2025 19th International Symposium on Medical Information and Communication Technology (ISMICT) | 979-8-3315-2548-4/25/$31.00 ©2025 IEEE | DOI: 10.1109/ISMICT64722.2025.11059426

# Secret Key Extraction using Galvanic Coupling in Wireless Body Area Networks

Stefano Caputo[1], Anna Vizziello[2], Antonio Coviello[3], Maurizio Magarini[3], Sara Jayousi[4], Pietro Savazzi[2], and Lorenzo Mucchi[1]

[1]Dept. of Information Engineering, University of Florence, Italy
Email: {name.surname}@unifi.it
[2]Dept. of Electronics, Computer and Biomedical Engineering, University of Pavia, Italy
Email: name.surname@unipv.it
[3]Dept. of Electronics, Information and Bioengineering, Politecnico di Milano, Italy
Email: {name.surname}@polimi.it
[4]Prato Campus, University of Florence, Italy
Email: {name.surname}@pin.unifi.it

***Abstract*—The evolution of wearable medical devices has made it essential to ensure not only efficient but also secure communication within wireless Body Area Networks (WBANs). Traditional wireless radio frequency transmission methods suffer from limitations in terms of security. Symmetric encryption is recognized to be a solution to provide security to low-resourced on-body devices, but it suffers from the problem of secret key distribution/sharing. Physical-layer security provides a solution to this issue by using the key agreement method: extracting the key from body signals. Anyway, many body signals are not easy to be extracted or processed. In this context, on-body communication via Galvanic coupling (GC) represents a promising alternative, leveraging the conduction of electrical signals through biological tissues to limit eavesdropping and reduce complexity, including energy consumption. This work proposes an innovative method for secret key extraction based on the reciprocity of GC channels. Two on-body devices can dynamically generate shared cryptographic keys, ensuring a secure communication channel without the need to transmit keys that could be vulnerable to attacks. Through an experimental analysis conducted on human subjects, we demonstrate the feasibility and security of this method, highlighting how the characteristics of a GC-based approach prevent an external attacker from reconstructing the key.**

***Index Terms*—Wireless Body Area Networks, On-body Communications, Galvanic Coupling (GC), Secret Key Extraction.**

## I. Introduction

Next-generation wearable medical devices are transforming modern healthcare by enabling continuous monitoring, targeted treatment, and more effective rehabilitation. These devices play a crucial role in treating conditions such as cardiovascular diseases, motor disorders, and chronic pain. However, ensuring secure and efficient communication between them remains a critical challenge [1], [2].

This work was supported by: the European Telecommunication Standard Institute (ETSI), Smart Body Area Networks (SmartBAN) Technical Committee, the European Union's Horizon 2020 programme under grants No. 872752 and No. 101017331, Fondazione Cassa di Risparmio di Firenze (project: smartHUB on Medical & Social ICT for Territorial Assistance, and the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

Traditional wireless communication methods, such as Bluetooth and other radio frequency (RF)-based transmission technologies, encounter limitations in terms of energy efficiency, security, and data integrity, particularly in wireless Body Area Networks (BANs) [3]. Recently, galvanic coupling (GC) has been proposed as an alternative technology for BAN that can be used for on-body communications with electrodes placed on the skin or intra-body communication with implanted electrodes [4]: low-power electrical signals travel through biological tissues to transmit data. This method confines signal propagation within the body, hence it reduces susceptibility to eavesdropping and interference from external signals while minimizing energy consumption [5]. In this paper we focus on GC on-body setting.

A promising application of this technique is secret key extraction for secure communication of on-body devices. By exploiting the unique physical properties of on-body GC channels, cryptographic keys can be dynamically generated between two legitimate devices, such as on-body sensors, ensuring secure and autonomous data exchange.

This paper explores the feasibility of cryptographic key generation using a GC-based approach, demonstrating how on-body communication can be leveraged to enhance security in wearable medical devices. This work aligns with the broader trend in WBAN security research, which seeks to establish robust and low-complexity cryptographic techniques tailored for medical applications [6]. Our proposed methodology ensures that key extraction remains resistant to adversarial attacks while maintaining minimal computational overhead, making it suitable for real-time, resource-constrained health applications.

