BG) through the traditional way from the finger blood. These measures are transmitted to the insulin pump. It also transmits this information to a laptop or PDA that uploads it to a data management server. The latter also uses a two-way communication scheme to gather reports and medical logs from the infusion



(a) Marin *et al.*'s work result

Figure 2.2: Format of the Communication Packet in the Insulin Delivery System according to Marin *et al.* [10] and Li *et al.* [11].

pump. The implanted sensor sends its measures to the infusion pump, the PDA, and the continuous glucose monitor system. The infusion pump, which is more likely to be the kernel of the system, also receives measures covered by the sensor. Finally, the patient possesses a remote control with basic buttons for stop/resume the injections and increases the insulin dose. This command message is sent directly to the infusion pump.

2.2.2 Remote control

Since cryptography is not employed in the insulin pump systems, Marin *et al.* [10] and Li *et al.* [11] were able to eavesdrop on the communication between the remote control and the infusion pump. Then, after reverse-engineering the communication protocol and packet format, the messages were analyzed and outlined. In Fig. 2.2, we see the format of the message sent to the pump that they have established.

Based on the results of previous research work, it is concluded that the communication protocol between the infusion pump and the remote control is based on the following:

- **Message header** containing the device type that is communicating with the infusion pump.
- **Device PIN** for device authentication.
- **Information** detailing which action has been performed on the controller by the pa-

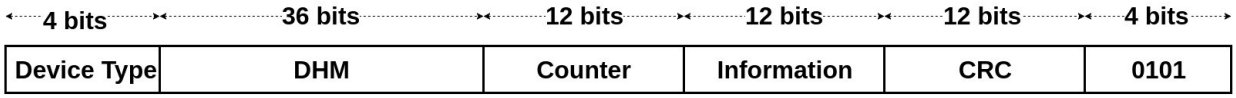


Figure 2.3: Proposed Packet Format.

tient.

- **Counter** for validating the legitimacy of the packet. If the counter indicated is higher than the value of the previous counter recorded in the log of the infusion pump, then the packet is not a replay attack item and the packet is legitimate.
- **CRC** for error check.

2.3 Proposed Communication Protocol

2.3.1 Message packet

Our goal in this work is to establish a secure authentication between the device remote control and the device itself. We started by analyzing the communication scheme used in a popular model of implantable insulin pumps and the protocol defined can be generalized for authenticating any remote control with the device. For implantable medical devices, the remote control is under the operation of the patient. Thus, it does not allow major configuration on the device, but allows just minor configurations that are needed by the patient on a daily basis and does not require the presence of a doctor. Our authentication protocol relies on plain text messages, with no use of encryption. This is mainly to reduce the computation cost on the different devices, and to avoid the physical pre-exchange of the encryption keys, that even if it is feasible for insulin pumps, for other devices, it is not. Our authentication protocol relies on two parts of the message: a modified Diffie-Hillman exchange protocol inspired by the original Diffie-Hillman (DH) key exchange protocol[21] and a counter. The message format considered here is as shown in Fig. 2.3.

Diffie-Hillman modified (DHM) exchange protocol

The DH protocol originally has a goal to enable two nodes to communicate over an insecure channel to reach an agreement on a single secret key [21]. This key can therefore be used by both sides, for example, to encrypt/decrypt messages. The privilege with DH protocol is that an eavesdropper cannot obtain the key even if he/she intercepts the full communication. Also, the DH algorithm uses modular exponentiation operations. These operations are more memory and CPU-efficient than regular exponential operations used by other algorithms. We aim to use the properties of the key computation in both nodes to generate the DHM segment, allowing the infusion pump to authenticate the remote controller. Both devices, during manufacturing, will have a shared primitive element g that is not open to the public. This will be the seed for our DHM. They also agree on a large prime number p. g should be a primitive root modulo p that generates the group $\mathbb{Z}_p^*$. In Fig. 2.4 we present the communication of solely the DHM segment to explain the authentication process.

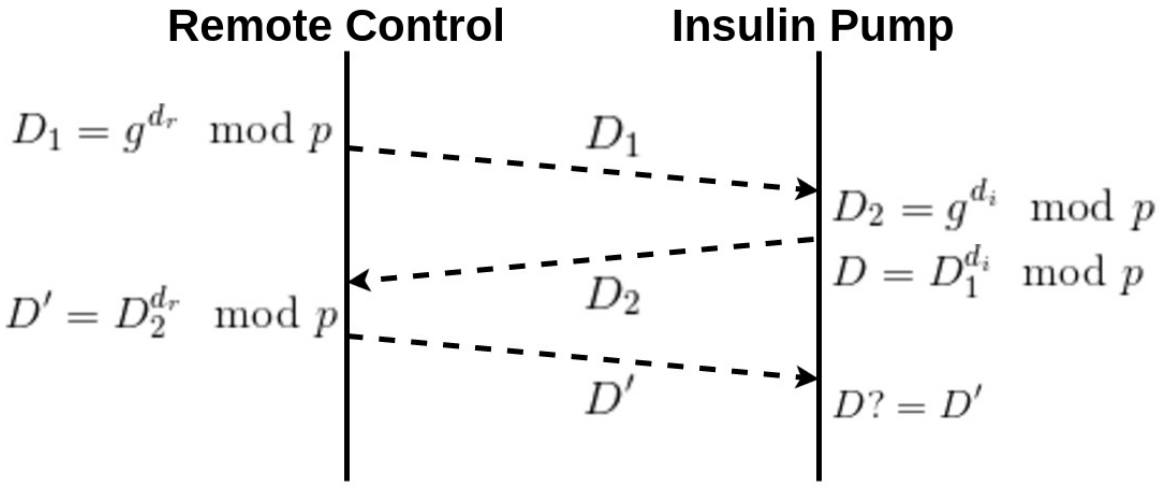


Figure 2.4: Simple Diffie-Hillman Modified Protocol.

The communication can be described as follows:

1. The remote control chooses a random number d_r in $\mathbb{Z}_p^*$ and computes $D_1 = g^{d_r} \mod p$. Then it sends it to the infusion pump.

2. The infusion pump now on its behalf chooses a random number d_i in $\mathbb{Z}_p^*$, computes $D_2 = g^{d_i} \mod p$ and sends it to the remote control. Then it also computes $D = D_1^{d_i} \mod p$.

3. The remote control now computes $D' = D_2^{d_r} \mod p$ and sends it back to the infusion pump.

4. According to the mathematical properties of $\mathbb{Z}_p^*$, the infusion pump should have $D = D'$. This equality is the proof for the insulin pump that the communication is being held with a legitimate remote control.

For an eavesdropper, all that he/she can catch are D_1 and D_2. The problem of computing D given those is known as the Diffie-Hellman problem. As long as p and g were chosen correctly, there is no known efficient algorithm [21] to compute these factors. To avoid using other complex algorithms like discrete logarithms, a time constraint [15] and packet expiration will be taken into consideration for our new protocol.

Counter

The counter is used inside the message to prevent Replay attacks: If an eavesdropper intercepts a message and resends it at a future time, the counter will give the information to the infusion pump that this message is expired and must be rejected. In order to consider the message as legitimate, the counter in the message sent must be equal to the last recorded counter in the device incremented by m, where m is in the order of 10. This window presents a security margin for the counter to prevent the device from discarding a legitimate message due to a previous connection failure. The counter is cyclic with a $2^{(length_{counter}-1)}$ period. In future work, we will study the feasibility of a Cryptographically Secure Pseudo-Random Number Generator [12] on such devices. This will certainly enhance the security of the counter prediction.

2.3.2 Communication protocol

For our new authentication protocol, the communication link between the remote control and the device will be considered to be a two-way link, enabling the system to verify the source of the message. The protocol is as illustred in Fig. 2.5:

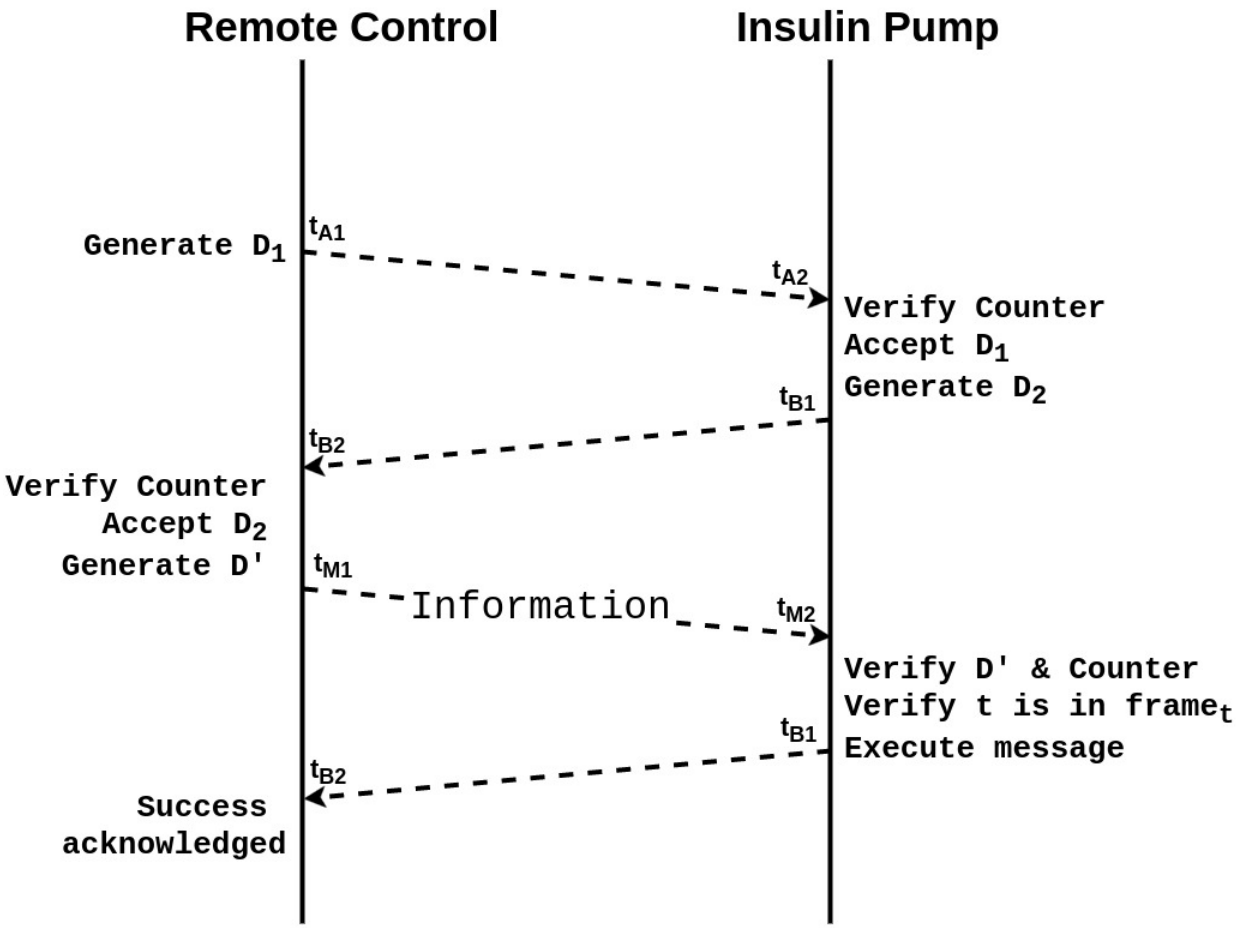


Figure 2.5: Remote Control - Infusion Pump Communication Protocol.

1. The remote control generates D_1 and sends it with a handshake message to the infusion pump.

2. The infusion pump saves the reception time t_{A2}, compares the received counter to the previous value it has on record from the last conversation. Then it generates D_2 and sends it back in another packet to the remote control with an incremented counter.

3. The counter validity is verified by the remote control. Next, it takes the received D_2 value and computes the D' value. It sends now a new packet to the infusion pump with D' value, an incremented counter value, and message related to the button triggered by the user.

4. The infusion pump now will verify the validity of the second counter, computes the communication cycle time and verifies its validity (Explained in more details in section 2.4.3). When verified, it finally computes the D value and compares it to the received D' value. In the equality scenario, it means that the message received is legitimate and is therefore executed. Then it sends a success acknowledgment to the remote control.

5. If the counter received and the communication cycle computed are validated by the remote control, this latter shows the operation success to the patient.

2.4 Security Analysis

2.4.1 DHM segment

The DHM segment contains the numbers generated by both of the devices as explained in section 2.3.1. This allows the device to authenticate the remote controller and ensures the message is coming from a legitimate source, as only the remote controller can generate a final D' equal to D generated in the device. An eavesdropper cannot engage in this case a spoof attack on the device, and the patient is therefore safe from malicious injections. Replicating an old approved communication that the attacker have eavesdropped earlier is also an impossible scenario, here it will be the role of the "Counter" segment, as explained in the following section.

2.4.2 Counter segment

To prevent Men-In-The-Middle (MITM) attacks, a counter is introduced to the packet. The counter indicates to the receiver if the packet has expired (the result of a replay attack). The counter is incremented in each step during the communication and validated when success is acknowledged. Otherwise, it is reset to the original value before the communication is initiated. A second approach for protecting the counter segment is to divide it into two parts in the message packet, as illustrated in Fig. 2.6.

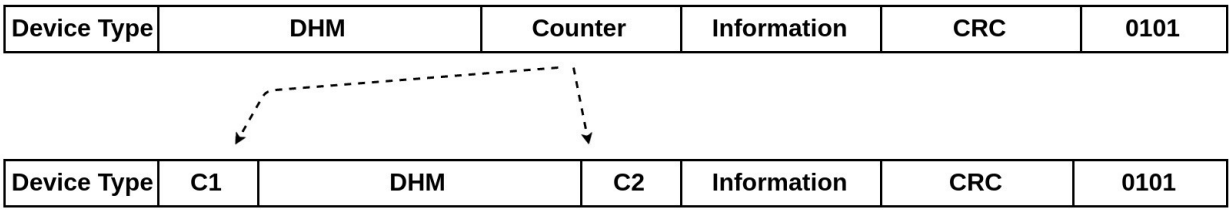


Figure 2.6: Counter Divided Segment in the New Packet Format.

The lengths of C1 and C2 are respectively (12-x) and x bits, where x is being chosen by the manufacturer. This division will make it impossible for an eavesdropper when intercepting different messages to analyze the packet and extract the counter segment. Therefore, the eavesdropper would not be able to modify it and create a new possible valid packet.

2.4.3 Time factor

To strengthen the authentication protocol's security, we introduce to the protocol a timing factor. The communication cycle is the sum of the computation time of the needed packets from the device added to the total transmission time of the full protocol: $Cycle_t = t_{M2} - t_{A2}$. We add to $Cycle_t$ margin security time ϵ. This can be computed under the assumption that the remote control is in a one-meter area of the infusion pump, which is legit as the patient is the one operating the remote control. If the effective time cycle ends in the infusion pump within this time limit, the communication protocol is fulfilled. Otherwise, this can be interpreted as a result of a MITM or a jamming attack. During the scenario of MITM

attacks, the packets will travel longer distances and will stop at more stations than it should be in a normal scenario. As for the jamming scenario, the jamming will make a full exchange of messages that will take a longer time than estimated. In the cases of exceeding $Cycle_t$, the infusion pump will stop listening to the remote control and trigger an alarm to inform the patient that his/her device is being hijacked so that the patient can take the needed countermeasures. Therefore, even the Resource-Depletion and Brute-force attacks [12] will be mitigated by this protocol.

