Platform for Multi-User Channel-Based Encryption of Speech Communication with AES on 2.45 GHz

Victor Van der Elst*, Ruben Wilssens*, Jelle Jocqué*, Joryan Sennesael*, Jo Verhaevert*,
Patrick Van Torre*, Hendrik Rogier*
*Ghent University - imec, IDLab, Department of Information Technology (INTEC)
Technologiepark-Zwijnaarde 126, 9052 Gent, Belgium, victor.vanderelst@ugent.be

***Abstract*—This paper outlines a hardware platform for half-duplex, real-time encrypted digital speech communication on 2.45 GHz. The platform is based on a STM32F415 MCU with a low power ADF7242 transceiver for wireless communication. The Advanced Encryption Standard (AES) Electronic Code Book encryption scheme is performed on the transmitted packets with symmetrically generated channel-based keys. Encryption keys of 128-bit are obtained, based on the unique reciprocal channel characteristics of the employed link. Key reconciliation is applied by means of a Hamming code and a cyclic redundancy check (CRC) to correct key mismatch. A multi-user system is introduced by splitting voice key distribution and speech communication into different abstraction layers. Measurements reveal a maximum communication range of 400 m without significant packet loss. A high key entropy of 0.94 bit is established with a packet rate of 167 packets/s and a key bit generation delay of four received signal strength (RSS) measurements.**

***Index Terms*—Digital speech communication, real-time, IEEE 802.15.4, channel-based keys, Advanced Encryption Standard (AES), ADF7242, STM32F415**

I. Introduction

Short range network protocols including Bluetooth, Bluetooth Low Energy (BLE), ZigBee and Internet Protocol version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) are receiving increased attention due to the rise of the Internet of Things (IoT). Communication applications often demand transmission of sensitive information, requiring secure encryption capabilities. On the other hand, IoT devices employing constrained resources lack the processing power to implement suitable cryptographic algorithms to secure network communication [1]. Additionally, mobile applications experience dramatic variations on the wireless communication link due to fading and shadowing. These effects on the received signal are considered disadvantageous for communication. Research in [2] shows that these channel variations can be exploited in lightweight algorithms to generate symmetric, channel-based keys.

The IEEE 802.15.4 standard includes security possibilities on the Media Access Control (MAC) layer with seven security levels [3]. These security possibilities require a secret code to encrypt data, this secret code is called a key. Key management and key generation algorithms are not included in the IEEE 802.15.4 standard and should be provided by the upper network layers [4]. Key distribution can form important security leaks in wireless transmission, exposing the encryption key to potential eavesdroppers. Implementing channel-based key generation eliminates key distribution, therefore reducing the risk of eavesdropping. Channel-based key generation is based on the fact that every communication channel between two parties is unique. This implies that channel variations due to fading and shadowing on this shared communication link can also be considered unique and reciprocal. The two communicating parties share a common source of information, out of which symmetric keys can be generated [4]. A third party does not have access to this information and cannot build an identical key.

A platform for digital voice communication using channel-based key generation was conceived in [5]. This paper describes the development of an improved hardware platform and introduces a protocol to allow multi-user communication. To achieve this, a common key needs to be distributed. This common key is distributed over the different unique links. Speech can then be encrypted using the Advanced Encryption Standard (AES) which is hardware accelerated.

The remainder of this paper is organized as follows, Section II describes the design of the hardware platform. In Section III the algorithms are explained. Finally Section IV describes the measurements.

II. Hardware platform

The hardware platform can be divided into five main parts, as illustrated in Figure 1 by the hardware diagram. Each part will be discussed in the following paragraphs, starting with the RF part. Next, the MCU and audio will be described. Finally, both the user interface and the power part are explained together in the last paragraph of this section, as they make use of the same micro-USB connector.

A. RF

The RF part, colored red in Figure 1, mainly consists of a transceiver IC, along with an Low Noise Amplifier (LNA) and a Power Amplifier/Low Noise Amplifier (PA/LNA). The ADF7242 is a low power, high performance transceiver operating in the 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band. The radio controller of the ADF7242 can operate in IEEE 802.15.4-2006 packet mode with a fixed data rate of 250 kbps and DSSS-OQPSK modulation [6].

Two radio frequency input/output (RFIO) ports are provided, allowing support for antenna diversity.