### A. State of the art

Secret key extraction in BANs is a crucial research area that aims to establish secure communication channels between on-body devices by leveraging the physical characteristics of the human body [7]. This section reviews the existing literature on authenticated secret key extraction techniques in BANs, with

a specific focus on methods utilizing GC and other physical layer characteristics.

Several works have explored key extraction techniques by leveraging the physical properties of the human body. One of the early contributions in this field is authenticated secret key BAN (ASK-BAN) [8], which introduced an authenticated secret key extraction mechanism using channel characteristics specific to BANs. ASK-BAN utilizes the inherent randomness of the body channel to generate cryptographic keys while incorporating authentication mechanisms to enhance security.

Building upon this approach, movement-aided authenticated secrect key BAN (MASK-BAN) [9] introduced a movement-aided mechanism to further improve key extraction efficiency. By leveraging movement-induced variations in the body channel, MASK-BAN enhances the entropy of the generated keys and improves resilience against adversarial attacks. Additionally, Yuan *et al.* [10] extended these ideas by proposing a method that emphasizes authentication during the key extraction process, ensuring robustness against potential eavesdropping and impersonation attacks.

Apart from channel characteristics, biometric-based approaches have also been explored for key generation in BANs. Roeschlin *et al.* [11] proposed a method that derives cryptographic keys from biometric body impedance measurements. This approach capitalizes on the uniqueness of individual biometric signals to enhance security while reducing reliance on traditional cryptographic techniques.

Another key aspect of research in this domain focuses on improving the performance and efficiency of key generation. Yao *et al.* [12] presented strategies to optimize secret key generation performance for on-body devices by reducing latency and enhancing robustness. Their work highlights the trade-offs between security and computational efficiency in real-world deployments of BANs.

In the context of GC, Tomlinson [13] investigated the physical layer design and implementation of a biometric authentication system using intra-body communication. This study underscores the potential of GC for secure and efficient communication within BANs, offering an alternative to traditional radio-frequency-based approaches.

Finally, Ali *et al.* [14] addressed a critical challenge in key generation—eliminating the reconciliation cost. Their proposed method enhances the efficiency of key agreement protocols for body-worn health monitoring devices by minimizing the overhead associated with key synchronization, thereby making the process more practical for real-time applications.

While existing methods provide strong foundations, the use of GC for key extraction remains an unexplored area with significant potentials, particularly in terms of security, reliability, and energy efficiency.

### B. Our contribution

We propose a novel method for secret key extraction using GC in BANs. Our approach leverages the reciprocity of on-body channels to enable secure key agreement between two legitimate on-body devices while preventing eavesdropping.

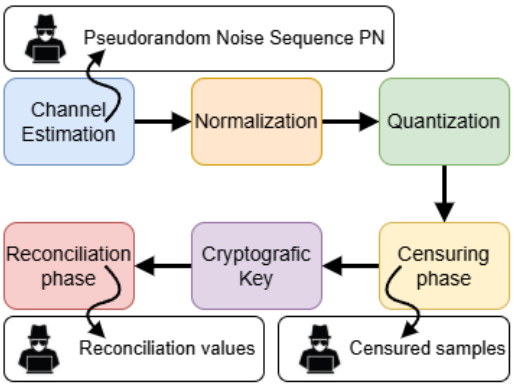



Fig. 1: Flowchart of secret key extraction.

We validate the reliability and security of the extracted keys through experimental analysis on human subjects. The proposed technique is designed to have low-complexity, making it ideal for low-resourced wearable devices. This work contributes to enhance secure on-body communication with minimal computational overhead.

## II. Methodology

The system examined in this experiment involves communication between two legitimate devices, Alice and Bob, which are in contact with the person's skin and communicate through GC technology. The communication between the two devices is bidirectional, and the channel between them can be considered symmetric. By exploiting the characteristics of the channel between the two devices, it is possible to extract a cryptographic key, which depends on the distances between the electrodes that make up the communication system and the subject. In the experimented system, an illegitimate device, eavesdropper (Eve), was considered, which will try to extract the encryption key to interpret the messages exchanged by the two legitimate devices.