2.5 Conclusion

In this section, we reviewed the wireless communication scheme between an implantable medical device and its remote control, to analyze existing security and privacy issues. We then analyzed the message packet used for delivering control sequences to the device, and proposed a new authentication protocol to ensure the identity of the communicating parties. This protocol relies on plain text messages for the communication, consequently avoiding the computation costs of encryption algorithms. However, the communication is not vulnerable to different malicious attacks that threaten the system. We analyzed the role of each segment constituting the wireless packet, showing the security role that it plays to protect the medical device. We believe that the proposed protocol can be applicable for any implantable medical device that includes a remote control operated by the patient.

CHAPTER 3

Light-Weight Solution to Defend Implantable Medical Devices Against Man-In-The-Middle Attack

[2] "Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack", **In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-5). IEEE**.

3.1 Introduction

One major security threat for IMDs is the Man-In-The-Middle (MITM) attack. It is defined when a malicious external party secretly eavesdrops and replays stored or relays altered communication segments between two parties assumed to be in a direct communication. Fig. 3.1 illustrates the scheme of this type of attacks. These attackers are a threat to IMDs mainly as they can:

- Intercept the patient's private information or medical logs and simply replay them to their destination.
- Store command packets as they listen to IMDs with simple architecture (Insulin Infusion pumps, cardiac pacemakers, etc.). These commands can be replayed at a later time with no alteration and trick the receiver that they are sent from a legitimate device. An example can be found in Marin's work [50] where the command packets include a fixed serial number for identification.
- Intercept the packets and jam their reception on the receiver's side. The attackers can then alter the message and resend it to the receiver as if it was sent originally from the authenticated sender.

These scenarios of MITM are straightforward in many wireless communication systems. Encryption or secure authentication cannot solve this problem systematically if they do not

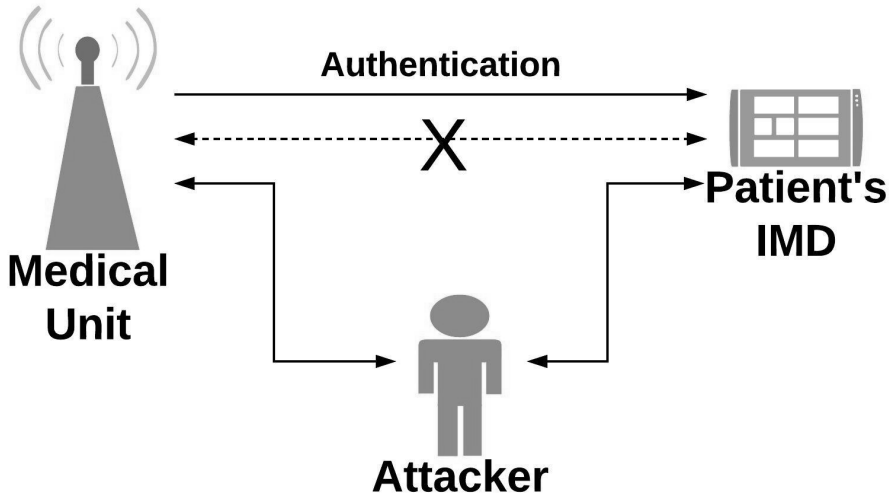


Figure 3.1: MITM Attack Scheme.

take it into account. Replaying an encrypted packet can be successful even if the attacker did not alter the packet.

In this section, we have designed a communication protocol to protect wireless IMDs from such scenarios with consideration to their resource constraints. This work relies on a dynamic signature processed by the IMD to acknowledge the commands it receives. Throughout the communication protocol, both ends of the communication are able to ensure if the execution of a received command is safe or illegitimate. The signature is based on a chaotic generator. The properties of this system are able to reveal the existence of a third party within the communication. Therefore, the IMD can ensure that the communication is held directly to the properly authenticated unit.

3.2 Low-Dimensional Chaotic Systems

3.2.1 Chaotic systems

Chaotic systems are determined systems with a non-linear behavior. They have a good attraction in the security field for three reasons [33]:

- Their ideal pseudo-randomness.
- Large and broad spectrum.
- Their sensitivity to the initial conditions that are fed to the system.

Therefore, research on chaotic systems for secure communications has been investigated thoroughly [35, 36, 37]. We can define chaotic systems as dynamic systems that are characterized by unpredictable observations from an external point of view, i.e., an observer of the output from the system cannot conclude that these observations are the result of a deterministic system. For that reason, they are considered pseudo-random systems. Also, they have a property of high sensitivity towards initial conditions change in the system. Therefore, chaotic systems can produce cryptographically secure pseudo-random number generators [12]. In addition, without the right initial conditions, the correct pseudo-random sequence cannot be regenerated.

3.2.2 Henon scheme

The Henon system is a two-dimensional system containing a single quadratic term as the non-linearity [39]. This map is known to display chaos for certain parameter values and initial conditions [34]. The Henon map [38] is a simplified model of the *Poincare map* in a discrete time that emerges from a solution of the Lorenz equations.

The Henon map is expressed in the following equations:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{3.1}$$

where $a > 0$, $b > 0$ (bifurcation parameters) [38].

The output of the system depends highly on the initial conditions represented by x_0 and

y_0. The bifurcation parameters used to show a chaotic behavior are $a = 1.4$ and $b = 0.3$. These values were fixed in a way that they are relatively small to prevent x_i and y_i from reaching infinity, without losing the line structure of the attractor[39]. The attractor of this chaotic system is plotted in Fig. 3.2. Disregarding the initial points, the system output points orbit around the Henon attractor in a random way. Any change in the initial conditions will affect the way these points orbit in the attractor.

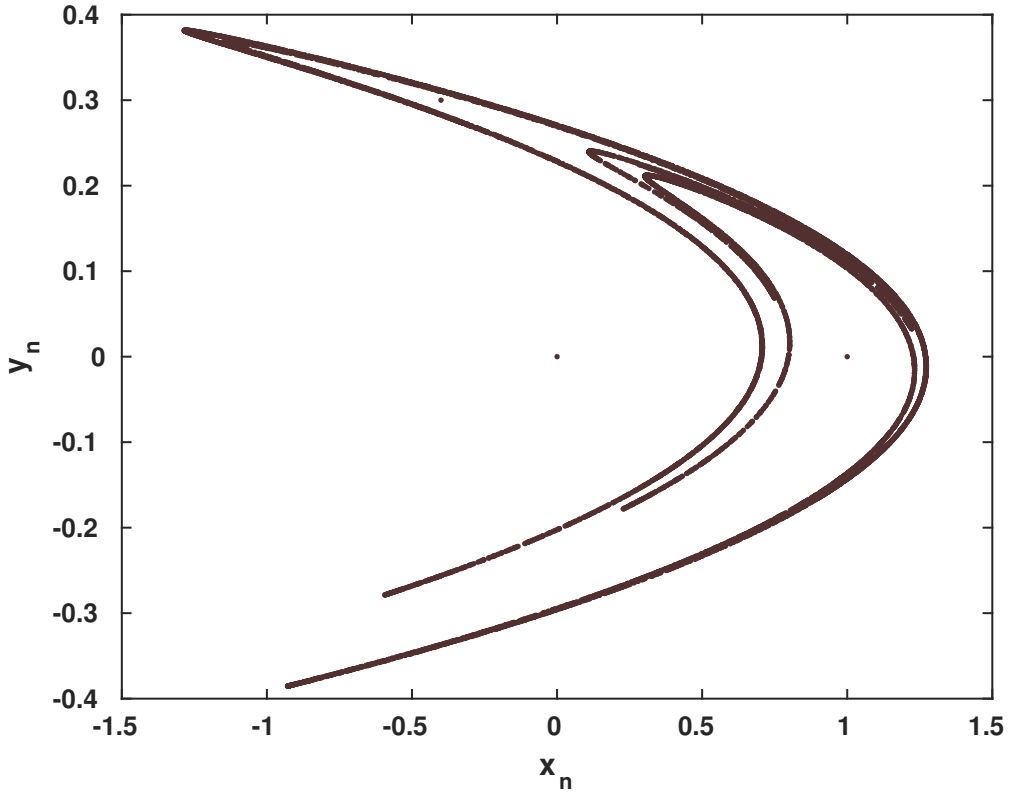


Figure 3.2: Henon Attractor for $x_0 = 0.2$ and $y_0 = 0.2$.

3.3 Dynamic Signature

Encryption has always been the manufacturer's solution to inhibit adversary's attempts to hijack implanted devices. In this work, we adopt a method that is similar to encryption, but its protocol uses less computational resources than common encryption protocols. The protocol presented by this work relies on the dynamic signatures of the commands received as a receipt acknowledgment. This dynamic signature is designed to encode and decode binary packets without relying on complex standard encryption algorithms such as DES or AES [40]. The proposed method relies on the Henon chaotic generator as a random number generator. Its pseudo-random behavior will assist both ends of the communication to achieve the same key without the necessity to wirelessly share it on a public medium.

Each signature will have k sub-signatures. These k packets will not necessarily be available simultaneously. Depending on the nature of the IMD, they can be divided onto multiple sending points (sensor network), or simply, available on different time/frequency slots. The signature of a message packet M is the print of this message on a matrix template. The signatures have no collisions, i.e., two different binary messages cannot have the same signature.

The template matrix TM is presented in Equation 3.2.

$$TM = \begin{bmatrix} 1 & 1 & 1 & 0 & \dots & \dots & 0 & 1 & 1 \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & 1 & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & 0 & \dots & \ddots & \ddots & 0 & \vdots & \vdots \\ 1 & 1 & 0 & \dots & \dots & 0 & 1 & 1 & 1 \end{bmatrix} \tag{3.2}$$

The size of the TM corresponds to the size chosen for the length of each sub-signature. The message signature is a matrix of the same size as TM, where each element is presented in

Equation 3.3:

$$S_{i,j} = M_i \times TM_{i,j} + (1 - M_i) \times (1 - TM_{i,j}) \tag{3.3}$$

Each row of S is a sub-signature. The sequence of the sub-signatures S_i will be arranged in a random shuffle using the Henon map generator. The signature algorithm is a reversible process. Once possessing the right seed for the chaotic map used and after receiving all the sub-signatures, the device can verify the authenticity of the signature. Therefore, it can validate the communication.

3.4 Communication Protocol

The protocol designed by this work intends to minimize the use of encryption/decryption algorithms in the IMD level. The IMD will only use the signature algorithm in one way. However, it is the sender's role to create and decipher the signed messages, as this device does not have any energy or computational constraints. It will be shown in the following section that this protocol is resource-friendly. Fig. 3.3 shows the communication steps. The sender, or the Control Unit (CU), will start with a handshake (HS) request. This request will include a sender's identification with the seed to be used in the chaotic generator. The initial conditions of the chaotic system would be synchronized using physical links due to the initial state of the whole system. The high sensitivity of the chaotic systems towards these conditions diminishes the need of their future update. Consequently, only the seed will be shared wirelessly in any communication scenario. The IMD will sign the received message and send it back to the CU.

If the CU validates the signature, it sends the user's commands to the IMD. The IMD has to acknowledge each received command message by sending back to the CU the generated k sub-signatures from each individual packet. The security aspect of this protocol is better explained in Section 3.5.1. In a general case, the IMDs do not receive a command chain in one instance. In the case of an implanted syringe, for example, the commands would be a

simple increase, decrease or a certain dose injection at one time. After sending the signature, the IMD will only execute the command after receiving a second signature, proving that the communication has been held with the authenticated CU. The IMD will validate the signature by comparing it to its own generated signature from the previous message. If this validation fails, the command is rejected and an alert is triggered that there may be a third party in the system.

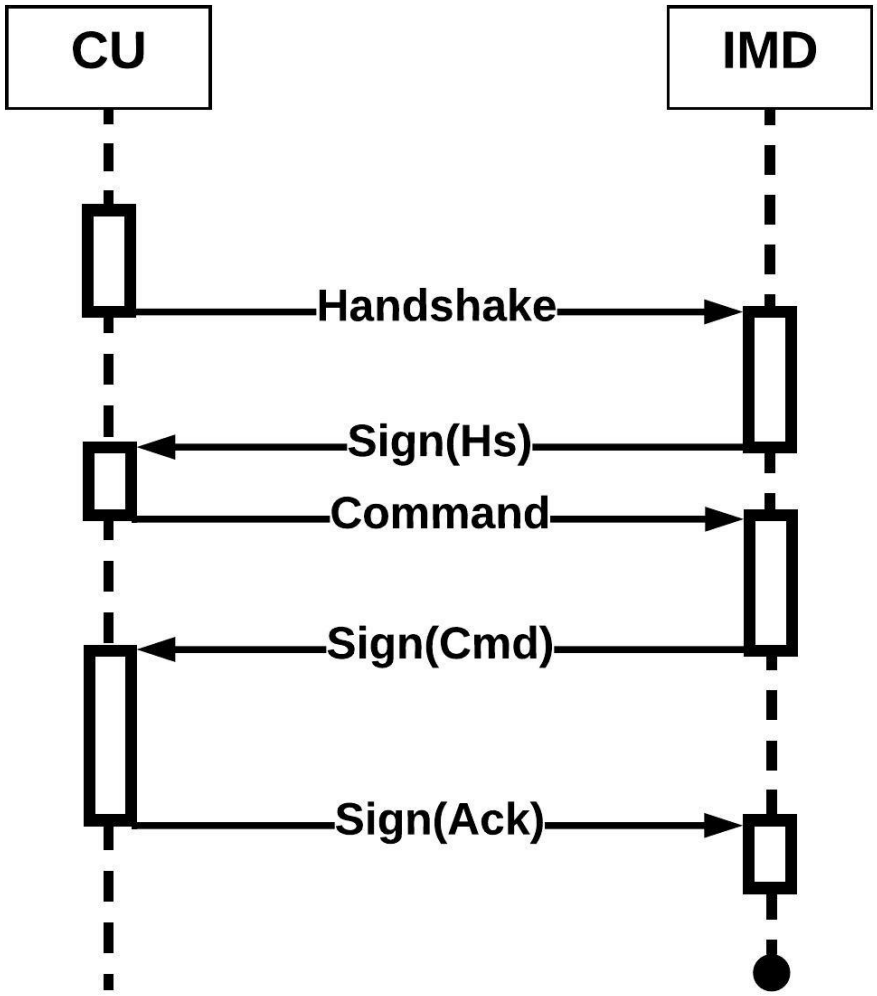


Figure 3.3: Message exchange of the protocol in a typical communication scenario.

3.5 Performance

3.5.1 Security Analysis

This protocol is designed specifically to defend IMDs from MITM attacks. The role of the dynamic signature is to ensure the authenticity of the commands received by the IMD. The IMD is not required to encrypt and decrypt all the messages it treats, reducing the computational cost of the protocol. The CU verifies the integrity of the received signature as explained in Fig. 3.3 before proceeding with the communication. The command message, the important segment in the communication, will not be executed unless the IMD verifies the integrity of the Sign(Ack). The latter is the result of an authentic signature received from the IMD. In the scenario of a MITM attack, an attacker is unable to personally sign any communication packet because it lacks the initial conditions of the Henon Map. Intercepting all the different sub-signatures that have been sent separately is a difficult task for an eavesdropper to achieve. Even in the scenario where he/she had them all, the lack of the correct sequence to arrange them will make the sub-signatures undecipherable. Each communication held will have a different seed for the Henon generator exchanged with the Handshake request. Therefore, each packet will expire when the communication ends. Any future replay of a previously eavesdropped packet will be rejected from the IMD. Thus, the attacker is unable to either replay previous commands nor to jam and alter the communication in real-time.

3.5.2 Randomness

This protocol relies on the random sequence generated by the henon map to shuffle the sub-signatures. This is done in order to harden the task of deciphering the communication by an external party. Any alteration in the order of the k sub-signatures will lead to an erroneous signature. This order is only shared between the CU and the IMD as they are the only two

devices with synchronized initial conditions and seed for their respective chaotic generator. The security aspects of any key generator relate highly to the randomness of its outputs[31]. The National Institute of Standards and Technology (NIST) [42] described procedures that aim to detect any deviation of a given binary sequence from being random.