Additionally, the transceiver features external PA/LNA support in hardware. The CC2592 LNA/PA of Texas Instruments [7] and GRF2201DS LNA of GuerrillaRF [8] are included as range extenders between the SMA connector and the transceiver, increasing the output power to maximally 22 dBm. A 2450LP14A100T bandpass filter by Johanson Technology [9] with a center frequency of 2.45 GHz and a bandwidth of 100 MHz is used in front of the SMA connectors. A conversion between the unbalanced LNA port and balanced half-duplex RFIO port of the transceiver is performed by the 2450BM15A0015E balun from Johanson Technology [10]. The CC2592 LNA/PA already includes an integrated matching network and balun, and hence requires few external components. Finally, impedance matched traces of 50 Ω have been routed from the transceiver to the MCU.

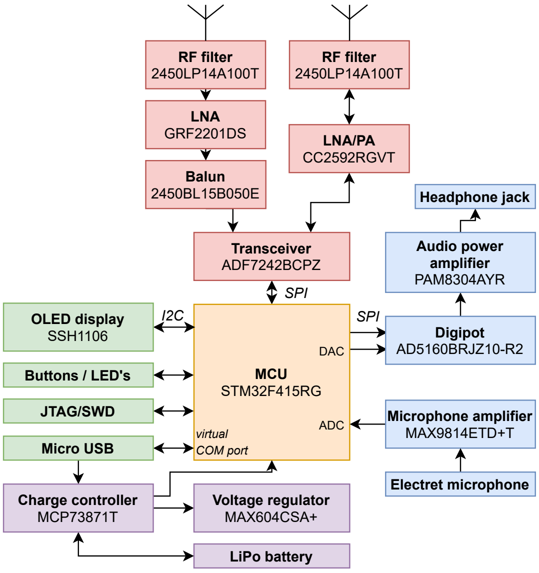

Fig. 1. Hardware Schematic. The RF Part is in red, MCU part in orange, Audio part in blue, User Interface part in green and power part in purple.

B. MCU

The main processing unit of the platform, colored orange in Figure 1, is a STM32F415RG MCU based on the high-performance ARM Cortex-M4, running at the maximum frequency of 168 MHz [11]. The MCU offers rich connectivity and integration and a crypto/hash processing unit provides hardware acceleration for AES-128.

C. Audio

The audio part is colored blue in Figure 1. Audio recording takes place on the transmitting device and is performed by an electret microphone. The captured signal is further amplified by a MAX9814ETD with automatic gain control and a low shutdown current [12]. The amplifier gain is set to 50 dB in hardware. The audio is sent to one of the MCU ADCs for sampling at 16 kHz with an 8-bit quantization resolution. On the receiving side, digital voice samples are converted back to analog signals using the DAC of the MCU at 8 kHz and forwarded to the D5160BRJZ10 digital potentiometer [13]. The output volume can be configured by the SPI interface of the MCU before entering the final amplifying stage. The PAM8304AYR is an efficient class D audio amplifier capable of driving an external 8 Ω speaker or headphones through a 3.5 mm audio jack up to 900 mW [14].

D. User interface and power supply

A user-friendly user interface, colored green in Figure 1, has been incorporated in the design. The 1.3” OLED screen with SSH1106 driver displays several settings and is supported by an RGB led. Six pushbuttons allow to navigate through the menu and select the MCU state. One of these pushbuttons is dedicated to switching the MCU in and out of the power conserving standby mode while another button acts as a push-to-talk button. The supply part of the system, colored purple in Figure 1, is powered by a 3.7 V Lithium Polymer battery with a capacity of 980 mAh, which can be recharged via the micro-USB port. The battery management is handled by the MCP73871T, which sends an interrupt to the MCU to indicate a low battery status. Finally, a micro-USB connector configured as virtual Communication (COM) port allows data transfer via the USB CDC protocol for real-time datalogging and measurements on a host computer.

III. Software

The real-time speech communication platform is based on the principle of a walkie-talkie, operating as a half-duplex system where only one party can exchange data alternately. To ensure that only authorized devices can participate, the transmitted audio packets should be encrypted with AES-128. Encryption keys can be generated using channel estimation measurements as described in [4]. The network of communicating devices functions as a distributed network, where every node maintains an updated list of participants and the related network key of that particular link. Whenever a device becomes the transmitter, it generates a voice key and distributes this common key to its participant list with encrypted packets over all active channels using their respective network keys. This section describes the proposed key generation algorithms followed by the implementation of a multi-user system.