In the following, the security protocols and challenges associated with BANs is discusses, as well as the algorithm used for extracting cryptographic keys from body signals.

### A. Secrect key extraction from body signals

Figure 1 shows the main phases that compose the cryptographic key extraction methods. For channel estimation, Alice and Bob use the same pseudorandom noise (PN) sequence, which is common a priori knowledge. Eve also knows this sequence. The two legitimate devices can thus estimate the communication channel between them. The continuous estimated channel at both parties is then quantized to obtain discrete secret keys. The values are mapped to discrete levels, ensuring that Alice and Bob derive nearly identical bit sequences. Since the channel is symmetric, the obtained values are similar — except for noise — and depend on the setup parameters, such as the distance between Alice's and Bob's electrodes. To improve the precision of the quantization process, the estimated channel is normalized to utilize the full

amplitude quantization range. Regardless, Eve can estimate the path loss and replicate the signal amplitude between Alice and Bob. In particular referring to Fig. 2, Alice represents a device with two transmitter (TX) and Bob another device with the two receiver (RX) electrodes, while Eve is another device with other two electrodes and is not represented in Fig. 2 for simplicity.

Amplitude quantization is applied by choosing a specific number of quantization bits ($b_q$) to reduce the influence of noise. The greater the number of $b_q$, the longer the cryptographic key will be, but the number of errors in the channel estimation made by Alice and Bob will also be higher. Alice and Bob will share the values within a chosen uncertainty interval, defined as a percentage of the quantization interval, near the quantization thresholds in an unencrypted form, as these values statistically cause the most errors. They remove these values from the channel estimation vector that are uncertain for Alice or Bob. The remaining values form a cryptographic key that can be used to encrypt future messages, ensuring that the information cannot be understood by Eve.

The channel estimation made by Alice and Bob will be different due to the noise present in the channel, and thus the two series of numbers will be different. In this way, besides Eve, the legitimate receiver is also unable to decrypt the message. To avoid this, a reconciliation phase is necessary. That is, an algorithm must correct the erroneous values in the channel estimation of Alice and Bob.

Eve will be aware of all the values exchanged between Alice and Bob throughout the entire key definition process. Specifically:

- The initial messages required for channel estimation, sent from Alice to Eve and from Bob to Eve.
- The values to be censored because they are close to the thresholds.
- The messages necessary for the reconciliation phase, thus the same percentage of corrected values.

### B. Potential Attacks by Eve on Cryptographic Key Extraction

Physical layer security, through the extraction of cryptographic keys from biometric features, represents a robust and user-friendly approach to safeguarding sensitive information. By integrating the unique and consistent nature of biometric data, this method enhances security while maintaining user convenience and privacy. Eve can employ different strategies to attempt to derive the cryptographic key:

- Eve can consist of a single device located on the person's body, similar to Alice and Bob. By estimating the channel in the same way as the legitimate devices, Eve can attempt to derive the cryptographic key.
- Alternatively, the device on the body can communicate the encrypted message to another device, and the cryptographic key can be sought by reproducing the same setup parameters as Alice and Bob but on a different person.

To prevent the first attack from being effective, it is necessary that the diversity between the setup parameters of the two legitimate devices and a legitimate device with Eve causes the channel between the transmitter and receiver to vary. While to make the second type of attack effective, it is necessary that, with the same setup parameters, the channel differs from person to person.

## III. Experimental Campaign

### A. Galvanic Coupling

GC uses on-body electrodes as both TX and RX to transmit low-power electrical currents (less than 1 mA) carrying data [4] at frequencies from 1 kHz to 100 MHz. In GC, an AC current flows through the body, which acts as a waveguide. The signal is applied differentially between two TX electrodes, with the primary current that carries the data flowing between the TX electrodes, while attenuated secondary currents are detectable at the two RX electrodes.

To understand the GC body channel, a channel impulse response (CIR) has been formulated [5]. Our objective is to leverage it to identify individual characteristics for the purpose of generating a secret key.