Monobit test

This test ensures the randomness of the whole sequence by verifying if the appearance proportions of 0's and 1's are approximately the same. Thus, there is not a value that is more probable to appear than the other.

The test assigns a value of -1 to each 0 and a value of 1 to each 1 in the n-bit sequence, then it computes the sum S_n into

$$s_{obs} = \frac{\|S_n\|}{\sqrt{n}}; \tag{3.4}$$

The test passes when $P_{value} = erfc\left(\frac{s_{obs}}{\sqrt{2}}\right) > 0.01$, with $erfc(\cdot)$ being the complementary error function. The result is interpreted as follows: if in the sequence there are too many ones or too many zeros, S_n will deviate from 0, and large values of S_n will lead to a small value of P_{value}.

Frequency Test within a Block

This test verifies the proportion of 1's within M-bit blocks. It determines if the frequency of 1's in the M-bit block is approximately the same as the frequency of 0, as expected from any random sequence. This test is a general form of the previous test, as the latter falls in this test when M is equal to the total length of the sequence.

The test divides the whole sequence into M-bit blocks, if there are any remaining bits, they are automatically discarded. Then, it computes the proportion π_i of 1's in each block i, and finally,

$$\chi^2(obs) = 4M \sum_{i=1}^{N} (\pi_i - 0.5)^2 . \tag{3.5}$$

The test passes when $P_{value} = igamc\left(\frac{N}{2}, \frac{\chi^2(obs)}{2}\right) > 0.01$, with N being the number of blocks in the sequence and $igamc(\cdot)$ being the incomplete gamma function. The result is interpreted nearly as the previous one: a small value of P_{value} indicates that there is a large deviation from the equal proportion of 1's and 0's in at least one of the blocks.

Runs test

A run is a continuous sequence of the same bit value. The run should also be bounded with a bit of the opposite value at its start and end. An example of a k_bit run is:

$$...0\underbrace{11...111}_{\text{k bits}}0...$$

This test verifies if the number of runs existing in the generated sequence is as expected from a random sequence. In other words, the test verifies if the oscillation between 0's and 1's is not too quick or too slow for a random sequence.

The test verifies this oscillation by calculating

$$v_n(obs) = \sum_{j=1}^{n-1} r(j) + 1; \tag{3.6}$$

$$\text{where } r(j) = \begin{cases} 0 & \text{if } bit_j = bit_{j+1} \\ 1 & \text{otherwise} \end{cases} \tag{3.7}$$

The test passes when

$$P_{value} = erfc\left(\frac{\|v_n(obs) - 2n\pi(1-\pi)\|}{2\sqrt{2n}\pi(1-\pi)}\right) > 0.01; \tag{3.8}$$

The result is interpreted as follows: A small value of $v_n(obs)$ indicates that the oscillation between 0's and 1's in the sequence is too slow to be considered as a random sequence, a large value of $v_n(obs)$ indicates that the oscillation is being too quick for a random sequence.

Test for the Longest Run of Ones in a Block

This test ensures that the length of the longest run of 1's within the different M-bit blocks of the generated sequence is compatible with the length of the longest run of 1's expected in a random sequence, with M a pre-set value from the NIST.

The test will compute the longest run k of 1's in each block, then will categorize the block into categories c_i depending on the value of k according to Table 3.1.

Table 3.1: The k values according to the block lengths.

$\mathbf{c}_i$	M=8	M=16
c_0	$k \leq 1$	$k \leq 4$
c_1	$k = 2$	$k = 5$
c_2	$k = 3$	$k = 6$
c_3	$k \geq 4$	$k = 7$
c_4	—	$k = 8$
c_5	—	$k \geq 9$

Then it will compute the frequencies of the longest run of the blocks ν_i = number of blocks falling in c_i. Afterwards, it will calculate

$$\chi^2(obs) = \sum_{i=0}^{L} \frac{(\nu_i - N\pi_i)^2}{N\pi_i};$$

where L and N are pre-determined by the NIST as shown in Table 3.2.

Table 3.2: The pre-set values of M, L and N according to NIST.

M	L	N
8	3	16
128	5	49

The test passes when $P_{value} = igamc\left(\frac{L}{2}, \frac{\chi^2(obs)}{2}\right) > 0.01$. The result value being not small shows that the generated sequences have no cluster of 1's or 0's.

Discrete Fourier Transform (Spectral) Test

This test focuses on the peak heights of the Discrete Fourier Transform (DFT) of the generated sequence. It looks in the sequence for periodic features that contradict the assumed

randomness of the bit chain.

The test assigns a value of -1 to each 0 and a value of 1 to each 1 in the n-bit sequence and sums it to produce a value X, then it applies the DFT, $S = DST(X)$. Afterwards, it computes $M = \|S(\text{first } n/2 \text{ bits})\|$ and the peak height threshold $T = \sqrt{\left(\log \frac{1}{0.05}\right) n}$. Finally, it computes $N_t = \frac{0.95n}{2}$, the expected theoretical number of peaks under the threshold T, and

$$d = \frac{N_o - N_t}{\sqrt{0.95 \times 0.05 \times (n/4)}};$$

with N_o the actual number of peaks in M that are less than the threshold T.

The test passes when $P_{value} = erfc\left(\frac{\|d\|}{\sqrt{2}}\right) > 0.01$. A low value of d indicates that there were actually too many peaks in M above the threshold T.

The results are shown in Table 3.3.

Table 3.3: Statistical NIST Test Results.

Test name	
Monobit Test	100%
Frequency within a block	100%
Run Test	100%
Longest Run	100%
DFT (Spectral)	100%

3.5.3 Signature Robustness

To ensure the robustness of the signature against statistical attacks, we have plotted Fig. 3.4. This plot is a matrix where each row represents the signature of a given message and the length of a row is equal to the bit-length of the message. Each element is the occurrence of the bit 0 in that position after a large number of trials to sign the given message with different generated keys. The figure shows that all the elements have a relatively equivalent probability (between 43% and 56%) to show the value 1 as to show the value 0. Therefore,

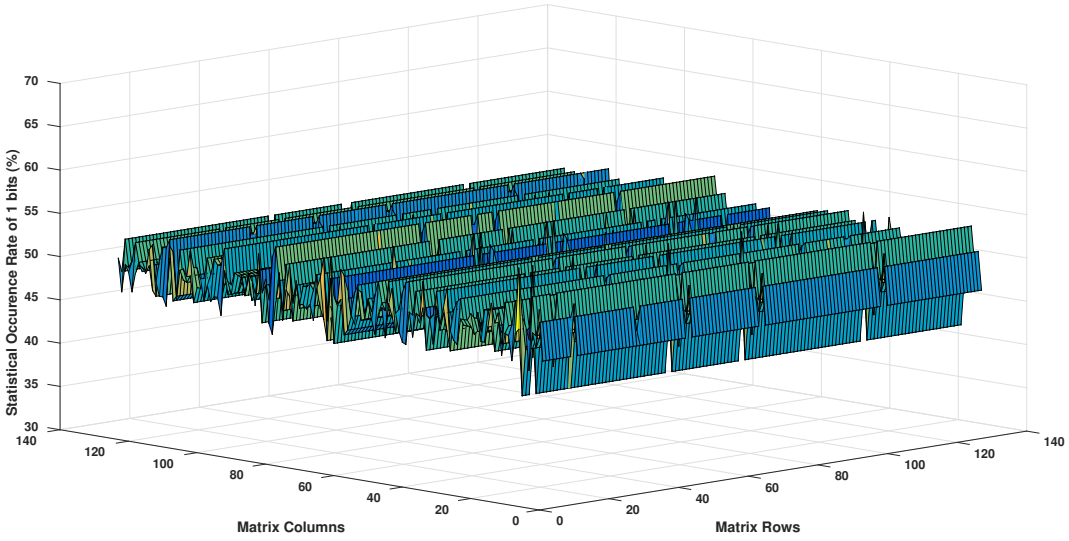


Figure 3.4: Matrix Element Occurrence of "1" bits.

it can be concluded that there is no pattern that allows an eavesdropper to statistically conclude the intercepted message with the single knowledge of the signature.

3.5.4 Hardware Implementation

Our proposed protocol consists of the implementation of the Henon map system and the signature algorithm. We simulated this with test vectors returned by a software simulation with the VHSIC Hardware Description Language (VHDL). The system has been implemented on Xilinx Spartan-6 [44] using a VHDL structural description. ISE Simulator (ISim) of Xilinx software tools [45] have evaluated the hardware resource requirements for our system. The synthesis results are displayed in Table 3.4 and Table 3.5, defining the hardware resources for Slices/Flip-Flops numbers and the speed performance.

3.6 Conclusion

A new approach to protect Implantable Medical Devices (IMDs) from Man-in-the-Middle (MITM) and replay attacks is introduced in this section. This defense mechanism is based

Table 3.4: Implementation Design Summary of a 128-bits Key Generator.

Number of occupied Slices	18 out of 1430
Number of Slice Register	51 out of 54576
Number of Slice LUTs	464 out of 27288
IO Utilization	68

Table 3.5: Implementation Design Summary of the Signature Algorithm using a 128-bits Key.

Number of occupied Slices	16 out of 1430
Number of Slice Register	20 out of 11440
Number of Slice LUTs	50 out of 5720
Number of fully used LUT-Flip Flop pairs	30 out of 61

on a chaotic generator for randomness purposes and on a signature algorithm to prevent any third party interference. This signature is dynamic based on the fact that it can only be validated by a trusted user. This trust is built with the use of the henon chaotic map. This map is highly sensitive to its initial conditions, statistically speaking, an attacker cannot reproduce the same output when eavesdropping on the communication. The protocol shows promising results. This permits the scheme to be considered for use with various types of IMDs like Infusion pumps, cardiac pacemakers and neuro-implants.

CHAPTER 4

Biometric-based Authentication Scheme for Implantable Medical Devices during Emergency Situations

[3] "Salt Generation for Hashing Schemes based on ECG readings for Emergency Access to Implantable Medical Devices", **In2018 International Symposium on Networks, Computers and Communications (ISNCC) 2018 Jun 19 (pp. 1-6). IEEE**.
[4] "Biometric-based authentication scheme for Implantable Medical Devices during emergency situations", **Future Generation Computer Systems. 2019 Feb 8**.

4.1 Introduction

To defend this threat, biometrics are among the solutions that have been studied. One of these biometrics is fingerprints. The patterns they provide are proven to relate uniquely to one person. This makes fingerprint a key feature to be used for authentication. Scanning the literature, several schemes have been proposed to secure general IMD access. To alleviate security vulnerabilities of IMDs, Ankarli *et al.* [52] presented a technique for physical layer authentication. This technique allows IMDs to avoid using any existing methods of cryptology. They provided also in their work some techniques to provide additional advantages for IMD implementations. They improved the processing complexity of IMDs algorithms and enhanced the overall communications performance. As for Kim *et al.* [53], they introduced a new vibration-based secure side channel to be used for IMD security. They provided the necessary analysis to prove the robustness of their scheme. The vibration signal was used as a wake-up signal and their analysis was established in a human body realistic model. Additionally, Long *et al.* [54] presented a study where an authentication protocol is based on the recognized standards of AES and SHA. They also demonstrated an encryption protocol for the same purpose and a model that protects against multiple network threats. Also, Chi *et al.* [55] presented in their work an encryption algorithm to encrypt and compress the IMD

data simultaneously. This compression will reduce the data transmission overhead and also ensures a high data confidentiality and usability. Their scheme was based on smartphones as a proxy to undertake most of the security-related tasks. The smartphone had the task to establish a connection between the IMD and the doctor, responsible for all operations on patients using IMDs, a secure channel. Their work is based on secret key sharing that were extracted from a physically inaccessible seed by outsiders. The main common point between these previous schemes is that they rely on the knowledge of both ends to each other, or that they both request to establish a link. These schemes may under emergency situations, e.g., loss of consciousness, medical situation in a foreign city, prevent an emergency medical team to interfere with the IMD. Without the user's or the IMD's doctor acknowledgment, the security schemes are intended to prevent any additional access to the IMD's functions.

We have designed this scheme in which the IMD access is based on these two biometrics while focusing on minimizing the analysis cost on both features and avoid sharing them publicly during all authentication requests from any legitimate device.This authentication can be triggered through an emergency flag during the access request. Upon approval, this scheme will be as a backdoor to access the IMD without the need for the user's knowledge. The scheme can be also in use for regular authentication, but its main goal is to guarantee legitimate access to the IMD when the user is unconscious.

The motivation behind this scheme is to guarantee foreign interventions with the IMD under emergency scenarios. The main purpose of the IMD is offering spatial freedom and remote health supervision. Also, the IMD should be well-protected against exterior threats, hence the fact that only the IMD technician and the patient's doctor should have direct access to the IMD, in addition to the user itself. However, for certain common medical conditions like diabetes and seizures, the patient may suddenly lose his conscious and needs immediate attention from the closest qualified medical team. Lacking the means to authenticate and obtain access to the IMD, the patient's life is threatened if the IMD does not hold backdoor access for before-mentioned scenarios. Consequently, we have elaborated the work

presented in this section to alleviate this problem while guaranteeing the patient's privacy and security. Under unsecure conditions, such scenarios represent an opportunity for attackers to hijack the IMD for present or future attacks.

4.2 One Factor Authentication

4.2.1 Goal

As a first step in this work, we want to use ElectroCardioGraphic (ECG) signals as a biometric to authenticate emergency medical staff. The scheme we designed plays the role of a backdoor in IMDs for emergency situations. This scheme grants access for legitimate non-previously authenticated parties that need control over the IMD to monitor the patients' life. At the same time, the IMD should ensure that the new authenticated device is a legitimate node. To achieve this purpose, our design will allow an external device to synchronize with the IMD to obtain a shared secret key. The shared key is used to create a signature related to the message sent to the IMD. On the IMD level, the signature can be validated or rejected by applying the secret key. In our design, we intend to prohibit any malicious eavesdropper on the wireless communication to estimate the resulting key. For this reason, we adopted the elliptic curve cryptographic properties. This scheme is to be used only in emergency situations. If the mechanisms are triggered under normal circumstances, the user would be notified and he/she has the possibility to interrupt it and take the needed precautions.

4.2.2 ECG Signal Acquisition

ElectroCardioGraph (ECG) [61] records depict the electrical activity of the heart. It is the time series of the electrical oscillations of the heart cyclic rhythm. ECG is very useful to inform that:

- The heart cycle is being normal, too slow, too fast or irregular by the duration of the

electrical activity.

- The performance of the heart muscle and its chambers is normal or abnormal. This is described by the different magnitude of the electrical activities.

The frequency range of an ECG signal is generally within [0.05,100] Hz and its dynamic range is about 1mV to 10mV. The performance of ECG acquisition system depends mainly on the accuracy and reliability of the detection of the QRS complex, as well as T- and P-waves. Fig. 4.1 illustrates the electrical signal variation describing the rhythm of a typical healthy person's heart. This periodic variation consists mainly of a PR interval representing the time that takes the electrical activity to move between the atria and ventricles and a QRS interval describing the depolarization of the ventricles. A third interval is also to be considered important which is the ST segment. The latter describes the time between depolarization and repolarization of the ventricles. The duration of the heartbeat can be

Figure 4.1: Normal ECG Waveform.

identified by measuring the time interval between two consecutive R peaks. This can be achieved by an external sensor on the wrist of the patient, for example. This sensor will communicate with the IMD using emergency flags, in order to synchronize with the device

and acquire a synchronized ECG signal. Afterwards, the sensor will send the data to the medical team device for further analysis.

