A 415 nW Physically and Mathematically Secure Electro-Quasistatic HBC Node in 65nm CMOS for Authentication and Medical Applications

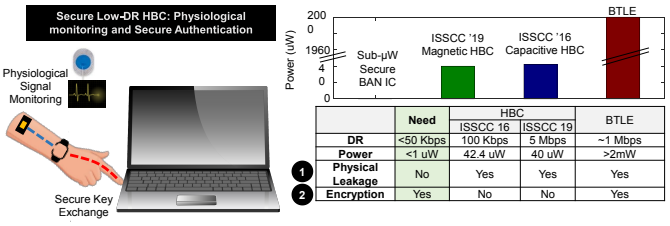
Shovan Maity, Nirmoy Modak, David Yang, Shitij Avlani, Mayukh Nath,
Josef Danial, Debayan Das, Parikha Mehrotra, Shreyas Sen
Purdue University

***Abstract*—Applications such as secure authentication, remote health monitoring require secure, low power communication between devices around the body. Radio wave communication protocols, such as Bluetooth, suffer from the problem of signal leakage and high power requirement. Electro QuasiStatic Human Body Communication (EQS-HBC) is the ideal alternative as it confines the signal within the body and also operates at order of magnitude lower power. In this paper, we design a secure HBC SoC node, which uses EQS-HBC for physical security and an AES-256 core for mathematical security. The SoC consumes 415nW power with an active power of 108nW for a data rate of 1kbps, sufficient for authentication and remote monitoring applications. This translates to 100x improvement in power consumption compared to state-of-the-art HBC implementations while providing physical security for the first time.**

***Index Terms*—Electro Quasi-static Human Body Communication, Physical Security, Mathematical Security, Low Power. AES-256, Secure Authentication, Physiological Monitoring**

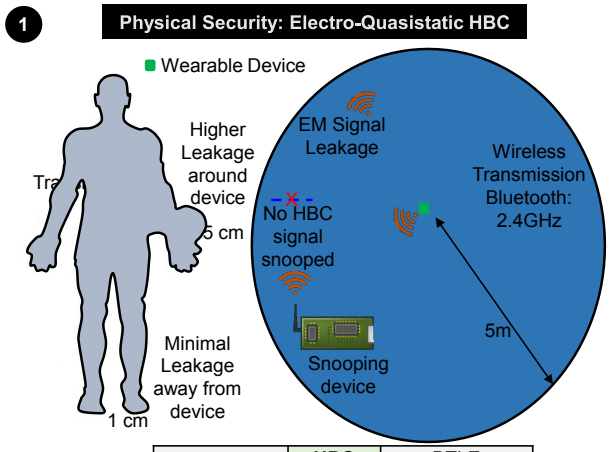
I. Introduction

Secure Communication around the Human Body is critical for applications like connected healthcare through physiological signal monitoring and secure authentication using wearable key, primarily needing data-rates (DR) <50kbps (Fig. 1). For example 256b key transfer with 50ms latency requires a data rate of 5.12kbps, or 1-ch EMG data acquisition with 16b resolution at 500sps results in a data rate of 8kbps. Perpetual battery-free operation or years of operating lifetime with small batteries for wearable patches calls for sub μW power consumption for these low-Data Rate communication, while simulatneously calling for end to end security. Human Body Communication (HBC) is the most promising technique for body area network communication achieving orders of magnitude lower power than traditional Bluetooth low energy [1], [2]. However, previous implementation used MHz frequency range leading to 1) $> 40\mu W$ power 2) lack of physical security, i.e. signals are snoopable by nearby attackers. Recently, in [3], the authors have described the physics of containing the transmission within the human body using low frequency (10kHz-1MHz) Electro-QuasiStatic (EQS) signals. While encryption provides strong-resistance against brute-force attacks, they are still vulnerable and the strongest security is achieved if the attacker doesn't have access to the physical signal itself. In this paper, we demonstrate end-to-end secure communication SoC through combination of AES 256 providing mathematical security and the first EQS-HBC IC implementation, providing physical security, all within 415nW total power, leveraging the low frequency operation of EQS-HBC.



	Need	HBC		BTLE
		ISSCC 16	ISSCC 19	
DR	<50 Kbps	100 Kbps	5 Mbps	~1 Mbps
Power	<1 uW	42.4 uW	40 uW	>2mW
1 Physical Leakage	No	Yes	Yes	Yes
2 Encryption	Yes	No	No	Yes

Fig. 1. Application of low data rate secure communication: Secure Authentication and physiological signal monitoring.