A correlative channel sounding technique [15], [16] is employed using pseudorandom noise (PN) sequences to experimentally assess the GC CIR. Indeed, the received signal can be expressed as $y(t) = x(t) * h(t) + n(t)$, with $x(t)$ being the transmitted signal and $y(t)$ the received signal, $h(t)$ is the channel's impulse response, $n(t)$ the additive noise, and $*$ the convolution operation. By correlating each side of the equation with $x(t)$, we derive:

$$R_{xy}(\tau) = h(\tau) * R_{xx}(\tau), \tag{1}$$

where $R_{xy}$ is the cross-correlation function of $x(t)$ and $y(t)$, $R_{xx}(\tau)$ is the auto-correlation function of $x(t)$, $\tau$ is the delay time, and $n(t)$ and $x(t)$ are assumed uncorrelated. Provided that the CIR $h(t)$ changes slowly over the time span required for determining the correlation function, Eq. (1) can be utilized to evaluate $h(t)$, assuming that $R_{xx}(\tau)$ approximates a Dirac delta function. To accomplish this, PN sequences are employed as the transmitted signal $x(t)$. The received signal is correlated with the transmitted PN to obtain an estimate of the CIR [15]. Using maximal-length PN sequences as the transmitted signal results in an auto-correlation function characterized by a prominent correlation peak and minimal side lobes. This property enables the identification of each multipath component at the receiver by correlating the channel output with the original PN sequence using a matched filter [16].

To measure the CIR, a polynomial PN sequence of degree $m = 14$ was transmitted in baseband using a linear-feedback shift register. The experimental platform [17] was adapted for correlative channel sounding (Fig. 2), requiring only two computers with sound cards for signal transmission and reception within a GC frequency band [17]. Battery-operated PCs prevent shared ground return paths between TX and RX, ensuring compliance with GC requirements. PN sequences are generated in Matlab, converted to analog, and transmitted via the TX's sound card through a *LINE OUT* jack to two electrodes introducing the signal into biological tissue. The

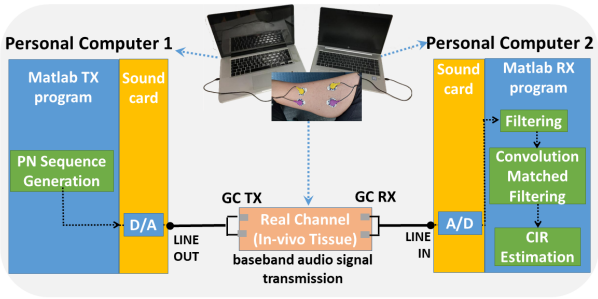



Fig. 2: Implemented GC testbed.

received signal is captured by two electrodes and transferred to the second PC via the *LINE IN* port. At reception, a 50 Hz filter and a convolutional matched filter correlate the channel output with the known PN sequence for CIR estimation. Audio is sampled at 48 kHz with 16-bit resolution.

### B. Experimental Setup

The GC on-body communication setup, detailed in [5], aimed to test electrode configurations for effective transmission and channel evaluation. Experiments were conducted on eight healthy subjects (24–30 years old) with signal acquisition on the forearm.

As shown in Fig. 2 and Sec. III-A, the setup consisted of two laptops (TX and RX) and four surface electrodes (PG10C, FIAB, Ag/AgCl, CE-certified). Electrodes were placed on the inner forearm, ensuring stable skin contact and circuit closure for signal transmission.

Each configuration was tested five times for statistical consistence. Electrode positioning followed two parameters: longitudinal distance ($d_l$) between TX and RX electrode pairs, and transverse distance ($d_t$) within each pair. Configurations included:

- $d_l = 3$ cm, 5 cm, 10 cm, 15 cm, with $d_t = 3$ cm.
- $d_l = 5$ cm, 10 cm, with $d_t = 5$ cm.

The RX electrodes were placed 3 cm from the wrist, with TX positioned per test configuration. Distances were measured from electrode centers, and polarity was consistently maintained across trials for uniformity.