A. Key generation

Radio channel measurements are automatically appended to received packets in the form of two 8-bit values: Received Signal Strength (RSS) and Signal Quality Indicator (SQI). The first parameter will be used in the quantization algorithms to generate equal keys on both sides of the link. Two key generation algorithms have been tested, the first algorithm is based on [2], [4], [5] and [15] where practical keys are generated. The second algorithm is based on [16] and [17]. Both algorithms exploit the highly correlated channel characteristics of two communicating devices to extract key bits. Unique channel variations due to different types of fading, shadowing and path loss as shown in Figure 2, are the main source of this shared, yet private information. The following subsections explain the implementation of these quantization algorithms.

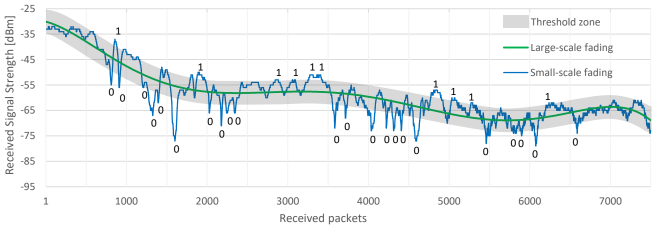

Fig. 2. Radio channel variations in mobile environment

1) Quantization algorithm 1: The first algorithm is based on [2], [4], [5] and [15] where practical keys are generated. The RSS of every packet is processed in an exponential moving average at both ends of the communication link. A weighting factor α of 0.1 is chosen to produce a stable average, as illustrated by the green curve in Figure 2. On the transmitting side, a censoring zone, in gray in Figure 2, based on a threshold value is defined around this moving average, in which the quantizer will not look for new key bits. Whenever a new RSS value is recorded outside of this zone, a logic 0 or a logic 1 is generated in case the RSS is respectively lower or higher than the threshold zone. Whenever a new key bit has been generated, the transmitter immediately returns a packet to inform the receiving end of this event without exchanging the actual bit level. Upon reception, the receiver itself generates a key bit based on the value of its measured RSS, relative to the moving average.

Due to a reasonable amount of errors in the formed keys, key reconciliation is applied to the algorithm. A (15,11)-Hamming forward error correcting code is employed in conjunction with a CRC32 error detecting code. For the Hamming code, the four parity bits of the codeword are sent within a key packet to allow the correction of one bit error in key fragments of 8 bits. A CRC checksum allows both parties to agree on a new 128-bit key by inserting the key fragment of 32 bits formed by four key fragments of 8 bits. If the checksum is identical on both sides, the 32-bit key matches completely without bit errors and the 128-bit key may be used as a new network key.

2) Quantization algorithm 2: Based on [16] and [17], the second algorithm uses a different approach for key bit generation and quantizes each measurement to an 'arbitrary' number of bits without censoring. In this 1-bit adaptive quantization scheme, the audio transmitter also acts as master while the receiver behaves as slave. RSS measurements are deployed to build quantization intervals which will generate a 128-bit key based on the 128 latest transmissions. All signal measurements are temporarily stored in memory and a RSS minimum and maximum are dynamically maintained within the transmission interval. As a proof of concept, eight equally-sized intervals are formed with these maxima. Improved security measures require to calculate the inverse cumulative distribution function (CDF) of the measured RSS for equally likely interval bins [16].

Next, a particular type of Gray code is implemented to assign a binary codeword to every quantization bin. The codewords consist of three bits d_0, d_1 and *e* as displayed in Table I, where neighboring intervals only differ by one bit in their respective codewords. On both the transmitter and the receiver, three 128 wide bit vectors are generated from the recent RSS measurements. Out of these three vectors appropriate key bits k_i are extracted according to the bit position *i*. Depending on the value of the *i*-th bit of bit vector *e*, the $d_{0,i}$ or $d_{1,i}$ bit values are used as key bit k_i. Upon generation of the bit vectors, the master node transmits its bit vector *e* to the receiver to reduce bit disagreements in the generated keys. When disagreements occur, it is very likely that only one bit of the multi-bit codeword will be in error due to the use of Gray coding. Passing the bit vector *e* provides a form of key reconciliation without providing an eavesdropper with too much information about the secret key bits. Knowing $e(k_i)$ eliminates half of the possible quantization levels, but codewords are equally likely given the knowledge of $e(k_i)$ [16]. Future study should investigate any possible security differences with the modification of generating equally-sized intervals using only absolute maxima without the calculation of the CDF as in [17].