4.2.3 Elliptic Curve Cryptography

In 1985, Elliptic Curve Cryptography (ECC) was presented by Miller [62] of IBM and Koblitz [63] of the University of Washington as an adequate alternative in cryptographic schemes for the traditional cryptosystems, e.g., DSA and RSA. ECC systems perform robustly even with short keys and have lower computational overhead compared to the traditional methods. This becomes important when the devices in question suffer from serious limitations in processing power, memory, and battery life [64].

We intend to exploit the hard-to-solve discrete log problem with ECC to secure the authentication between the two new devices. This problem is as follows:

For this purpose, each end, separately, would generate randomly its secret key SK_i. Then, each will compute its public key $PK_i = f(g, SK_i)$ and share it with the other end wirelessly. The function f is most likely to be the modular exponentiation [65]. After sharing the public key, both parties would achieve a final key $FK_i = f(SK_i, PK_j)$. Due to the properties of ECC, both are sharing the same secret $FK_i = FK_j$. This can be achieved publicly if a group G and a fixed group element g are previously agreed upon.

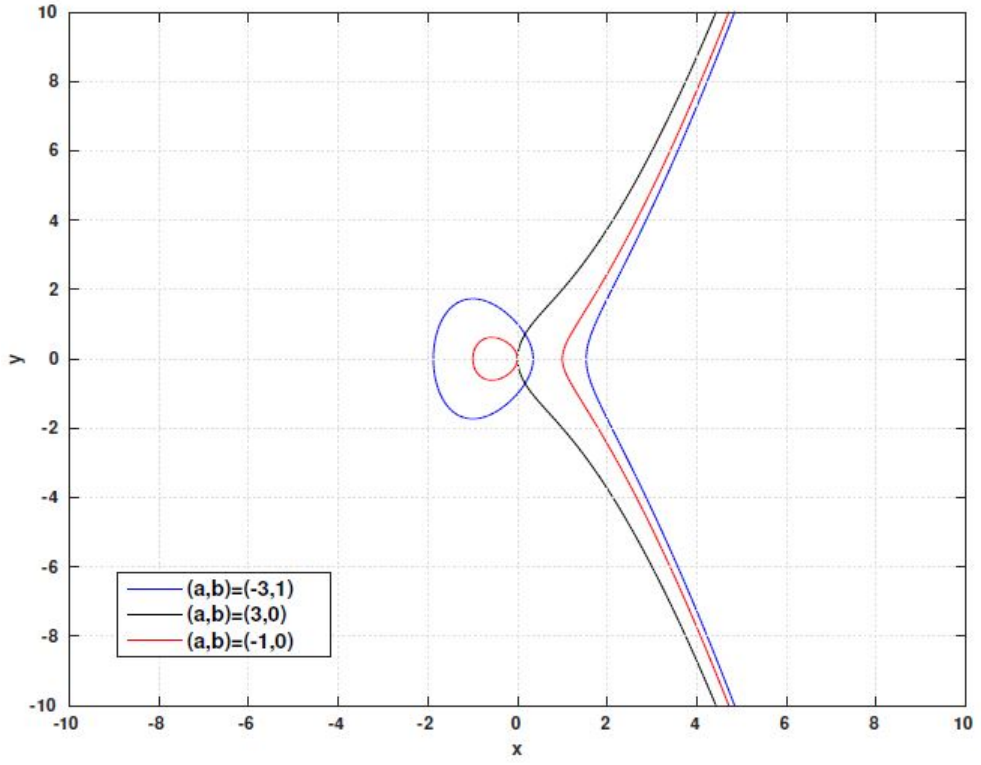
In more details, the elliptic curve is given by Equation 4.1:

$$y^2 = x^3 + ax + b \tag{4.1}$$

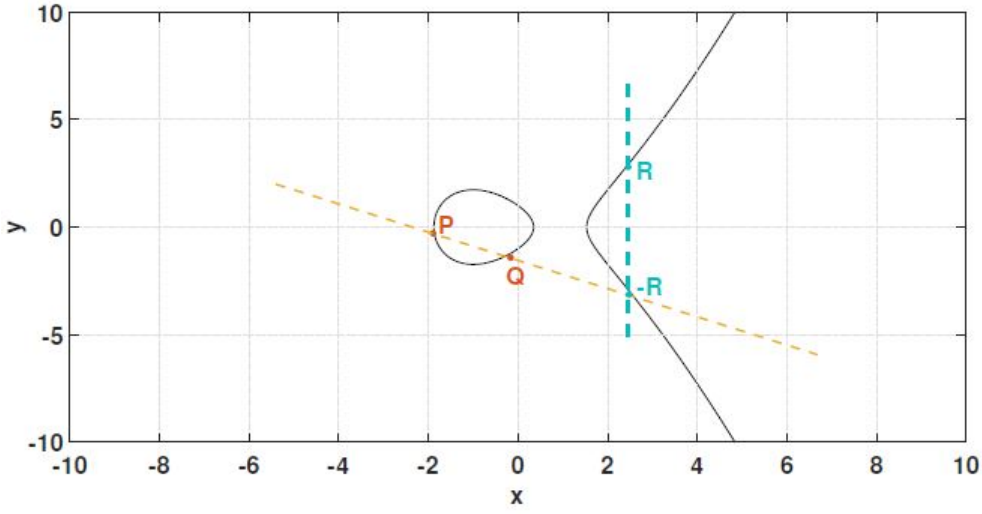
where x, y, a and b are elements in a Galois Field [64]. The pair (a,b) defines the elliptic curve. An example of these curves with different (a,b) pairs is described in Fig. 4.2.

The group of the elliptic curve is closed under the addition operation given by:

$$R(x_R, y_R) = P(x_P, y_P) + Q(x_Q, y_Q), \text{ such that}$$



(a)



(b)

Figure 4.2: (a) Elliptic Curves for Different (a,b) Pairs and (b) the Graphical Resolution of an Elliptic Curve System.

$$\text{if } x_P \neq x_Q : \begin{cases} \alpha = \dfrac{y_Q - y_P}{x_Q - x_P} \\ x_R = \alpha^2 - x_P - x_Q \\ y_R = \alpha \times (x_P - x_R) - y_P \end{cases} \tag{4.2}$$

$$\text{if } x_P = x_Q : \begin{cases} \alpha = \dfrac{3 \times x_P^2 + a}{2 \times y_P} \\ x_R = \alpha^2 - 2 \times x_P \\ y_R = \alpha \times (x_P - x_R) - y_P \end{cases} \tag{4.3}$$

For the computation of $R = k \times P$, all what we need to do is compute

$$R = \underbrace{P + P + ... + P}_{\text{k times}} \tag{4.4}$$

For our design, the point R represents the final shared secret key, k represents the individual secret key and P represents the shared key. The Elliptic Curve Discrete Logarithm Problem given here, is that, with a prior knowledge of P and R, it is practically unfeasible to obtain k such that $R = k \times P$.

4.2.4 Security Scheme

The average inter-beat time of any human heart is between $665ms$ and $1.5s$. In order to guarantee the achievement of synchronized keys, we had to verify if both acquisitions (the IMD and the sensor) will include the same readings. In the literature, the average latency time for an IMD to detect electric signals on a body-level wireless communication is defined to be $200ms$ [66] in the worst case. Therefore, both devices will synchronize their acquisition while taking into accounts these delays. A threshold is computed accordingly to the R-peak frequency in order to discard any out-of-sync heart beat. This will ensure that both devices will record similar ECG acquisitions.

Fig. 4.3 demonstrates the procedure of establishing a secret key. This key will be used

for request validation. The shared secret key will finally be $Seret\_Key = k_a \times R_b = k_b \times R_a$. Both devices have the necessary variables to compute it. k_a and k_b could be:

- Random numbers generated independently in the IMD and the medical team system, respectively.
- Numbers specific to the devices themselves, like hidden PIN or ID numbers. This can be the case when a decreased computational work is desired.

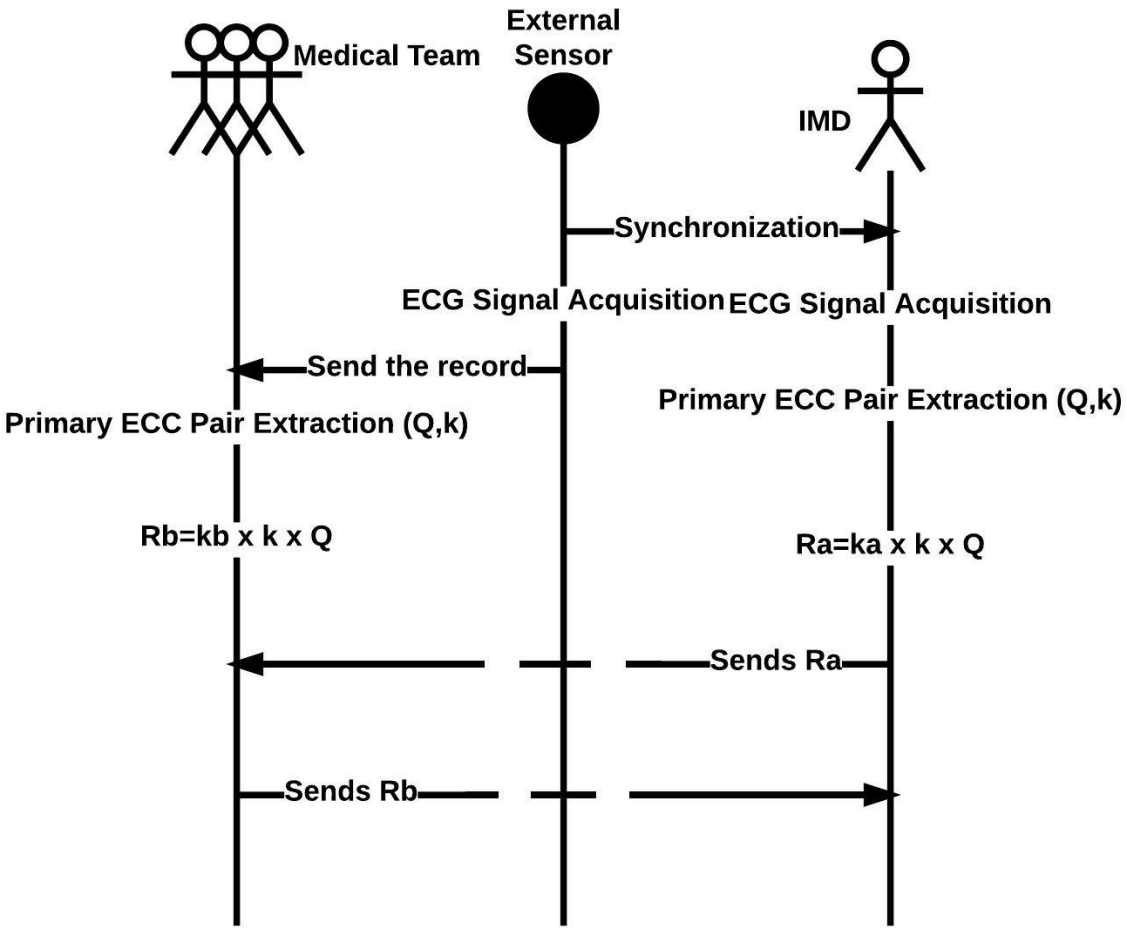


Figure 4.3: Secret Key Establishment Protocol.

In order to generate the pair (x_P, k) of the Elliptic-Curve algorithm, the measured values of R-R intervals in ms will be converted into a binary format. Table 4.1 explains an example

of this conversion when a 4-bit value is assigned to each measure. The range of the values recorded is to be divided into 2^{bits} intervals limited by th_i.

Table 4.1: Look-Up Table for Conversion Measures

Measured Value	**Binary Value**
$\geq th_i$	0100
$\geq th_{i+1}$	0101
...	...
$\geq th_{i+n}$	1110

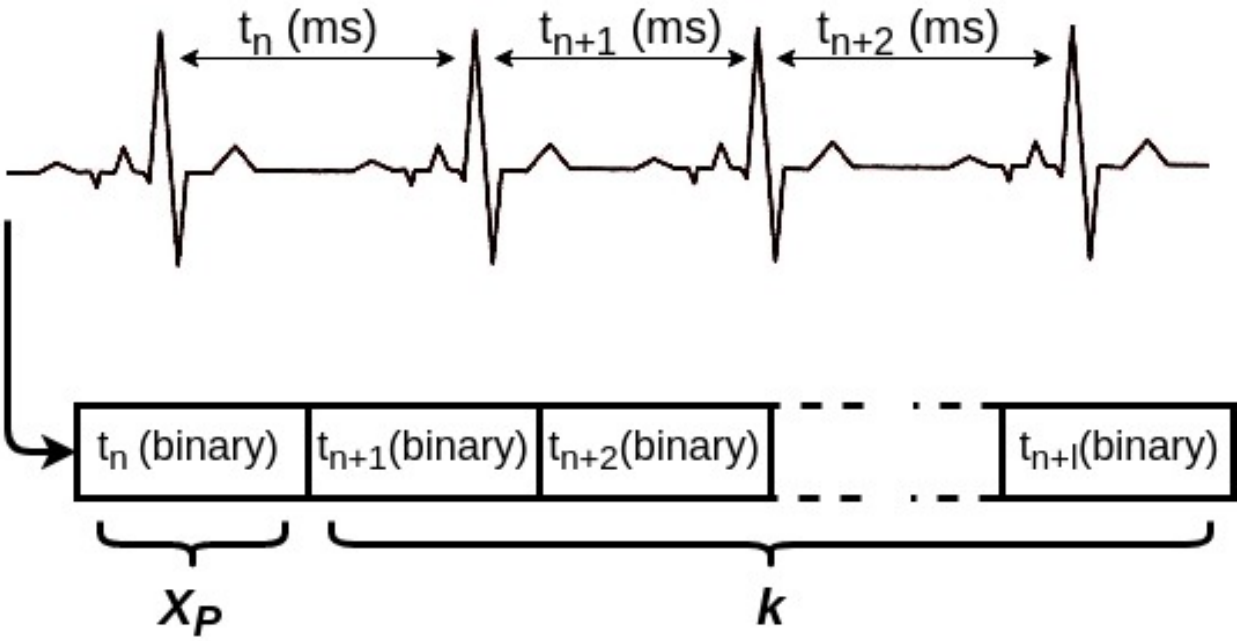


Figure 4.4: Keys Extraction from Inter-beat Values.

Fig. 4.4 explains the extraction process. Each part computes the secret key from the initial keys acquired from the ECG signal.

4.3 Two Factor Authentication

4.3.1 Goal

The second factor we intend to add to our authentication scheme in this work is fingerprint readings. The shared key at this level is a result of a two-way function that has the ECG reading and the fingerprint data as inputs. We intend to use the fingerprint scan as a second proof for the IMD that the party requesting authentication is a legitimate party and is with the IMD user. This scheme allows the medical team to gain access to the IMD without the need of the user permission, even if they were never authenticated before. The team will acquire the fingerprint of the user in the moment of the emergency and will use to form the authentication key. As for the IMD, it will use the stored fingerprint data in its system to verify the integrity of the received key. If the received key is in conform with the generated key, the IMD will accept any request from the medical team's end.

4.3.2 Fingerprint Recognition

Human fingerprints have been widely used to identify the person's identity as they have been proven to be unique to each individual. Human fingerprints show particular permanent patterns that are associated with the identity of that person. They are considered as one of the most reliable human features that can be easily acquired [67]. The fingerprints are constituted of ridges, called minutiae. The most notable types of minutiae are ridge ending and ridge bifurcation. These two allow an automatic matching between different fingerprints when detected. A minutia is characterized by a list of attributes that includes its type (as shown in Fig. 4.5), its position within the fingerprint scanned and its orientation. These three attributes help match the different minutiae along the fingerprints, the more similar they are, the more likely the fingerprints are associated to one individual.