### C. Test procedure

Before running the codes, the technical setup must be properly configured to ensure efficient transmission. The steps to follow are:

- Cable connection: TX is connected to the LINE OUT output, while RX is connected to the LINE IN input.
- Volume adjustment: Set the volume of LINE IN and LINE OUT to 80% of the maximum level, while all other channels should be disabled to avoid interference. Other values of volume could be tested although not reported in the paper.
- Audio format configuration: On both laptops, set the communication format to "2 channels, 16-bit, 48000 Hz", disabling any audio optimizations.
- Return path avoidance: Disconnect the laptops from the power supply to avoid common ground return paths between TX and RX.
- Electrode placement: Apply the electrodes to the subject's skin, maintaining the indicated distances.
- Transmission start: The RX code must be executed approximately 2 seconds before TX, ensuring that the RX is actively listening when the TX starts signal emission. If the signal is cut off, the test is considered invalid and must be repeated.

This experimental configuration allows for testing intracorporeal communication under controlled conditions, optimizing transmission quality and signal stability.

## IV. Numerical Results and Discussion

The data from the measurement campaign was post-processed in MATLAB to simulate the performance of the system for extracting cryptographic keys from the subjects' biological characteristics. For each subject and each electrode position, 5 repetitions were available, resulting in 5 different channel estimates. For each simulation, a pair of these 5 channel values was considered to simulate the channel estimation performed by Alice and Bob. Therefore, for each subject in each electrode position, there are 10 different channel realizations to perform the key extraction.

Reliability was defined as the number of errors made in the channel estimation by Alice and Bob after the phase of censoring uncertain values. For the system to function correctly, it is necessary that this error percentage be corrected during the reconciliation phase. Thus, the reliability value is useful for correctly choosing the reconciliation algorithm, which must be able to correct this number of errors without exceeding, otherwise it would compromise the system's security. Consequently, security was defined as the number of cases where Eve estimates the channel between herself and Alice with fewer errors than Bob. In this case, after the reconciliation phase, Alice, Bob, and Eve have the same channel estimate and therefore the same cryptographic key.

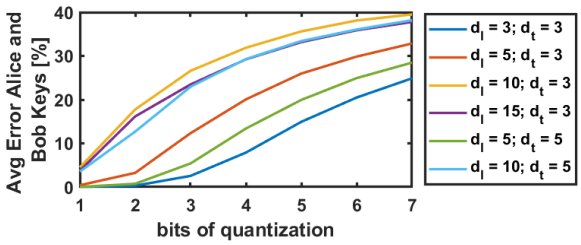
Tables I and II show the percentage values of reliability and security of the system with 1, 3, and 5 quantization bits. The figures show the average of reliability and security performances for each subject (Figs. 3b and 4b) and each electrode position (Figs. 3a and 4a). In all simulations, an uncertainty interval of $\pm 15\%$ of the quantization interval was considered for the censoring phase.

### A. Reliability Performance

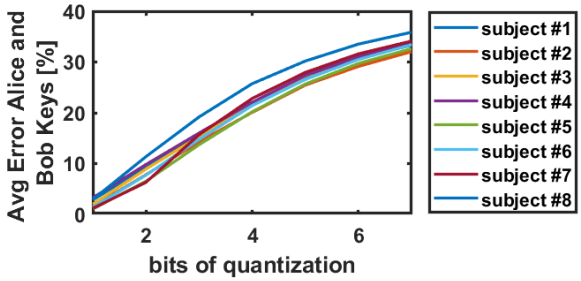
To calculate the reliability percentage, the number of errors made by Alice and Bob was determined relative to the total number of values remaining after the censoring phase. On average, with $b_q = 1$, we have a cryptographic key of 443 bits; with $b_q = 3$, a cryptographic key of 852 bits; and with $b_q = 5$, a cryptographic key of 1286 bits.