	HBC	BTLE
Private Space	~few cm	> 5m

Fig. 2. Electro-Quasistatic (EQS) HBC provides physical security by confining the signal within a close proximity of the human body. This increases the private space significantly compared to wireless radio wave based communication where the signal is available up to a range of 5 meters.

The frequency used for HBC heavily impacts the signal leakage (Fig. 2) and hence the vulnerability to a nearby attacker. Signal transmission in the EQS regime (f < 10s of MHz) enables signal confinement within a range of <1cm around most of the body and <15 cm near transmitting device, providing physical security.

Previous HBC implementations primarily used 50Ω termination at the receiver, resulting in a high loss at low frequencies ($f < \frac{1}{R_L C_G}$) due to the capacitive return path (Fig. 3a). Hence, the frequency range of operation for those implementations were generally >10MHz ([1], [2], [4], [5]) leading to significant signal leakage out of the body. Capacitive high impedance termination enables flat band HBC channel

978-1-7281-6031-3/20/$31.00 ©2020 IEEE

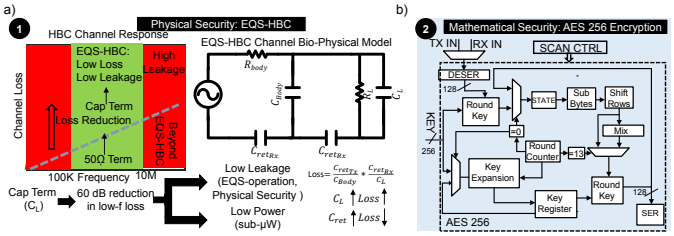


Fig. 3. a) Capacitive high impedance termination at the receiver-end enables flat-band channel response down to 100 kHz, enabling secure EQS-HBC. b) Block diagram of the AES 256 core providing mathematical security.

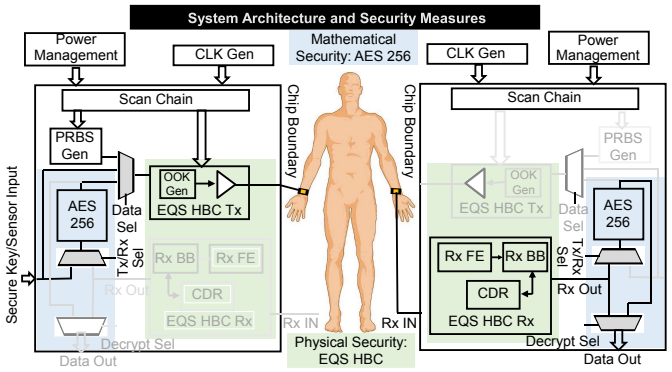


Fig. 4. Overall Architecture with the physical and mathematical security measures highlighted (green: physical security, blue: mathematical security).

($Loss = \frac{C_{retTx}}{C_{Body}} \frac{C_{retRx}}{CL}$), down to <100kHz (Fig. 3a). Hence, high impedance capacitive termination at the receiver allows low-loss at low frequency (0.1-1MHz) which enables 1) physical security through low-frequency EQS-HBC operation and 2) sub μW power due to low-carrier frequency (f_c) operation.

II. System Architecture

The overall SoC has a digital transmitter, AES-256 core and a mixed signal receiver (Fig. 4). Low-DR broadband implementation will suffer from high loss (< 100kHz), imposing stringent sensitivity requirements, motivating narrowband modulation to improve sensitivity. Also, it is necessary to choose a f_c < 10MHz for EQS physical security. A narrowband architecture with low carrier frequency and low baseband-frequency (for low-DR), minimizes overall system power. Along with EQS physical security an AES-256 core enables strong end-to-end security by providing mathematical security. Since, the signal leakage in EQS-HBC is very close to or below the noise floor, it is only possible for an attacker to snoop the signal through averaging over a long time. Frequency Hopping (FH) at the transmitter enhances the physical security of EQS-HBC by denying the attacker averaging capability over a narrow band of frequencies.