Several approaches have been proposed to achieve a strong fingerprint matching tech-

nique. This is due to the fact that several assumptions had to be taken for fingerprint matching:

- When scanned, the fingers may be placed in different locations during acquisition, resulting therefore in a translation or in a rotation of the fingerprint.
- Non-linear deformation may take place during the acquisition process due to the finger pressure on the sensor.
- Two different scans of the same fingerprint can lead to two results with some different minutiae.

4.3.3 Fingerprint Reading

Image processing

As a common procedure, a pre-process of the acquired fingerprint image takes place before the extraction of its feature [68]. To improve the image, an histogram equalization is applied on the image to increase the contrast of the image lines. This enhances the detection of the features. After this, a normalization [69] takes place. This gives the fingerprint image a balanced data magnitudes, matching a pre-defined mean and variance elaborated by the algorithm. Following this step, the direction and frequency of ridges are estimated following local ridges orientation and their local frequencies. After these steps, the image is converted to a black-and-white image. This step is intended to help in the segmentation of the fingerprint. Finally, an image thinning takes place to define the lines of the fingerprint features on a single-pixel level. Therefore, minutiae can be extracted at each pixel level with a 3x3 filter.The filter detects, according to the black pixels representing the fingerprint's ridges, the type of that ridge. Fig. 4.5 shows some examples of minutiae detection within a 3x3 pixels filter (discontinuous line). A continuous line along the filter means there is a continuous ridge, so no minutiae are located on those coordinates. If the pixel shows a ridge end (white

pixels) or a bifurcation, then a minutia is detected and its characteristics are extracted.

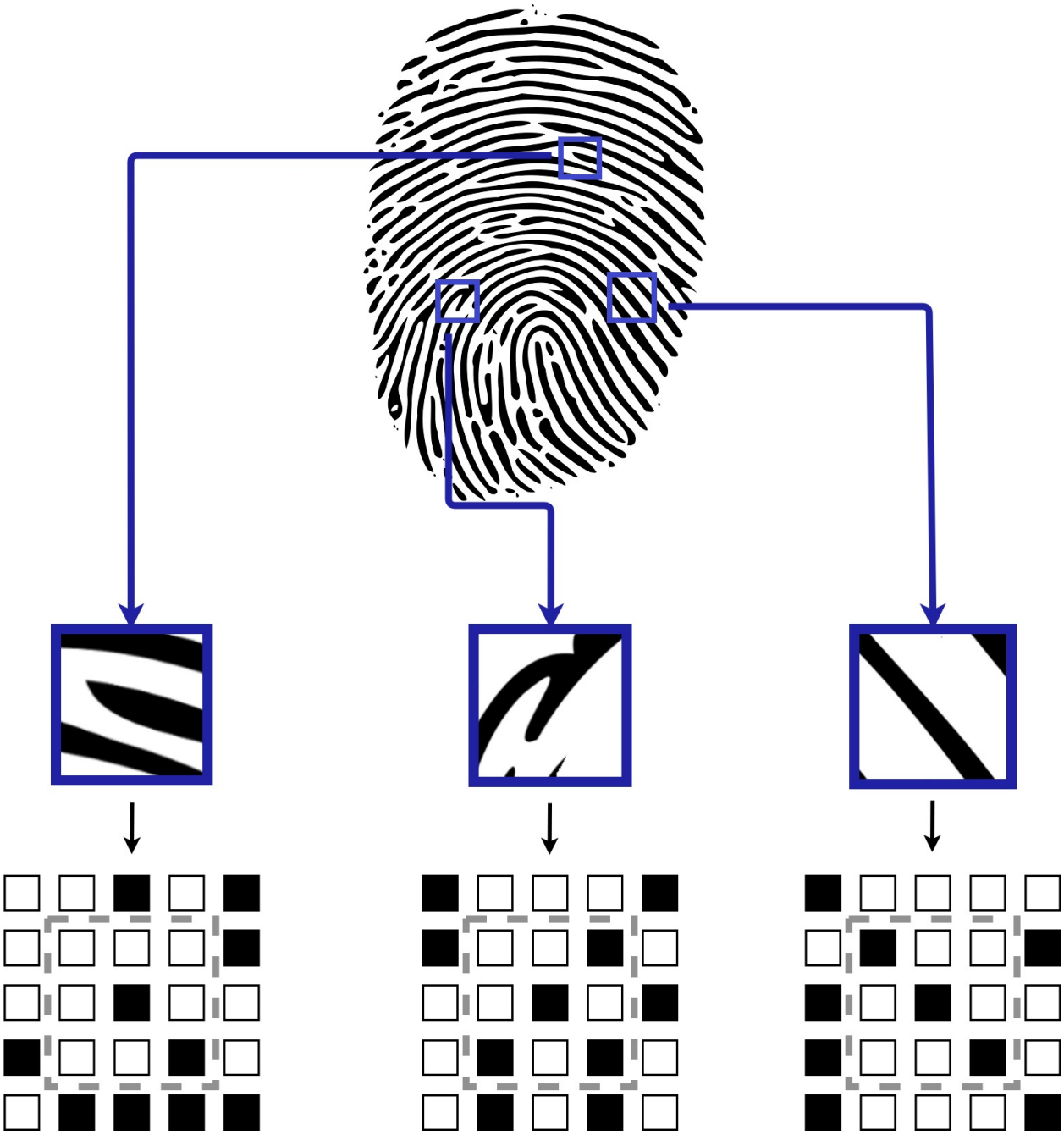


Figure 4.5: From left to right: Continuous ridge, ending ridge and bifurcation examples for minutiae detection and identification.

This process is not implemented in the IMD. The stored fingerprint will be received after the processing of the scans. As for any future acquisition, it will be processed by auxiliary devices. Therefore, we have not accommodated this step for the IMD, as it is independent.

It is better that the IMD is not burdened by this processing scheme in its configuration.

4.3.4 Minutiae Matching

To match the fingerprint scanned with another one, the minutiae matching rate is the metric used to identify similarities between both. The first step before computing the matching rate is to align the fingerprints according to local minutiae structures. This improves the miscalculation due to the translation or the rotation of the fingers while acquiring the print. After the alignment, every two minutiae (each belongs to a different fingerprint) in a close location and orientation are paired together and are considered as a corresponding pair. The more corresponding pairs are between two fingerprints, the higher the matching score is. After a full analysis of the database and the scan quality, a threshold is set for the score to define the minimum score that needs to be obtained to consider both fingerprints as similar. Several algorithms exist in the literature that provide this step [70, 71, 72].

4.3.5 Scheme

Starting from the first use of the IMD implementing the security scheme presented in this work, the user will have his/her fingerprint stored in the device. This information will be used later for any authentication attempt to verify the identity of the person asking for the IMD access. This will be the first factor to enable the success of the authentication, the fingerprint of the requester must match the stored one. When the medical team arrives at the emergency location, it would know how to operate. A standardization of the scheme will be present. Identifying that the patient is equipped with an IMD, they will scan his/her finger to activate the authentication scheme. This will whether deactivate the IMD or give an authentication key for the medical team to operate the IMD. For each IMD, a specific case of study will be achieved to decide.

The second factor of this scheme is the instantaneous ECG signal, as shown in Section 4.2. The user will start by recording the ECG signal information to generate the first needed

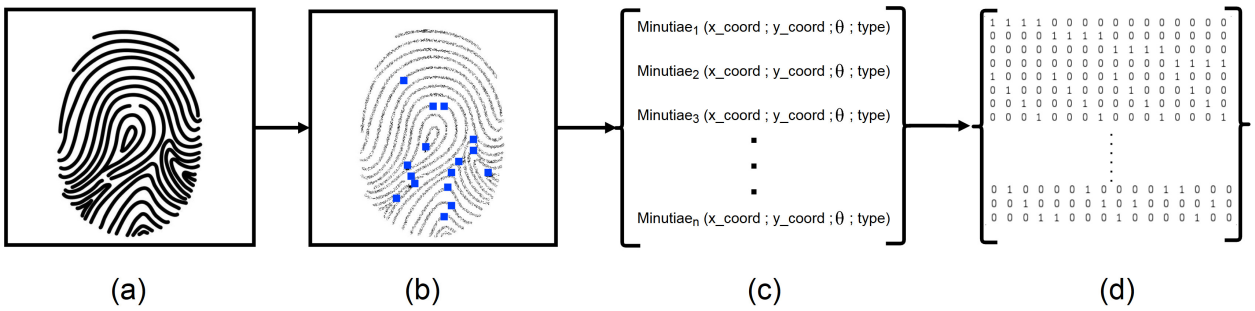


Figure 4.6: Fingerprint Scan Transformation Process. (a) Scan acquisition. (b) Minutiae Identification. (c) Minutiae Characteristics Matrix. (d) Binary Form of the Minutiae Characteristics Matrix Encoded with Hadamard.

sequence. This sequence is established as explained in Section 4.2.4. Once it is computed, it will be encoded according to a Hadamard encoder [73]. The use of this encoder is for the purpose of extending the size of the previous input to match relatively the data format of the fingerprint reading. For the fingerprint reading, the minutiae characteristics will undergo a second encoding scheme to form a binary matrix detailing the features of the scanned fingerprint. Fig. 4.6 represents the transformation process that a fingerprint scan undergoes through our protocol. Once achieved, the scheme will possess two sequences generated from the two different biometric readings, as shown in Fig. 4.7. Both outputs will contain the singularities of each biometric. They join afterward in a summation function (XOR function as an example to lower the complexity) to form the authentication key. The use of this simple function is to guarantee the non-waste of the hardware resources of the IMD. More sophisticated IMDs can rely on two-way deterministic functions. This key is to be sent to the IMD to request access. A public share of this key is permitted as it is considered as a token of the medical team. Replay attacks are prevented using this procedure. As it will be proven in Section 4.5, ECG readings are equivalent to a random process. Hence, the fingerprint cannot be identified nor the key cannot be replayed in a future time. The ECG reading result would expire by the next attempt.

The IMD will receive a request to operate the emergency authentication scheme. It will be informed that the patient is in a critical situation and will accept to process the

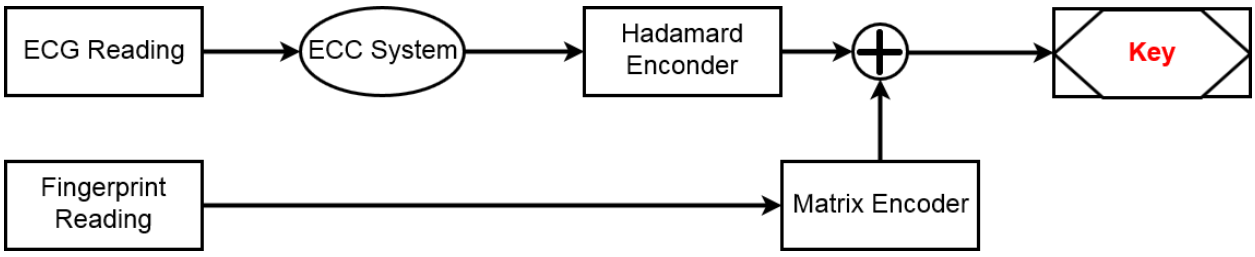


Figure 4.7: Sender's Key Generation Scheme using ECG and Fingerprint Readings.

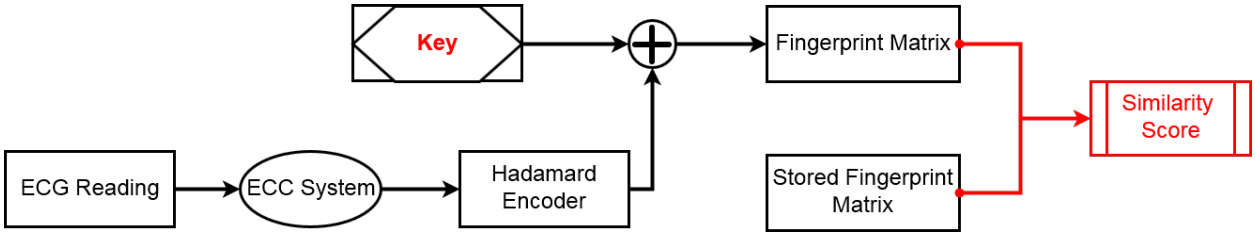


Figure 4.8: Receiver's Key Decoding Scheme using ECG and Fingerprint Readings..

authentication request. In case of any malicious manipulation of this backdoor, it can alert the user to verify his surroundings. After processing the key, as explained in Fig. 4.8, the fingerprint matrix can be extracted. The result will be in a form of a binary matrix containing the minutiae features of the scanned fingerprint. This matrix will be compared to the one stored within the IMD to verify if the sender is an authorized user that has just scanned the patient's finger. If the matching score is higher than a given threshold, the sender is granted the IMD access.

4.3.6 Similarity Score Computation

The similarity score of the fingerprints is based on the ratio of the matching minutiae between both fingerprints and the total number of identified minutiae. After the alignment of the fingerprint, two minutiae from the same type are considered similar if they have the same spatial coordinates and the same orientation. If we consider that a given minutiae is represented by (x, y) spatial coordinates and an angle θ, two minutiae are similar if:

- They both belong to the same type of minutiae τ.

- $$\begin{cases} \sqrt{\Delta x^2 + \Delta y^2} \leq D_{th} \\ \\ \min(|\Delta\theta|, 2\pi - |\Delta\theta|) \leq \theta_{th} \end{cases} \tag{4.5}$$

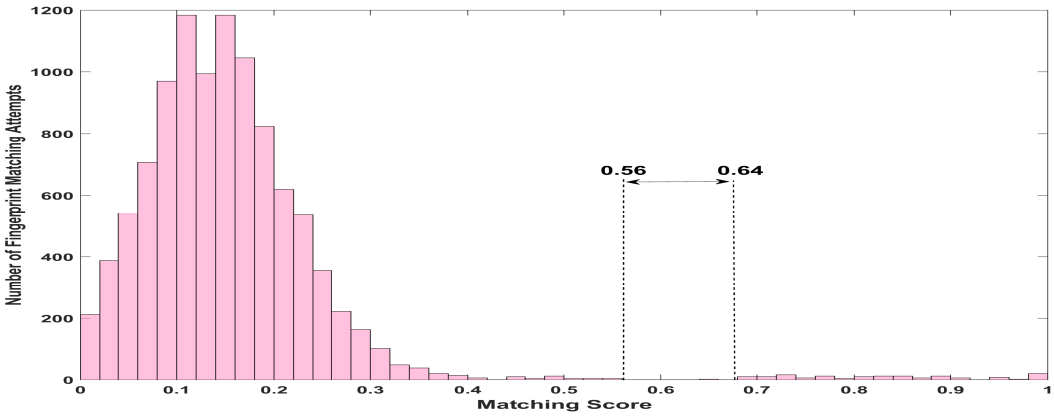


Figure 4.9: Histogram of the matching scores of different fingerprint matching attempts.

with Δx, Δy and $\Delta\theta$ being the difference between the x-coordinate, y-coordinate and the orientation of the minutiae, respectively.