TABLE I
QUANTIZATION INTERVALS GRAY CODING

Quantization level	**Gray code**			**RSS interval**	
	d_1	d_0	e		
1	0	0	0	$[RSS_{\min}$	$; RSS_{\min} + \frac{\Delta}{8}[$
2	0	0	1	$[RSS_{\min} + \frac{\Delta}{8}$	$; RSS_{\min} + \frac{2\Delta}{8}[$
3	0	1	1	$[RSS_{\min} + \frac{2\Delta}{8}$	$; RSS_{\min} + \frac{3\Delta}{8}[$
4	0	1	0	$[RSS_{\min} + \frac{3\Delta}{8}$	$; RSS_{\min} + \frac{4\Delta}{8}[$
5	1	1	0	$[RSS_{\min} + \frac{4\Delta}{8}$	$; RSS_{\min} + \frac{5\Delta}{8}[$
6	1	1	1	$[RSS_{\min} + \frac{5\Delta}{8}$	$; RSS_{\min} + \frac{6\Delta}{8}[$
7	1	0	1	$[RSS_{\min} + \frac{6\Delta}{8}$	$; RSS_{\min} + \frac{7\Delta}{8}[$
8	1	0	0	$[RSS_{\min} + \frac{7\Delta}{8}$	$; RSS_{\max}]$

The second algorithm has considerable advantages with respect to the algorithm implementing censoring: faster key generation rates, reduced radio channel traffic, decreased bit disagreement and multi-bit quantization extensions as proven in [16] and [17]. The practical implementation is tested with entropy measurements for different generation rates in Section IV.

B. Multi-user

Recently, a real-time voice communication platform was described in [5], implementing channel-based key generation between two devices. The current platform focuses on a networking protocol allowing multiple users to take part in encrypted voice communication with channel-based keys. Every device contains a networking identification number, making individual devices addressable. The master device, broadcasting audio packets with a common voice key, receives acknowledgement packets from all slave devices. Next, the destination and source addresses are extracted from all received packets. When the destination address does not match the device's networking identification number, the packet is discarded. Oppositely, when a match occurs, the device checks its list of authorized devices using the source address. The key generation algorithm parameters of that device are updated if it is authorized to receive encrypted messages. Packets for new key bits, Hamming codes, CRC and the voice key can be produced when the algorithm criteria are met. The transmission of these key packets (red and green) takes place in between the audio packets (blue) on the network layer as displayed in Figure 3.

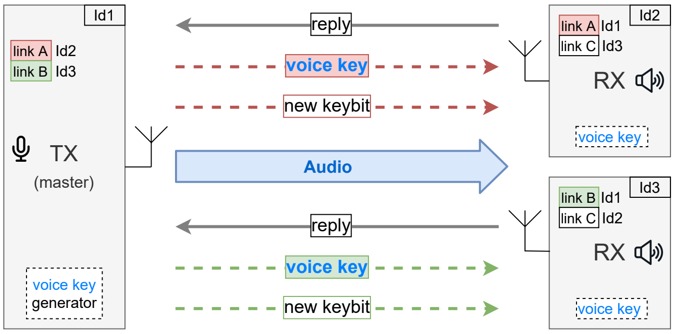

Fig. 3. Overview abstraction layers. The voice communication using a common voice key is split from the key distribution.

IV. Measurements

A. Spectrum

Measurements on the output power of the platform with the additional RF amplifier were taken on a FSV4 signal and spectrum analyzer from Rohde & Schwarz. The Max Hold function allows for peak detection of burst signals on the transmitting device. The transmit power of the ADF7242 is programmed to its maximum of +4.8 dBm in high power mode. The average output power of the half-duplex RFIO port measured -0.51 dBm at a center frequency of 2.45 GHz with the ADF7242 set to +4.8 dBm. This is a rise of 14 dB relative to measurements of a similar platform in [5], without additional range extenders. These results are 10 dB lower than the expected 24 dB gain of the RF amplifier. A possible source of this attenuation is mismatch and needs further verification. Additional measurements should be performed to determine the output power at each stage of the RF circuit.

B. RSS

All further measurements were performed using external dipole antennas with an input impedance of 50 Ω and a gain of 2.1 dBi. A series of discrete measurements were done to determine the performance of the LNA/PA and the maximum range of the platform in different environments. Line-of-sight (LOS) and non-line-of-sight (NLOS) situations were tested. Figure 4 displays the received signal strength measurements on the ADF7242 transceiver. Measurement points stop at -95 dBm as this is the minimum sensitivity of the ADF7242. Additionally, a sweep of signal strengths was captured in LOS over a range of 400 m with the transmitter moving away from the receiver at a constant speed. These strengths were captured during a 60 s interval with audio packets being transmitted at a rate of 500 packets/s. Voice communication was never interrupted during these measurements. Figure 5 shows the captured RSS together with the averaged RSS curve as described in Section III.