A. Transmitter Design

The *fully-synthesized* EQS-HBC transmitter (Fig. 5) has a programmable PRBS generator along with external data loading capability. The input data is deserialized, encrypted through an AES-256 core, serialized and subsequently used for OOK modulation, chosen for simplicity and low power. Direct Digital Synthesis (DDS) of the OOK signal is done by utilizing the baseband data as a control signal to a multiplexer

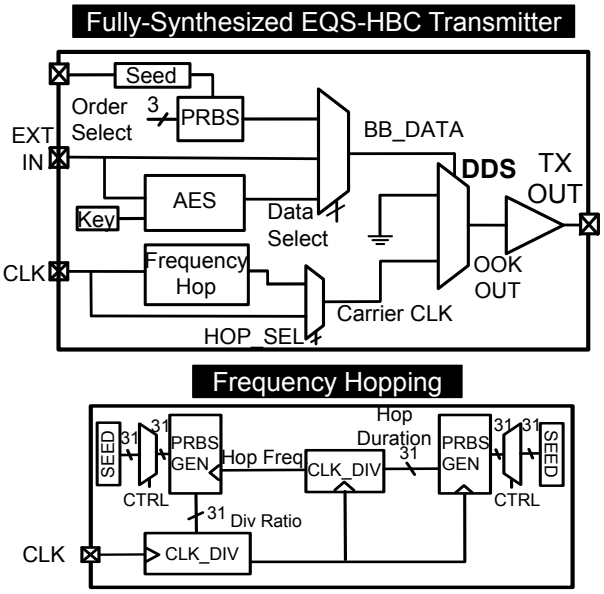


Fig. 5. Detailed Architectural Block diagram of the EQS-HBC Transmitter. The Frequency Hopping (FH)block generates the carrier frequency depending and selectively pass the carrier clock. The carrier frequency is derived from the input clock by varying the division factor on a pseudorandom manner, to enable Frequency Hopping, with a variable hop duration using a second PRBS generator. Both generators can be initialized with their own independent seed values. The output buffer is optimized to drive the equivalent capacitance seen at body (~2pF, i.e. return path capacitance at the wearable transmitter).

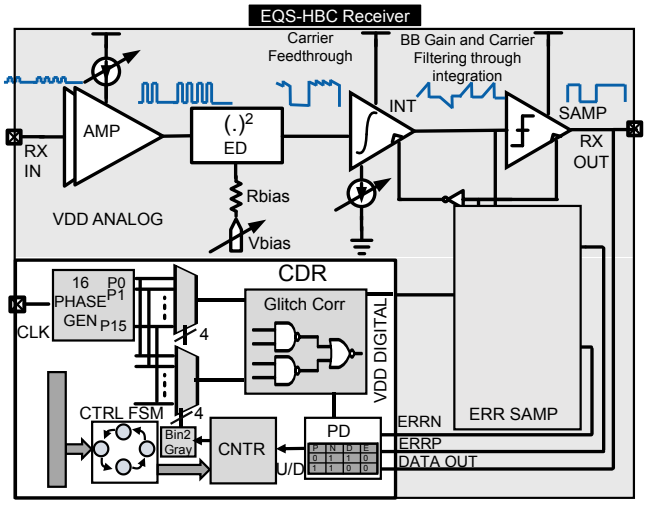


Fig. 6. Receiver architecture with the analog front-end consisting of amplifier, ED, integrator, sampler. The Clock Data Recovery loop requires two extra samplers and the control logic is synthesized.

B. Receiver Design

The EQS-HBC receiver front-end (Fig. 6) utilizes a 2-stage current starved self-biased common source amplifier, which is ultra-low power due to the low carrier frequency of EQS-HBC. A passive, gate biased, tunable, 4 stage envelope detector (ED) [6] is used for demodulation due to the relatively relaxed sensitivity requirements. This is also suitable for reception