TABLE I: Reliability Performance Analysis: Average Percentage Error Between Alice's Key and Bob's Key Relative to Key Length. Results obtained with 1, 3, and 5 bits of quantization.

| | | Subjects [$b_q = 1$; $b_q = 3$; $b_q = 5$] | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | #1 [%] | #2 [%] | #3 [%] | #4 [%] | #5 [%] | #6 [%] | #7 [%] | #8 [%] |
| Setup | $d_l = 3$; $d_t = 3$ | [0; 1; 13] | [0; 0; 8] | [0; 2; 14] | [0; 2; 14] | [0; 1; 13] | [0; 2; 15] | [0; 5; 21] | [0; 8; 23] |
| | $d_l = 5$; $d_t = 3$ | [0; 9; 24] | [0; 9; 24] | [0; 10; 24] | [0; 10; 24] | [0; 14; 27] | [1; 16; 29] | [0; 15; 28] | [0; 16; 28] |
| | $d_l = 10$; $d_t = 3$ | [5; 27; 37] | [3; 26; 36] | [5; 27; 37] | [8; 30; 39] | [2; 23; 32] | [4; 26; 35] | [3; 24; 33] | [5; 28; 36] |
| | $d_l = 15$; $d_t = 3$ | [8; 28; 36] | [3; 26; 36] | [3; 25; 33] | [8; 29; 37] | [0; 14; 26] | [1; 19; 30] | [0; 18; 29] | [7; 29; 37] |
| | $d_l = 5$; $d_t = 5$ | [0; 5; 19] | [0; 2; 16] | [0; 5; 20] | [0; 2; 17] | [0; 5; 20] | [0; 6; 20] | [0; 10; 24] | [0; 8; 23] |
| | $d_l = 10$; $d_t = 5$ | [4; 22; 33] | [3; 22; 34] | [4; 24; 34] | [4; 22; 33] | [4; 26; 35] | [2; 19; 30] | [3; 22; 33] | [5; 26; 35] |




(a) Average Percentage Error Between Alice's Key and Bob's Key Relative to Key Length for each setup




(b) Average Percentage Error Between Alice's Key and Bob's Key Relative to Key Length for each subject

Fig. 3: Reliability Performance in function of bits of quantization

In Table I, it is evident that Alice and Bob can consistently characterize the channel with minimal errors (less than 10%, marked in green) when using only 1 bit of quantization, regardless of the configuration and subject. As the number of quantization bits increases, successful channel characterization with few errors is only achievable in configurations with high signal-to-noise ratios.

In Fig. 3a two distinct clusters of curves can be observed. In the upper cluster the 3 curves (light blue, purple, and yellow curves) shows a more rapid grow, compared to the lower cluster of 3 curves (blue, green, and orange curves). The upper cluster curves are associated to greater distances between electrodes and thus to a lower received signal.

Finally, in Fig. 3b, it can be observed that on average, all subjects have the same performance in terms of reliability. This indicates that the key extraction method can be applied to all subjects and that the error depends only on the distance, i.e., the signal-to-noise ratio.

### B. Security Performance

For the calculation of the security percentage, the number of simulations in which Eve's errors were fewer than Bob's errors was counted relative to the total number of Eve's cases. Eve could be in a different position or estimate the channel in another subject. Therefore, a total of 235 possible attacks by Eve were considered for each pair of legitimate channel measurements, excluding only the 5 measurements taken at the same electrode distance on the subject.

In Table II, it is evident that using only 1 bit of quantization results in poorer performance compared to using 3 bits, as a single bit cannot adequately distinguish between different channels. In the three configurations with sufficient signal-to-noise ratio, Eve's success rate in finding the key is low (less than 20%, marked in green). At the closest points ($[d_l = 3,\ d_t = 3]$ and $[d_l = 5,\ d_t = 5]$), Eve rarely, or in some cases never, manages to extract the key.

The two clusters of curves defined in the Fig. 3a follow a similar behavior in Fig. 4a. As the number of quantization bits increases, the curves in upper cluster (light blue, purple, and yellow curves) show rapid grow of Eve's success rate before achieving a stable value. Meanwhile, the curves in the lower cluster (blue, green, and orange curves) show a reduction of Eve's success and thus an increase of the security performance of the system before achieving a stable value.