In order to compare two fingerprint scans F_α and F_β, the scan will be locally aligned. We define a minutiae point i by the vector $M_i = (x_i, y_i, \theta_i, \tau_i)^T$. A fingerprint scan contains N minutiae points. A set of random $\Upsilon = \{i \ / \ i \in \text{Minutiae points set}\}$ is defined with cardinality $0.25 \times N$. The factor $N_f = 0.25$ was chosen after statistical test for giving the best score close to the score of the fingerprint matching if all minutiae points were considered. Fig. 4.10 shows the average effect of N_f variation on the accuracy of the matching score of fingerprints belonging to the same person. We define $Ng(i)$ the minutiae points in the same spatial circle of radius r and center (x_i, y_i). Now for each $(i, j) \in \{\Upsilon_\alpha \times \Upsilon_\beta \ / i \in$

$Ng(j)$ and M_i similar to $M_j\}$:

$$\begin{cases} dx = x_j - x_i \\ dy = y_j - y_i \\ d\theta = min(|\theta_j - \theta_i|, 360 - |\theta_j - \theta_i|) \end{cases} \tag{4.6}$$

Then according to (dx, dy), F_β will translated so that $(dx, dy) = (0, 0)$; and according to $d\theta$, F_β will rotated so that $d\theta = 0$. We call the result of the latter F'_β.
The algorithm will compute the number η_i of similar minutiae between F_α and F'_β according to the thresholds $(\Delta x,\ \Delta y, \Delta\theta)$. The final local score is:

$$S = \frac{\eta_i^2}{|\Upsilon_\alpha| \times |\Upsilon_\beta|} \tag{4.7}$$

The final score will be the highest η_i.

Fig. 4.9 shows the resulting score of matching different fingerprints. These fingerprints were collected through different databases [80] that offer fingerprint scans for different individuals and different scans for the same individual, to allow a better analysis of the fingerprint algorithms. To enhance the data, the scans originiating from the same individual were multiplied by inducing several modification to the original sample, e.g., cropping, rotation, blurring. This histogram shows clearly a gap between the scores resulted from comparing different individuals' fingerprints and from comparing different scans of the same individual's fingerprint. This can easily clear the choice of the threshold to be defined for the protocol to conclude from the computed score if the fingerprints belong to the same person or not.

4.4 Security Analysis

The IMD is threatened from two different types of attackers: passive and active. Emergency situations represent an advantage for attackers to launch their attacks. Most of IMDs, with

their simple resources, will simply stop working or open its access to the environment under such circumstances. This is due to the fact that an abnormality in the user's health had happened and the IMD may behave as an obstacle for urgent interventions. This can easily be the opportunity for attackers to hijack the disregarded IMD. Our scheme focuses well on this scenario and offers access to any foreign medical team to control the IMD while the user is unconscious. At the same time, this same scheme can be used in general situations for authentication needs to avoid any waste of resources. The wireless exchange of the generated key prevents any kind of Man-In-The-Middle attacks. The ECG reading plays the role of an expirable token that makes the key expirable for Replay attacks. The combination of both biometric prevents any spoofing, phishing and jamming attacks. Packet sniffing is shown through the results presented in the following section to be uninformative to eavesdroppers. This was mainly enhanced by introducing the properties of ECC systems. This scheme helps any new medical staff to access the IMD to take the needed actions while ensuring that no other malicious party can take place in the communication. If the emergency access was triggered under a regular scenario, the IMD can inform the user and he/she will take the necessary precautions. Also, an abnormality detection scheme [75] can be used to detect emergency situations and when the authentication can take place. In a more general context, the user can trigger this mechanism to authenticate a new doctor too.

Among the problems an IMD can face, are the regulatory authorities [76], e.g., the US Food and Drug Administration (FDA). Such authorities must ensure the safety and security of medical devices designed for commercial use. For this reason, the FDA has placed the responsibility for the device's security issues with the medical product manufacturer. They published for this matter premarket [77] and postmarket guidelines [78]. These guidelines englobe the management procedure of medical device cybersecurity risks throughout the product life cycle. As the scheme provided through this work has no reason to be constantly updated, regulations should not be a major issue. Basically, FDA has concerns for security patches and update plans for security reason. This work has shown that once it is designed

within the IMD's scheme, it is functional against most of the possible malicious attacks. Additionally, the security scheme is shown effective from the design scheme.

4.5 Results

4.5.1 One-Factor Scheme

Randomness tests

To guarantee that the generated binary sequences from the ECG instantaneous readings are truly random, we have used the National Institute of Standards and Technology (NIST) [42] statistical test suite. The results are shown in Table 4.2.

Table 4.2: Results of Randomness Tests Applied on Multiple Sequence Generations

Randomness Test	**Success Rate**
Monobit Test	89%
Frequency Test	100%
Runs Test	96%
DFT	100%

Furthermore, we have analyzed the generated sequences from the ECG readings for patterns consisting of multiple bits. This ensures that eavesdropped sequences are not threatened by statistical attacks. We have tested for every different bit configuration its occurrence probability in the sequence. Fig. 4.11 shows the average probability of a bit sequence with a given length to appear in a generated bit chain from ECG readings. The figure features also the probability deviation of the most probable sequence and the least probable sequence. We can observe well the deviation is very small. This ensures that there can be no pattern to be detected in any generated sequence to help the attacker to predict any future generated sequence.

FAR-FRR

The False Acceptance Rate (FAR) [79], exhibits the possibility that the security system will mistakenly accept an authentication attempt from an unauthorized user. It is defined as follow:

$$FAR = \frac{Number\ of\ false\ acceptance\ trials}{Total\ number\ of\ authentication\ attempts} \tag{4.8}$$

The False Recognition Rate (FRR) [79], displays the possibility that the security system will falsely reject an authentication attempt by an authorized user. It is defined as follow:

$$FRR = \frac{Number\ of\ false\ recognition\ trials}{Total\ number\ of\ authentication\ attempts} \tag{4.9}$$

The results are shown in Table 4.3. The analysis have been run through different data segments extracted the ECG recordings offered by PhysioNet [74] database. This database offers several physiologic signals for academic use by the biomedical research community. For ECG signals, they offer python and MatLab libraries to thoroughly investigate the recordings they have. The recording we have investigated are from different subjects. These subjects contain healthy persons along with few of them showing some dysfunctional heart activities. The subjects are from different age intervals too. Each data is linked to its origin through the analysis to keep track of right and false authentications.

Table 4.3: FAR & FRR Rates

Metric	**Rate**
FAR	0.9%
FRR	6.3%

4.5.2 Two-Factor Scheme

Formal Security Analysis

To present this protocol in a formal verification, we opted to use the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The AVISPA tool serves to verify the efficiency of a programmed cryptographic protocol [81] using High-Level Protocols Specification Language (HLPSL) [83]. This language assists the role of each participant in the given protocol; while defining all the significant scenarios of these participants in a role architecture. The role system contains a number of sessions, principals and roles. An intruder (I) in HLPSL is modeled according to the Dolev-Yao model [84] where I plays as an authentic role. Using different back-ends to analyze the protocol, the output of this tool generally contains:

- Summary section: It notifies whether the programmed protocol is safe, unsafe or unpredictable.
- Details section: It defines the conditions that have been considered during the analysis.
- Goal section: It designates the considered goals of the test.
- Back-end section: It declares the back-end name that has been used.
- Comments and Statistics section: It describes the trace of any present attack.

For our work, we have implemented three basic roles:

- Sensor: Defines the communication role of the sensor acquiring the ECG signal.
- Medical Team: Defines the intervening medical system.
- IMD: Defines the IMD from the patient's side.

The implementation covers the phase of sending the ECG signal from the sensor to the medical team and the parameters exchange between the IMD and the medical team to obtain the final secret key. The proposed protocol is simulated under the Constraint-Logic-based Attack Searcher (AtSe) back-end using the AVISPA web tool [81]. This back-end translates the protocol into a set of constraints to pinpoint the possible attacks on protocols [82]. The executability check has been well attained for this protocol. The execution of any protocol sometimes is incomplete. This is mainly due to some modeling errors. This gives erroneous simulation results and might give a false positive on the security of the protocol. That is why most consider the executability test as indispensable in AVISPA. This back-end checks if the legitimate agents in the protocol - which are in our case the medical team, the sensor and the IMD - can execute the specified protocol safely during the existence of an intruder. During this check, the AtSe verifies additionally the possibility of any Man-in-The-Middle attack by an intruder. The test result shown in Fig. 4.12, which ensures that the proposed protocol can defend replay attack.

Identification Rate

The histogram in Fig. 4.13 shows the matching score resulted by the authentication algorithm presented in this work. Different sample of fingerprints and ECG recording have been used, belonging to the same or different subjects. According to the data, any score higher than the value of 0.57 corresponds to a legitimate authentication request. Any score lower than the value of 0.5 corresponds to an illegitimate authentication request. The interval between these two values is where there is an overlap between legitimate and illegitimate requests. Therefore, the threshold upon which it is decided to grant access to the user will be within this interval. The decision of the exact value can be achieved statically while reviewing the FAR-FRR metrics that correspond to each threshold.

We have analyzed the FAR and the FRR metrics of this work's scheme to identify how reliable it is. Commonly, biometrics are very reliable to identify any identity. However,

when using low resources to analyze the data, the accuracy of the identification is not always ensured. Fig. 4.14 and Fig. 4.15 show the results of our analysis on the database we have collected. The database includes fingerprints and ECG readings of the same and different subjects. The data has been shuffled and processed through our protocol. Then we have compared the results of our algorithm with the actual identification result. We have introduced a sensitivity parameter to this algorithm. The lower this parameter is, the less accurate are the biometric readings. This sensitivity factor reflects the sophistication of the IMD in use. This helped to give more realistic results as inputs to our algorithm. The sensitivity parameter can affect the accuracy of the fingerprint scan or the precision of the ECG signal acquisition. We can see through the figures that the results are acceptable and promising for the success of the authentication request. Fig. 4.14 shows the Receiver Operating Characteristic (ROC) curves for different sensitivity levels. We can conclude from this how close the curve is to the upper-left corner that our work offers a good trade-off between the sensitivity and the specificity of the authentication algorithm. Fig. 4.15 demonstrates how statistically efficient can our algorithm be. It represents the statistical probability of the possible score of the authentication attempt of an imposter or a legitimate node. The figure shows two cases: The first one where the ECG corresponding input is discarded (Fingerprints only) and the second one featuring the complete algorithm. This figure shows the important contribution of the ECG corresponding input to the functionality of the algorithm.

4.6 Conclusion

In this section, we have investigated the security of Implantable Medical Devices (IMDs) from malicious attacks by providing a new backdoor scheme for any medical team to get involved in any emergency scenario. Authentication usually takes place between two previously identified parties. In emergency scenarios, this can be a problem as the IMD will refuse any sudden intervention. We have designed a backdoor to the IMD access while taking

into consideration that an attacker may take advantage of the scheme. We introduced first a one-factor authentication scheme. This scheme relies on instantaneous ECG readings to grant access to the new medical team. The ECG readings were enhanced with elliptic curve cryptography to provide more security for the patient. For more sophisticated IMDs, we have designed a two-factor authentication scheme. The latter relies on two different types of biometrics: The first is instantaneous and the second is fixed. We have evaluated the security this scheme can provide the IMD while ensuring it is hardware-friendly towards the limitations of any IMD. We concluded that the proposed system can be used by different kinds of implantable medical devices, and can ensure users' secure wireless communication even in emergency situations.

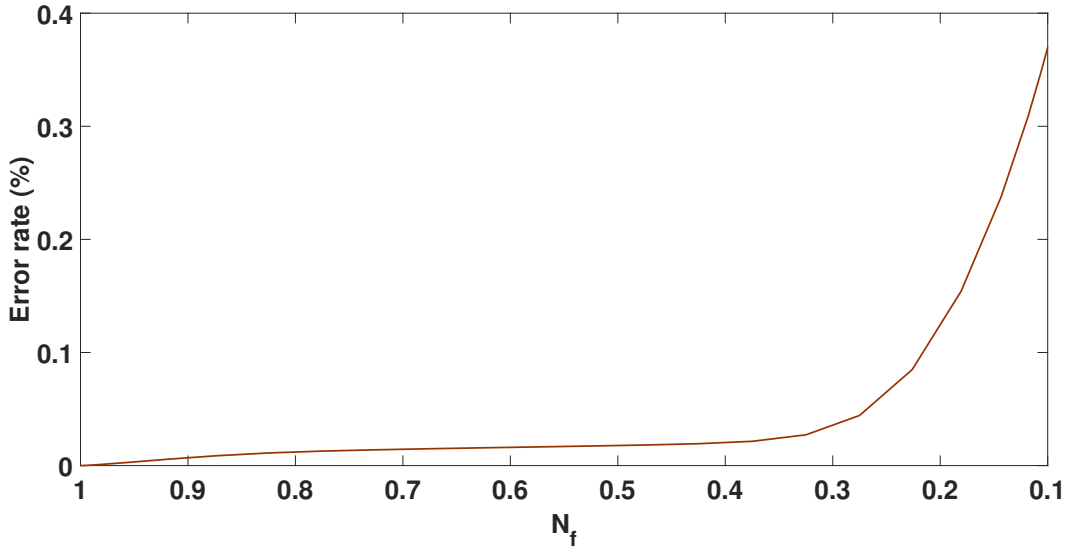


Figure 4.10: N_f Factor Average Effect on the Accuracy of the Matching Algorithm on the Same Person's Fingerprints

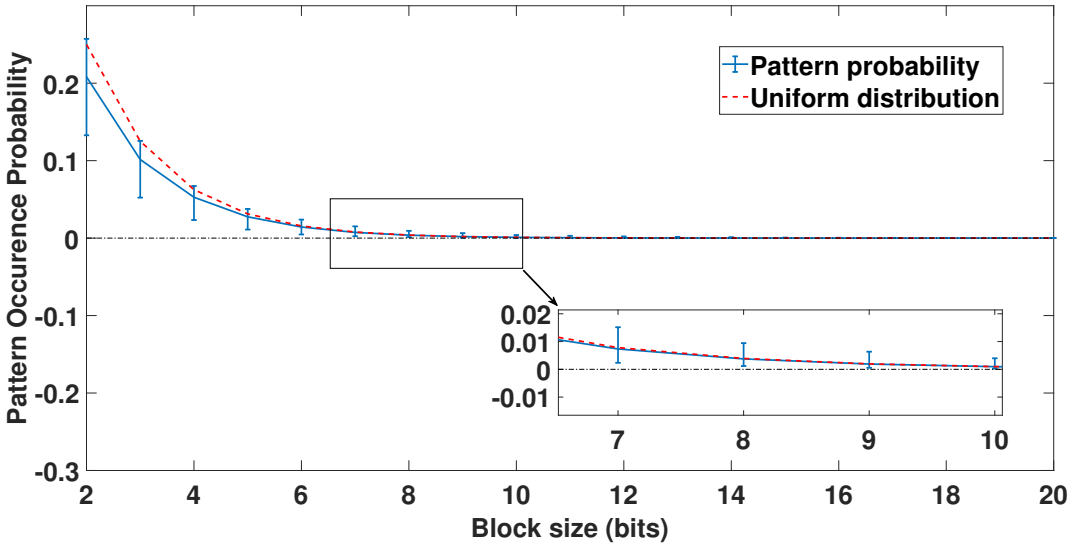


Figure 4.11: Occurrence Probability of Bit Sequences with a Pre-defined Length.