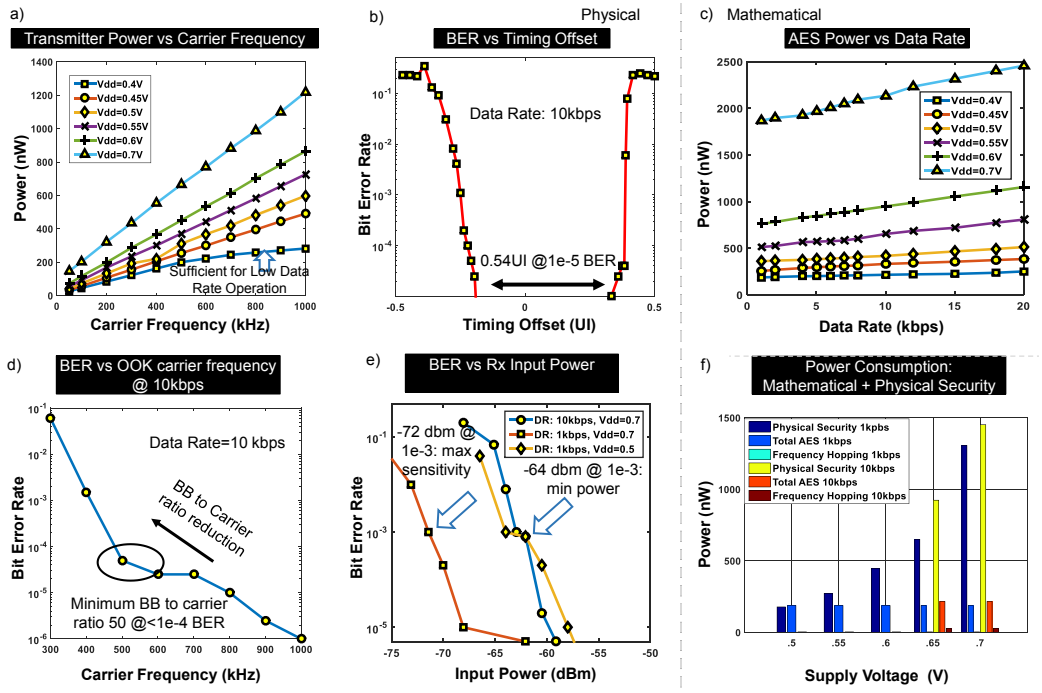


Fig. 7. Measurement results from the EQS HBC SoC. Physical security: a) Transmitter power consumption across different supply voltages . The Transmitter operates at 0.4V Vdd, which is sufficient for these low data rates, b) Bathtub curve at the receiver showing 0.54UI opening at 10^{-5} BER, d) BER performance keeping the data rate fixed at 10kbps and varying the carrier frequency, e) Sensitivity analysis of the receiver showing -72dbm sensitivity at the highest sensitivity point. Mathematical security: c) AES power consumption with frequency for different supply voltages. f) Overall system power consumption showing the contribution of each type of security measure.

of the transmitted signal with variable carrier frequency due to frequency hopping. Since the carrier to data rate ratio is 100 in this work compared to 10^6 in [6], a 4-stack ED was adopted. The ED restricts the maximum baseband data rate for a fixed carrier frequency, requiring tunability through bias control. A resettable integrator provides low pass filtering to reject the carrier feedthrough on the ED output and high gain at low power, utilizing the low-DR. A regenerative latch-based sampler is used to digitize the signal. An integrating Mueller-Muller CDR is used to provide phase alignment between data and clock from a digitally synthesized 16-phase clock generator, which uses off-chip crystal based reference without PLL, suitable for low carrier frequency operation.

C. AES 256 Encryption Core

The AES 256 core has a parallel data path implementation with 16 parallel sbox look up tables for each byte operation (Fig. 3b). The input data is deserialzied over 128 cycles for 128 bit plain text input. The 14 encryption rounds creates an additional 14 cycle latency. The ciphertext is serialized and transmitted over 128 cycles at the transmitter end.

III. Measurement Results

A. Power, Performance Results

The EQS-HBC SoC node, fabricated in 65nm CMOS technology, takes a $0.17mm^2$ active area. The transmitter power, dominated by the output buffer dynamic power, varies from 38nW (Data Rate=1kbps, f_c=100kHz) to 240nW (DR=10kbps, f_c=1MHz) (Fig. 7a). The AES core runs at baseband clock and its power consumption is dominated by leakage power for such low data rates. Hence, power is minimized by running the transmitter at a supply voltage of 0.4V achieving 42nW active power operation (Fig. 7c). Fig.7b shows the EQS-HBC receiver performance with 0.54UI timing margin for a BER of 10^{-5} at 10 kbps data rate. To minimize power, the carrier frequency is reduced keeping data rate constant and shows acceptable BER of 10^{-4} at 10 kbps DR and 500kHz carrier frequency, as shown in Fig. 7d . The receiver shows a sensitivity of $400\mu V$ (-64dBm with 50Ω for comparison) for minimum power operation at 0.5V supply, providing enough sensitivity even for 60dB EQS-HBC channel-loss with 0.4V transmitted voltage. With a higher supply voltage operation of 0.7V the receiver shows a sensitivity of -72dBm at 1 kbps and -63dBm at 10 kbps DR (Fig. 7e). Operating at the lowest power mode requires 227nW for physical security, with an additional 188nW for mathematical security through encryption (Fig. 7f).