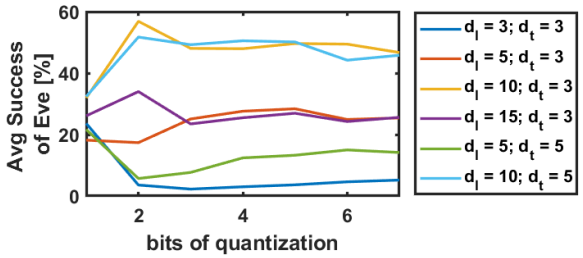
Finally, from Fig. 4b, it can be observed that the system's behavior varies among different subjects, confirming that the channel between different subjects is different. Therefore, this optimized method can be used for extracting a cryptographic key.

## V. Conclusions and Future Directions

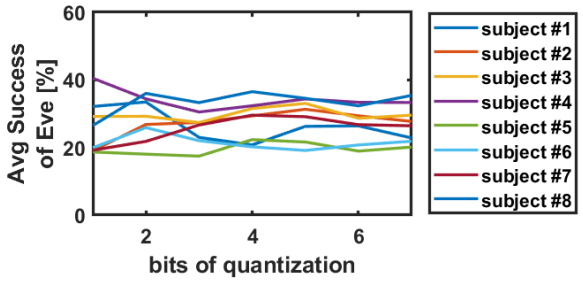
In this paper, we have explored the use of GC for secure key extraction in BANs. By leveraging the unique characteristics of on-body communication channels, we have demonstrated that it is possible to generate symmetric cryptographic keys in a secure and energy-efficient manner. Our experimental results show that: (i) the extracted secret keys are long enough for a standard symmetric encryption protocol, e.g., AES-256 or higher; (ii) if Alice and Bob are using only 1 bit of quantization to extract the key, this could not be enough to ensure that the key is not also extracted by Eve; (iii) if Alice and Bob are using 5 bits of quantization, this often provides too many errors and the key could not be successfully extracted; this could anyway be solved by using a longer

TABLE II: Security Performance Analysis: Average Percentage Success of Eve. Results obtained with 1, 3, and 5 bits of quantization.

| | | Subjects [$b_q = 1$; $b_q = 3$; $b_q = 5$] | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | #1 [%] | #2 [%] | #3 [%] | #4 [%] | #5 [%] | #6 [%] | #7 [%] | #8 [%] |
| Setup | $d_l = 3$; $d_t = 3$ | [18; 0; 2] | [18; 0; 0] | [25; 2; 3] | [28; 2; 3] | [28; 1; 2] | [29; 1; 3] | [30; 6; 9] | [13; 5; 8] |
| | $d_l = 5$; $d_t = 3$ | [15; 17; 28] | [12; 15; 20] | [24; 17; 28] | [24; 21; 29] | [17; 34; 35] | [24; 28; 23] | [20; 35; 34] | [10; 33; 29] |
| | $d_l = 10$; $d_t = 3$ | [45; 48; 52] | [18; 43; 55] | [48; 47; 54] | [66; 67; 69] | [10; 27; 22] | [16; 53; 41] | [19; 45; 43] | [34; 54; 60] |
| | $d_l = 15$; $d_t = 3$ | [63; 14; 25] | [15; 54; 55] | [27; 31; 33] | [47; 32; 41] | [4; 2; 3] | [8; 10; 11] | [5; 7; 7] | [41; 38; 40] |
| | $d_l = 5$; $d_t = 5$ | [25; 6; 8] | [14; 2; 3] | [25; 9; 14] | [29; 4; 11] | [25; 6; 18] | [21; 11; 12] | [14; 16; 23] | [19; 8; 14] |
| | $d_l = 10$; $d_t = 5$ | [27; 51; 42] | [36; 51; 55] | [26; 59; 65] | [50; 56; 52] | [29; 36; 48] | [21; 30; 23] | [27; 51; 59] | [43; 60; 56] |




(a) Average Percentage Success of Eve for each setup




(b) Average Percentage Success of Eve for each subject

Fig. 4: Security Performance in function of bits of quantization

PN sequence to estimate the channel. Challenges remain, including optimizing key generation over longer distances, assessing the effects of body movements and physiological variations, and ensuring integration into wearable medical devices for long-term stability and compliance [18].