File

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL
  BOUNDED_SEARCH_DEPTH

PROTOCOL
  /home/span/span/testsuite/results/c3prot.if

GOAL
  As Specified

BACKEND
  CL-AtSe
```

Figure 4.12: Result of the AtSe Analysis.

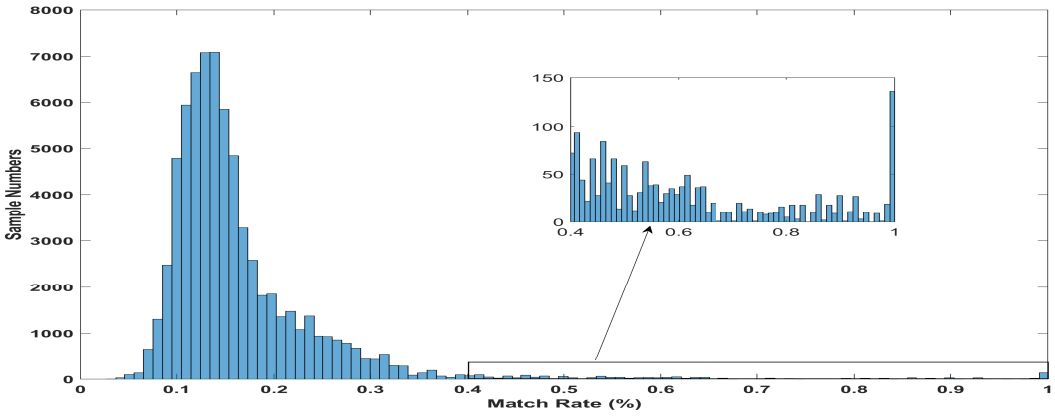


Figure 4.13: Histogram of the matching scores.

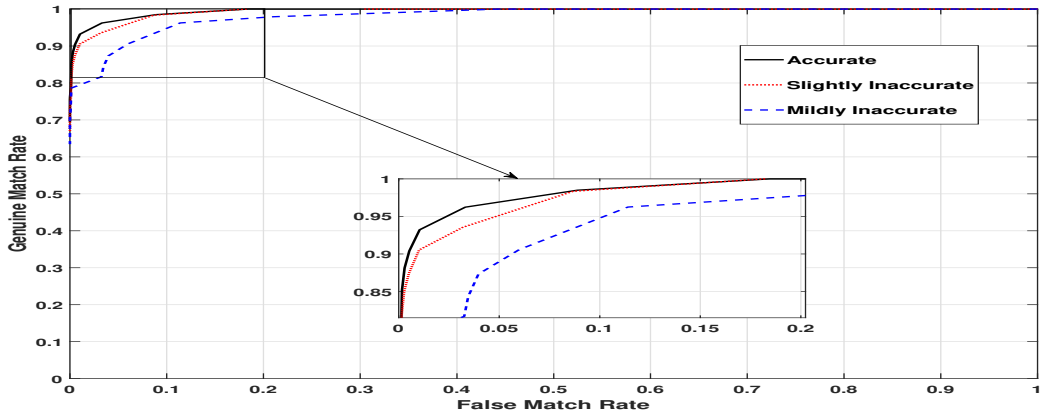


Figure 4.14: ROC curves evaluation of the proposed algorithm.

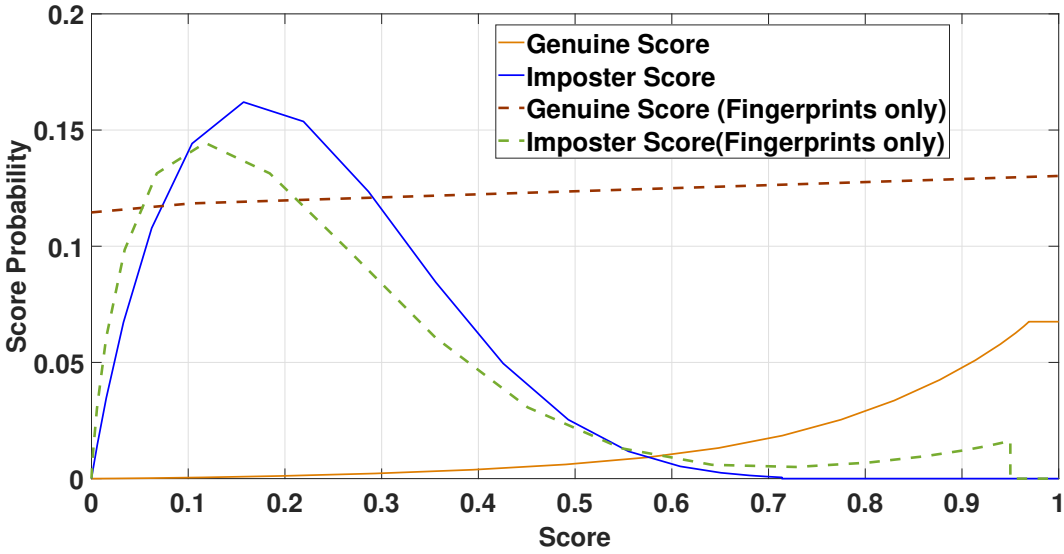


Figure 4.15: Distribution of the possible achieved scores by an imposter or a legitimate user authentication.

CHAPTER 5

Conclusion

In this Thesis, we have proposed some new schemes to defend Wireless Implantable Medical Devices (IMDs). Although the use of wireless technology is improving the remoteness and the efficiency of IMDs, it puts them in a huge security risk. This threatens both the safety and the privacy of the user. Any malicious attack on a medical device may hurt or even kill patients. Or it may also simply steal the patient's data, which is not tolerable as the data is very sensitive and private.

Regular security schemes are not always compatible. This is mainly due to the hardware constraints of IMDs (small CPU, Memory, Battery â) and that mainly these resources are dedicated to medical efficiency. Also, Wireless Sensor Networks schemes are incompatible on IMDs. This is due to the difference in energy use, node dispersion, fault toleranceâ

We have investigated in the second section the Insulin Pump device case, to analyze existing security and privacy issues. We have proposed a new authentication protocol to ensure the identity of the communicating parties. This protocol relied on plain text messages for communication, but immune to different malicious attacks that threaten the system. In chapter three, we have targeted Man-in-the-Middle (MITM) and replay attacks. To protect IMDs, we have proposed a defense mechanism is based on a chaotic generator for randomness purposes and on a signature algorithm to prevent any third party interference. We have tried to build a trust between communicating parties using a dynamic signature. In the fourth chapter, we have examined the security of IMDs during emergency situations. We have proposed a new backdoor scheme that any medical team can resolve the patient's issue under any emergency scenario. As the IMD may refuse any sudden intervention. We have designed an IMD access scheme that relies on biometrics for its proper working This scheme can use only one factor for the authentication scheme. It relies on instantaneous ECG readings to grant access to the new medical team. For the more sophisticated IMDs, the scheme can use two parameters for the authentication scheme: The first is instantaneous and the second is

fixed. We have chosen for the second factor to use fingerprint readings.

We have analyzed all these proposed schemes, and we have found that they have promising results to protect IMDs. We have evaluated their security performance while ensuring its hardware efficiency regarding IMDs. We concluded that any of the proposed schemes can be used by IMDs, and can ensure users' secure wireless communication while protecting them from intruders.

References

[1] Belkhouja T, Du X, Mohamed A, Al-Ali AK, Guizani M., New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control, **InGLOBECOM 2017-2017 IEEE Global Communications Conference 2017 Dec 4 (pp. 1-5). IEEE**.

[2] Belkhouja T, Mohamed A, Al-Ali AK, Du X, Guizani M., Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack, **In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 1-5). IEEE**.

[3] Belkhouja T, Mohamed A, Al-Ali AK, Du X, Guizani M., Salt Generation for Hashing Schemes based on ECG readings for Emergency Access to Implantable Medical Devices, **In2018 International Symposium on Networks, Computers and Communications (ISNCC) 2018 Jun 19 (pp. 1-6). IEEE**.

[4] Belkhouja T, Du X, Mohamed A, Al-Ali AK, Guizani M., Biometric-based authentication scheme for Implantable Medical Devices during emergency situations, **Future Generation Computer Systems. 2019 Feb 8**.

[5] Medfusion 4000 Wireless Syringe Infusion Pump, http://www.smithsmedical.com/catalog/syringe-pump/medfusion-4000-syringe-pump/medfusion-4000-wireless-syringe.html.

[6] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, Security and Privacy for Implantable Medical Devices, **IEEE Pervasive Computing, Special Issue on Implantable Electronics, Jan. 2008**.

[7] D. Halperin,T. S. Heydt-Benjamin,B. Ransford,S. S. Clark,B. Defend,W. Morgan,K. Fu,T. Kohno,W. H. Maisel, Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, **Proceedings of the 29th Annual IEEE Symposium on Security and Privacy, May 2008**.

[8] S. Gollakota, H. Hassanieh, B. Ransford, D. Dina, K. Kevin, They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices, **Proc. ACM SIGCOMM, 2011**.

[9] F. Xu, Z. Qin, C. C. Tan,B. Wang, Q. Li, IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian, **Proc. IEEE INFOCOM, 2011**.

[10] E. Marin, D. SingelÃ©e, B. Yang, I. Verbauwhede, B. Preneel, On the Feasibility of Cryptography for a Wireless Insulin Pump System, **Proc. CODASPY 2016**.

[11] C. Li, A. Raghunathan, N. K. Jha, Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System, **IEEE 13th International Conference on e-Health Networking, Applications and Services, 2011**.

[12] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, **August , 2001**.

[13] X. Hei, X. Du, S. Lin, I. Lee, PIPAC: Patient Infusion Pattern based Access Control Scheme for Wireless Insulin Pump System, **in Proc. of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013**.

[14] X. Hei, X. Du, J. Wu, F. Hu, Defending Resource Depletion Attacks on Implantable Medical Devices, **n Proc. of IEEE GLOBECOM 2010, Miami, Florida, USA, Dec. 2010**.

[15] Y. Liu, J. Li, M. Guizani, Lightweight Secure Global Time Synchronization for Wireless Sensor Networks, **IEEE Wireless Communications and Networking Conference (WCNC), 2012**.

[16] S. Liang, and X. Du, Permission-Combination-based Scheme for Android Mobile Malware Detection, **in Proc. of IEEE ICC 2014, Sydney, Australia, June 2014**.

[17] D. He, S. Chan, M. Guizani, Mobile application security: malware threats and defenses, **IEEE Wireless Communications, 2015**.

[18] D. He, S. Chan, M. Guizani, Handover authentication for mobile networks: security and efficiency aspects, **IEEE Network, 2015**.

[19] X. Hei and X. Du, Biometric-based two-level secure access control for implantable medical devices during emergencies, **IEEE INFOCOM, 2011**.

[20] M. Rostami, A. Juels, F. Koushanfar, Heart-to-Heart (H2H): Authentication for Implanted Medical Devices, **Proc. ACM SIGSAC, 2013**.

[21] N. Ferguson, B. Schneier T. Kohno, Cryptography Engineering, **ch11, Oct. 2015**.

[22] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha, A. Raghunathan, Vibration-based secure side channel for medical devices, **Proc. Annual Design Automation Conference, 2015**.

[23] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin,S. Capkun, Proximity-based access control for implantable medical devices, **Proc. Computer and communications security, 2009**.

[24] S. Y. Chang, Y. C. Hu, H. Anderson, T. Fu, E. Y. L. Huang, Body area network security: robust key establishment using human body channel, **Proc. USENIX Conference on Health Security and Privacy, 2012**.

[25] D. E. Denning: Information warfare and security, **Addison-Wesley, December 1998**.

[26] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, A Review of Security Challenges, Attacks and Resolutions for Wireless Medical Devices, **Wireless Communications and Mobile Computing Conference (IWCMC), 2017**.

[27] L. Wu, X. Du, M. Guizani, and A. Mohamed, Access Control Schemes for Implantable Medical Devices: A Survey, **IEEE Internet of Things Journal, May 2017**.

[28] P. Kumar and H. J. Lee, Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, **Sensors, 2012**.

[29] X. Du, M. Guizani, Y. Xiao, H. H. Chen" A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks, **IEEE Transactions on Wireless Communications, March, 2009**.

[30] M. Zhang, A. Raghunathan, N. K. Jha : MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection, **IEEE Transactions on Biomedical Circuits and Systems, December 2013**.

[31] S. Vaudenay: A classical introduction to cryptography, **September 2005**

[32] Y. W. Law, M. Palaniswami, L. Van Hoesel,J. Doumen, P. Hartel, P. Havinga, Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols, **ACM Transactions on Sensor Networks, February 2009**.

[33] K.M. Short, Unmasking a modulated chaotic communications scheme, **International Journal Bifurcat Chaos, 1995**.

[34] H. Richter, The generalized Henon maps: Examples for higher-dimensional chaos, **International Journal of Bifurcation and Chaos, June 2002**.

[35] H. J. Li, J. L. Chern: Coding the chaos in a semiconductor diode for information transmission, **Physics Letters A, August 1995**.

[36] Y. H. Yu, K. Kwak, T. K. Lim: Secure communication using small time continuous feedback, **Physics Letters A, January 1995**.

[37] H.H. Nien, C.K. Huang, S.K. Changchien, H.W. Shieh, C.T. Chen, Y.Y. Tuan: Digital color image encoding and decoding using a novel chaotic random generator, **Chaos, Solitons and Fractals, November 2005**.

[38] W. F. H. Al-Shameri, Dynamical Properties of the HÃ©non Mapping, **International Journal of Math. Analysis, Vol. 6, 2012**.

[39] M. Henon, A Two-Dimensional Mapping with a Strange Attractor, **Communications in Mathematical Physics, 1976**.

[40] C. Beierle, P. Jovanovic, M. M. Lauridsen, G. Leander, and C. Rechberger, Analyzing Permutations for AES-like Ciphers: Understanding Shift Rows, **Conference: Topics in Cryptology - CT-RSA 2015**.

[41] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, W. H. Maisel: Security and Privacy for Implantable Medical Devices, **IEEE Pervasive Computing, January 2008**.

[42] National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, **April, 2010**.

[43] IEEE P802.15 Working Group for WPANs, Channel Model for Body Area Network (BAN), **April, 2009**.

[44] Xilinx, Spartan-6 Family Overview, **Xilinx, 2011**.