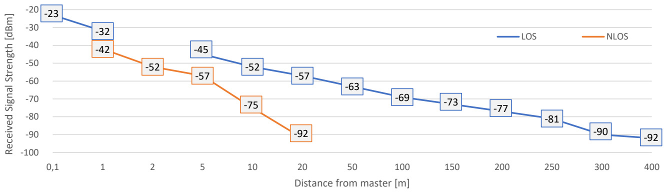

Fig. 4. Distance measurements using RSS for both LOS and NLOS.

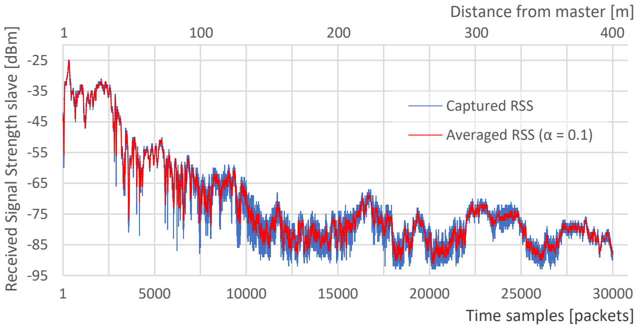

Fig. 5. RSS distance sweeps with 500 packets/s.

C. Key generation

1) Algorithm 1: The key generation was tested for different algorithm parameters to ensure that equal keys are generated and updated frequently, without any drawbacks on the safety of the key. The key entropy, the Key Error Rate (KER) and the key update rate have been analyzed for two packet rates, based on the sample count per packet. In all measurements a threshold of 3 dB is used with a weighting factor α of 0.1. With a packet rate of 167 packets/s, each packet consisting of 48 samples, key bits are generated at a reasonably high rate as indicated in Figure 6.

To maintain high entropy, delays are introduced between choosing different key bits. Larger packet rates at 250 packets/s, having 32 samples per packet, were tested but yield a low entropy, even with delays. A reduction of the KER from 33.3% to 9% was obtained by using the lower packet rate with 48 samples per packet. The final parameters are chosen to be 48 samples with a delay of 4 measurements, based on the higher key bit rate without significant loss in entropy. With 22 key bits/s generated, a new 128-bit network key can be produced every 5.8 seconds or nearly every second when the current 128-bit key is updated in steps of 32-bit keys.

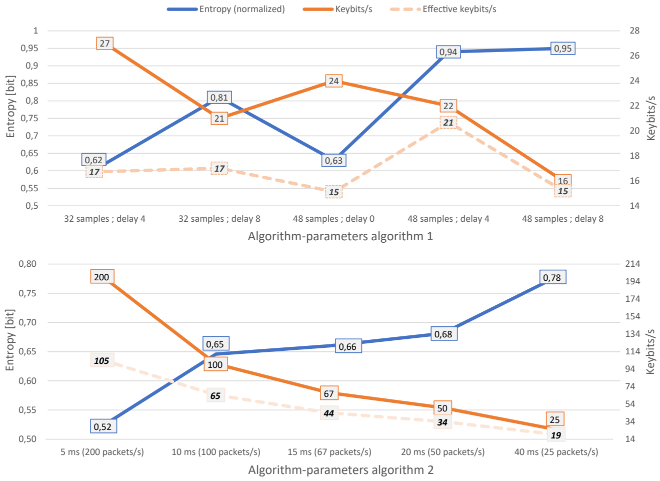

Fig. 6. Key entropy and key bit generation rate with different parameters.

2) Algorithm 2: For the second algorithm, a testing code was uploaded to the current hardware platform. The code mainly consists of a periodic interrupt that broadcasts dummy packets on the transmitting master device. The receiving slave device answers with an acknowledgement packet. Both devices store the measured RSS of the received packets in a buffer. If a device received 128 acknowledgment packets, it generates the bit vectors d_0, d_1 and e from these RSS measurements. The master device transmits the bit vector e to the slave device. The slave then replaces its bit vector e with the receiving one from the master device to allow for error correction as stated in Subsection III-A2, and generates a key.

The key entropy is determined for five different packet rates and is shown in Figure 6. All measurements were performed in a mobile environment during one minute. In all situations the entropy of the generated keys remained relatively low, fluctuating between 0.5 and 0.8 bit. Yet, because of the high update rate of the keys, the effective number of new key bits generated is still relatively high, ranging between 25 and 200 key bits per second.