In conclusion, GC-based key extraction offers a secure, low-power alternative to conventional cryptographic key exchange in BANs. Future advancements could enhance wireless medical communication security, promoting broader WBAN adoption among patients and healthcare professionals.

## REFERENCES


[1] A. Coviello, C. Cavigliano, V. Tasso, E. T. Tavassi, Y. Giacalone, and M. Magarini, "Emerging peripheral nerve injuries recovery: advanced nerve-cuff electrode model interface for implantable devices," in *2024 Global Conference on Wireless and Optical Technologies (GCWOT)*, pp. 1–7, IEEE, 2024.

[2] L. Mucchi, S. Jayousi, A. Martinelli, S. Caputo, and P. Marcocci, "An overview of security threats, solutions and challenges in WBANs for healthcare," in *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, p. 1–6, IEEE, May 2019.

[3] C. Quartana, A. Coviello, P. M. Ros, F. Del Bono, D. Demarchi, U. Spagnolini, and M. Magarini, "Wireless data transfer for implanted real-time peripheral nerve interfaces," in *EAI International Conference on Body Area Networks*, pp. 45–63, Springer, 2024.

[4] M. Swaminathan, A. Vizziello, D. Duong, P. Savazzi, and K. R. Chowdhury, "Beamforming in the body: Energy-efficient and collision-free communication for implants," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, 2017.

[5] A. Vizziello, P. Savazzi, R. R. Guerra, and F. Dell'Acqua, "Experimental channel characterization of human body communication based on measured impulse response," *IEEE Transactions on Communications*, vol. 72, no. 7, pp. 3970–3984, 2024.

[6] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6G networks," *IEEE Open Journal of the Communications Society*, vol. 2, p. 1901–1914, 2021.

[7] L. Hernández-Álvarez, E. Barbierato, S. Caputo, J. M. de Fuentes, L. González-Manzano, L. H. Encinas, and L. Mucchi, "Keyencoder: A secure and usable EEG-based cryptographic key generation mechanism," *Pattern Recognition Letters*, vol. 173, p. 1–9, Sept. 2023.

[8] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, WISEC'13, ACM, Apr. 2013.

[9] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet of Things Journal*, vol. 2, p. 52–62, Feb. 2015.

[10] J. Yuan, L. Shi, S. Yu, and M. Li, "Authenticated secret key extraction using channel characteristics for body area networks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS'12, p. 1028–1030, ACM, Oct. 2012.

[11] M. Roeschlin, I. Sluganovic, I. Martinovic, G. Tsudik, and K. B. Rasmussen, "Generating secret keys from biometric body impedance measurements," in *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, CCS'16, p. 59–69, ACM, Oct. 2016.

[12] L. Yao, S. T. Ali, V. Sivaraman, and D. Ostry, "Improving secret key generation performance for on-body devices.," in *BODYNETS*, pp. 19–22, 2011.

[13] W. J. Tomlinson, *Physical layer design and implementation of a biometric authentication system using galvanic coupling intra-body communication*. PhD thesis, Northeastern University Library, 2018.

[14] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, p. 2763–2776, Dec. 2014.

[15] P. B. Papazian and J. J. Lemmon, "Radio Channel Impulse Response Measurement and Analysis," *NTIA Technical Report TR-11-476*, May, 2011.

[16] W. J. Tomlinson, F. Abarca, K. R. Chowdhury, M. Stojanovic, and C. Yu, "Experimental assessment of human-body-like tissue as a communication channel for galvanic coupling," in *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, pp. 1–6, 2015.

[17] A. Vizziello, P. Savazzi, G. Magenes, and P. Gamba, "Phy design and implementation of a galvanic coupling testbed for intra-body communication links," *IEEE Access*, vol. 8, pp. 184585–184597, 2020.

[18] G. Borghini, S. Caputo, L. Mucchi, A. Rashid, S. Jayousi, M. Hämäläinen, T. Paso, and M. Hernandez, "Security of wireless body area networks for healthcare applications: Comparison between ETSI and IEEE approaches," in *2023 IEEE 17th International Symposium on Medical Information and Communication Technology (ISMICT)*, p. 1–6, IEEE, May 2023.