[45] Xilinx, ISim User Guide, **April, 2012**.

[46] J. Ray, P. Koopman: Efficient High Hamming Distance CRCs for Embedded Networks,**Dependable Systems and Networks, 2006**.

[47] National Institute of Standards and Technology: The Keved-Hash Message Authentication Code, **Federal Information Processing Standards Publication, 2001**.

[48] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian", **in Proc. IEEE INFOCOM**, Apr. 2011, pp. 1862â1870.

[49] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices", **In Proc. of Computer and communications security**, pages 410â419, 2009.

[50] Marin, D. Singele, B. Yang, I. Verbauwhede, B. Preneel, "On the Feasibility of Cryptography for a Wireless Insulin Pump System", **Proc. CODASPY 2016**.

[51] Guanglou Zheng, Gengfa Fang, Rajan Shankaran, Mehmet A. Orgun, "An Improved Binary Sequence Generation for Securing Wireless Body Area Networks", **Data Science and Data Intensive Systems (DSDIS) 2015 IEEE International Conference, pp. 734-735, 2015**.

[52] Ankarali ZE, Demir AF, Qaraqe M, Abbasi QH, Serpedin E, Arslan H, Gitlin RD.: Physical layer security for wireless implantable medical devices. **In Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on 2015 Sep 7 (pp. 144-147). IEEE.**

[53] Kim Y, Lee WS, Raghunathan V, Jha NK, Raghunathan A.: Vibration-based secure side channel for medical devices. **In Proceedings of the 52nd Annual Design Automation Conference 2015 Jun 7 (p. 32). ACM.**

[54] Long WJ, Lin W.: An authentication protocol for wearable medical devices. **In Emerging Technologies for a Smarter World (CEWIT), 2017 13th International Conference and Expo on 2017 Nov 7 (pp. 1-5). IEEE.**

[55] Chi H, Wu L, Du X, Zeng Q, Ratazzi P. e-SAFE: Secure, Efficient and Forensics-Enabled Access to Implantable Medical Devices. **arXiv preprint arXiv:1804.02447. 2018 Apr 6.**

[56] Tams B, MihÄilescu P, Munk A.: Security considerations in minutiae-based fuzzy vaults. **IEEE Transactions on Information Forensics and Security. 2015 May;10(5):985-98**.

[57] Li C, Hu J.: A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures. **IEEE Transactions on Information Forensics and Security. 2016 Mar;11(3):543-55**.

[58] Chavan S, Mundada P, Pal D.: Fingerprint authentication using Gabor filter based matching algorithm. **In Technologies for Sustainable Development (ICTSD), 2015 International Conference on 2015 Feb 4 (pp. 1-6). IEEE**.

[59] Yuan C, Sun X, Lv R.: Fingerprint liveness detection based on multi-scale LPQ and PCA. **China Communications. 2016 Jul;13(7):60-5**.

[60] Jin Z, Lim MH, Teoh AB, Goi BM, Tay YH.: Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication. **IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2016 Oct;46(10):1415-28**.

[61] R. Gupta, M. Mitra, J. Bera: ECG Acquisition and Automated Remote Processing, **Springer India, 2014.**

[62] V. Miller: Uses of elliptic curves in cryptography, **In Advances in Cryptology, Crypto 85, Springer Verlag LNCS 218, 417-426, 1986.**

[63] N. Koblitz. Elliptic curve cryptosystems, **Math. Comp., 48, 203-209, 1987**

[64] K. Lauter: The advantages of elliptic curve cryptography for wireless security, **IEEE Wireless Communications, Volume: 11, Issue: 1, Feb 2004.**

[65] Kapoor V, Abraham VS, Singh R.: Elliptic curve cryptography. **Ubiquity. 2008 May 1;2008(May):7**.

[66] D. B. Smith, D. Miniutti, T. A. Lamahewa, L. W. Hanlen : Propagation Models for Body-Area Networks: A Survey and New Outlook, **IEEE Antennas and Propagation Magazine, Vol. 55, No. 5, October 2013.**

[67] Martin M, Å tefan K, L'ubor F.: Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino. **TELKOMNIKA. 2018 Apr 1;16(2):755-65**.

[68] D. Chek Ling Ngo, A. Beng Jin Teoh, J. Hu: Biometric Security. **Cambridge Scholars Publishing, ISBN (10): 1-4438-7183-4, 2015**.

[69] T. M. Khan, D. G. Bailey, M. A. U. Khan, and Y. Kong.: Efficient hardware implementation strategy for local normalization of fingerprint images. **J. Real-Time Image Process., vol. 1, pp. 1â13, Jul. 2016**.

[70] Lee W, Cho S, Choi H, Kim J.: Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners. **Expert Systems with Applications. 2017 Nov 30;87:183-98**.

[71] Tran MH, Duong TN, Nguyen DM, Dang QH.: A local feature vector for an adaptive hybrid fingerprint matcher. **In Information and Communications (ICIC), 2017 International Conference on 2017 Jun 26 (pp. 249-253). IEEE**.

[72] Ali MM, Mahale VH, Yannawar P, Gaikwad AT.: Fingerprint recognition for person identification and verification based on minutiae matching. **In Advanced Computing (IACC), 2016 IEEE 6th International Conference on 2016 Feb 27 (pp. 332-339). IEEE**.

[73] Hadi A, Alsusa E: On the application of the fast Hadamard transform in Polar codes. **In Signal Processing Advances in Wireless Communications (SPAWC), 2016 IEEE 17th International Workshop on 2016 Jul 3 (pp. 1-5). IEEE**.

[74] PhysioBank Databse, https://physionet.org/physiobank/, **2016.**

[75] Rathore H, Al-Ali A, Mohamed A, Du X, Guizani M. DLRT: Deep Learning Approach for Reliable Diabetic Treatment. **InGLOBECOM 2017-2017 IEEE Global Communications Conference 2017 Dec 4 (pp. 1-6). IEEE.**

[76] Williams PA, Woodward AJ.: Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. **Medical Devices (Auckland, NZ). 2015;8:305.**

[77] US Food and Drug Administration, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff. **2014.**

[78] US Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff Additional Copies. **2016.**

[79] M. E. Schuckers: Computational Methods in Biometric Authentication, **Information Science and Statistics, Springer-Verlag London Limited, 2010.**

[80] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano and J. Gonzalez-Rodriguez: BioSec baseline corpus: A multimodal biometric database. **Pattern Recognition, Vol. 40, n. 4, pp. 1389-1392, April 2007**.

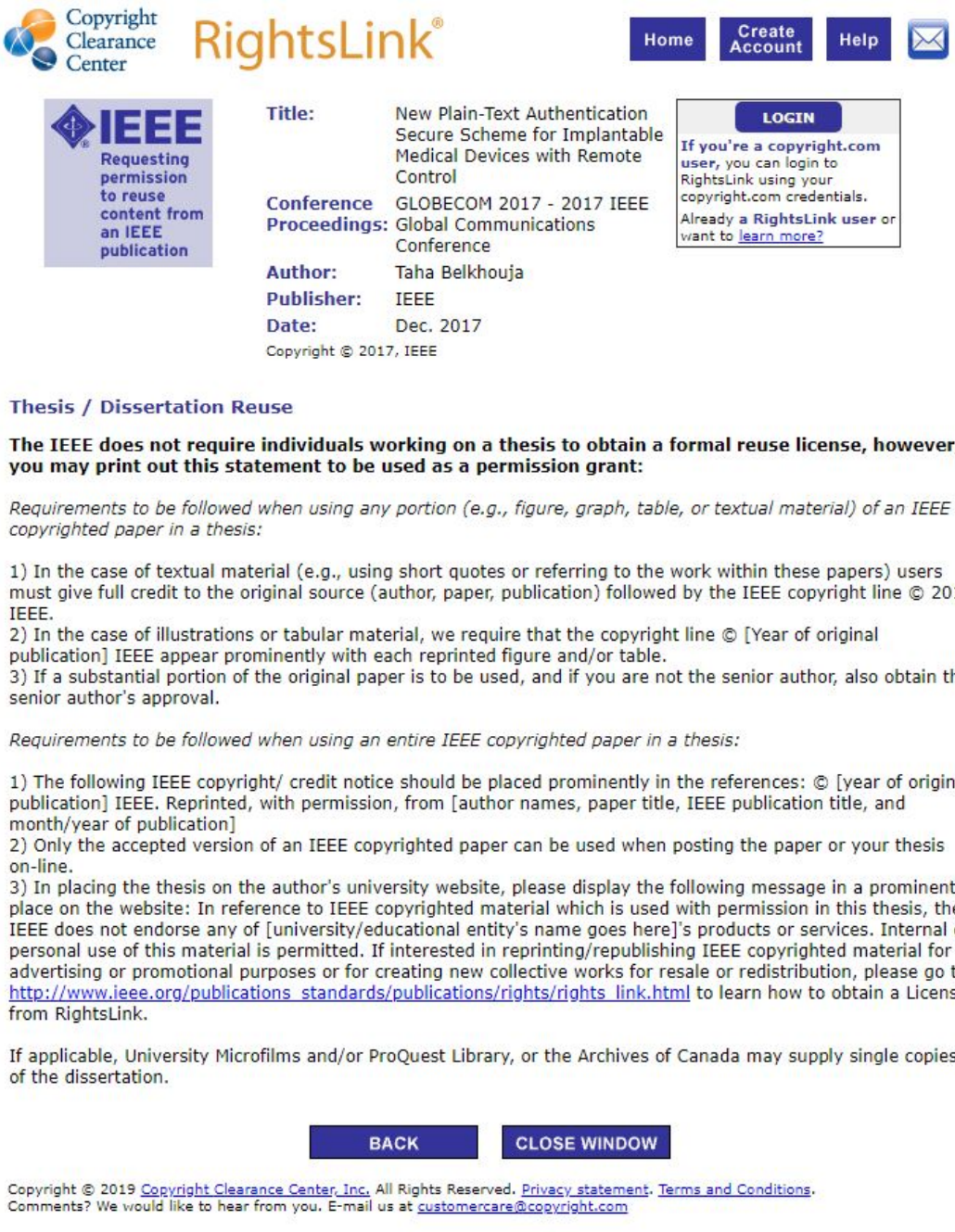
[81] Vigano L.: Automated security protocol analysis with the AVISPA tool. **Electronic Notes in Theoretical Computer Science. 2006 May 12;155:61-86**.

[82] AVISPA Team. AVISPA v1. 1 user manual: http://avispa-project. org/package/user-manual. pdf. **2006 Jun**.

[83] von Oheimb D.: The high-level protocol specification language HLPSL developed in the EU project AVISPA. **In Proceedings of APPSEM 2005 workshop 2005 Sep 13 (pp. 1-17)**.

[84] Backes M, Pfitzmann B.: Symmetric encryption in a simulatable Dolev-Yao style cryptographic library. **In null 2004 Jun 28 (p. 204). IEEE**.

Appendix A: IEEE Copyright Permission



Copyright Clearance Center RightsLink®

Home | Create Account | Help

IEEE Requesting permission to reuse content from an IEEE publication

Title: New Plain-Text Authentication Secure Scheme for Implantable Medical Devices with Remote Control

Conference Proceedings: GLOBECOM 2017 - 2017 IEEE Global Communications Conference

Author: Taha Belkhouja

Publisher: IEEE

Date: Dec. 2017

Copyright © 2017, IEEE

LOGIN

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.

Already a RightsLink user or want to learn more?

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK | CLOSE WINDOW

Copyright © 2019 Copyright Clearance Center, Inc. All Rights Reserved. Privacy statement. Terms and Conditions.
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

Appendix B: IEEE Copyright Permission

Copyright Clearance Center RightsLink®

Home | Create Account | Help

IEEE Requesting permission to reuse content from an IEEE publication

Title:	Light-Weight Solution to Defend Implantable Medical Devices against Man-In-The-Middle Attack
Conference Proceedings:	2018 IEEE Global Communications Conference (GLOBECOM)
Author:	Taha Belkhouja
Publisher:	IEEE
Date:	Dec. 2018

Copyright © 2018, IEEE

LOGIN

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.

Already a RightsLink user or want to learn more?

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

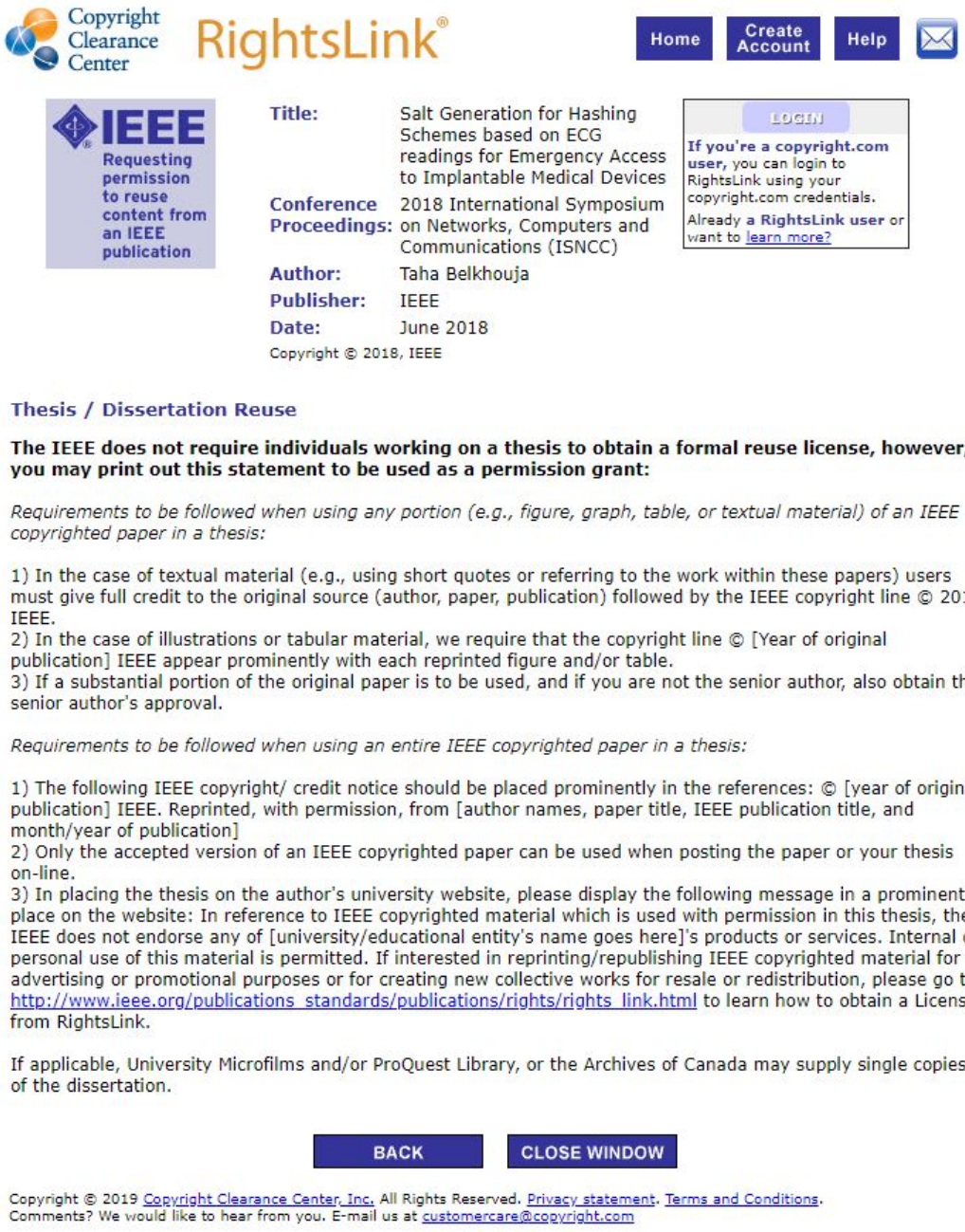
1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK | CLOSE WINDOW

Copyright © 2019 Copyright Clearance Center, Inc. All Rights Reserved. Privacy statement. Terms and Conditions.
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

Appendix C: IEEE Copyright Permisson



Copyright Clearance Center RightsLink®

Home | Create Account | Help

IEEE Requesting permission to reuse content from an IEEE publication

Title: Salt Generation for Hashing Schemes based on ECG readings for Emergency Access to Implantable Medical Devices

Conference Proceedings: 2018 International Symposium on Networks, Computers and Communications (ISNCC)

Author: Taha Belkhouja

Publisher: IEEE

Date: June 2018

Copyright © 2018, IEEE

LOGIN

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.

Already a RightsLink user or want to learn more?

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK | CLOSE WINDOW

Copyright © 2019 Copyright Clearance Center, Inc. All Rights Reserved. Privacy statement. Terms and Conditions.
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

Appendix D: Elsevier Copyright Permission

Copyright Clearance Center RightsLink®

Home | Create Account | Help

Title: Biometric-based authentication scheme for Implantable Medical Devices during emergency situations

Author: Taha Belkhouja,Xiaojiang Du,Amr Mohamed,Abdulla K. Al-Ali,Mohsen Guizani

Publication: Future Generation Computer Systems

Publisher: Elsevier

Date: September 2019

© 2019 Elsevier B.V. All rights reserved.

LOGIN

If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials.

Already a RightsLink user or want to learn more?

Please note that, as the author of this Elsevier article, you retain the right to include it in a thesis or dissertation, provided it is not published commercially. Permission is not required, but please ensure that you reference the journal as the original source. For more information on this and on your other retained rights, please visit: https://www.elsevier.com/about/our-business/policies/copyright#Author-rights

BACK | CLOSE WINDOW

Copyright © 2019 Copyright Clearance Center, Inc. All Rights Reserved. Privacy statement. Terms and Conditions.
Comments? We would like to hear from you. E-mail us at customercare@copyright.com