The KER and Bit Disagreement Rate (BDR) of the generated keys show that with an average KER of 78% and a BDR of 27.66% further key reconciliation is necessary for mobile environments.

V. Conclusion

In this paper the design and development of a hardware platform for real-time encrypted digital speech communication on 2.45 GHz is tested. The hardware platform transmits encrypted audio packets using AES with a shared voice key, which is transmitted over an abstracted network layer with channel-based keys. This abstraction allows for a secure key distribution network to support multiple users wishing to participate in the encrypted voice communication. The RF section is improved with additional range extenders allowing voice communication up to 400 m in LOS situations.

Two key generation schemes were tested. The censoring algorithm is tested with different packet rates and key bit delays, to ensure an optimal entropy and update rate of the generated keys. A packet rate of 167 packets/s and a key bit delay of 4 RSS measurements yielded optimal results with new 128-bit keys being generated every 5.8 seconds. Based on these findings, a highly secure voice communication system is achieved. The second algorithm shows promising results, but can only be used in mobile environments. Future research should investigate the addition of key reconciliation and equally likely intervals on the second algorithm to optimize the key agreement and the key entropy.

References

[1] S. Li, "Chapter 1 - introduction: Securing the internet of things," in *Securing the Internet of Things*, S. Li and L. D. Xu, Eds. Boston: Syngress, 2017, pp. 1–25.

[2] P. Van Torre, Q. Van den Brande, J. Verhaevert, J. Vanfleteren, and H. Rogier, "Key Generation Based on Fast Reciprocal Channel Estimation for Body-worn Sensor Nodes," *2017 11th European Conference on Antennas and Propagation (EuCAP)*, pp. 293–297, 2017.

[3] "IEEE 802.15.4-2020 – IEEE Standard for Low-Rate Wireless Networks," 2020.

[4] P. Van Torre, "Channel-Based Key Generation for Encrypted Body-Worn Wireless Sensor Networks," *SENSORS*, vol. 16, no. 9, p. 1453, 2016.

[5] J. Jocqué, P. Van Torre, J. Verhaevert, and H. Rogier, "Platform for Digital Voice Communication with Channel-Based Key Generation," *Antennas and Propagation (EuCAP) 2021 15th European Conference*, pp. 1–5, 2021.

[6] Analog Devices, *Low Power IEEE 802.15.4/Proprietary GFSK/FSK Zero-IF 2.4 GHz Transceiver IC*, 2010. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/ADF7242.pdf

[7] Texas Instruments, *CC2592 2.4-GHz Range Extender*, 2014. [Online]. Available: https://www.ti.com/lit/ds/symlink/cc2592.pdf?ts=1620074225995

[8] Guerilla RF, *High Gain LNA2.4 GHz ISM; 802.11 b, g, n*, 2021. [Online]. Available: https://www.guerrilla-rf.com/prodFiles/2201/GRF2201DS.pdf

[9] Johanson Technology, *High Frequency Ceramic Solutions*, 2003. [Online]. Available: https://www.johansontechnology.com/datasheets/2450LP14A100/2450LP14A100.pdf

[10] ——, *High Frequency Ceramic Solutions*, 2013. [Online]. Available: http://www.farnell.com/datasheets/1722470.pdf

[11] STMicroelectronics, *STM32F415xx, STM32F417xx Datasheet*, 2020. [Online]. Available: https://www.st.com/resource/en/datasheet/dm00035129.pdf

[12] Maxim Integrated, *Microphone amplifier with AGC and low-noise microphone bias*, 2006. [Online]. Available: https://datasheets.maximintegrated.com/en/ds/MAX9814.pdf

[13] Analog Devices, *256-Position SPI-Compatible Digital Potentiometer*, 2014. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/AD5160.pdf

[14] Diodes Incorporated, *3W Mono Class D audio amplifier*, 2013. [Online]. Available: https://www.diodes.com/assets/Datasheets/PAM8304.pdf

[15] T. Castel, P. Van Torre, and H. Rogier, "RSS-Based Secret Key Generation for Indoor and Outdoor WBANs using On-body Sensor Nodes," *Proceedings of the 2016 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–5, 2016.

[16] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[17] D. Kreiser, Z. Dyka, S. Kornemann, C. Wittke, I. Kabin, O. Stecklina, and P. Langendörfer, "On Wireless Channel Parameters for Key Generation in Industrial Environments," *IEEE Access*, vol. 6, pp. 79 010–79 025, 2018.