B. Secure Key Transfer Demonstration

The feasibility of secure EQS-HBC is shown through a demonstration of authentication by secure key transfer between a wearable node with EQS-HBC IC and a PC. Fig. 8 shows the block diagram of the Tx/Rx PCB(5x5cm),through body received signal, out of body leakage waveforms during EQS-HBC transmission. The transmitter board, worn by the user on the wrist, sends the key at 5kbps data rate with carrier frequency of 500kHz and is decoded by an EQS-HBC receiver at the PC end, which is communicated to the PC through USB. The data reception shows a transmission latency of 0.4ms, sufficiently low for authentication applications. Out

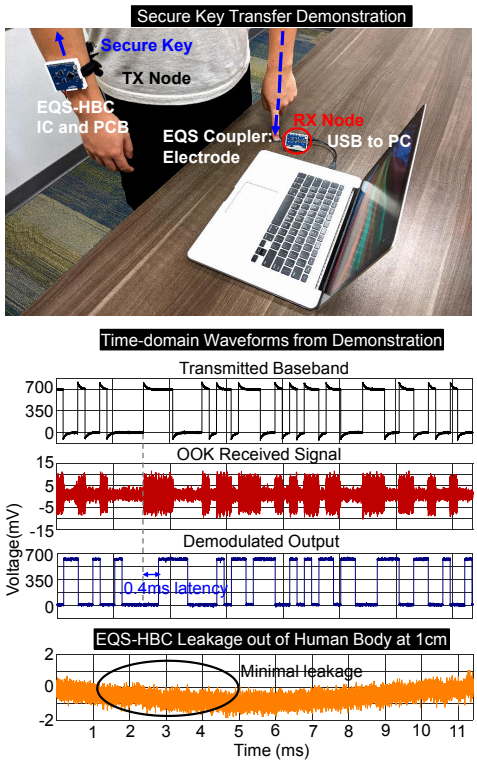


Fig. 8. Demonstration of Secure Key Transfer using EQS-HBC. The user transmits a key, which is securely transmitted through EQS-HBC to the receiver. Captured time domain waveforms showing the transmitted voltage, the received waveform and the demodulated output. Signal leakage measurements showing signal leakage below the noise floor.

Comparison Table with State of the Art HBC Transceivers

	This Work	H. Cho ISSCC '16	W. Saadeh JSSC '17	J. Jang ISSCC '18	J. Park ISSCC '19	J. Lee ISSCC '14
HBC Technique	EQS	Capacitive	Capacitive	Capacitive	Magnetic	Capacitive
Process	65nm CMOS	65nm CMOS	65nm CMOS	65nm CMOS	65nm CMOS	65nm CMOS
Supply Voltage	0.5	0.8	1.1	1.2	0.6	1.1
Modulation	OOK	OOK	8 P-OFDM BPSK	QPSK/BPSK	OOK	3-Level Walsh Coding
Data Rate	1-20Kbps	100kbps	0.2-2Mbps	80Mbps	5Mbps	60Mbps
Tx Power		21uW	0.87mW	1.7mW	18uW	1.85mW
Rx Power		42.5uW	1.1mW	8mW	24uW	9.02mW
Total Power		63.5uW	1.97mW	9.7mW	42uW	10.87mW
Sensitivity	-64dBm @10^{-3} BER	-60dBm @ 10^{-5} BER	-83.1dBm @ 10^{-3} BER	-40dBm @ 10^{-5} BER	-56dBm @ 10^{-3} BER	-58dBm @ $<10^{-5}$ BER
Operating Frequency	100KHz-1 MHz	10/13.56 MHz	20-120 MHz	20-60 MHz 140-180 MHz	40 MHz	40-80 MHz
Encryption		No	No	No	No	No
Physical Security		No	No	No	No	No

Fig. 9. Comparison table comparing the EQS-HBC SoC with other state of the art HBC implementations.

of body leakage at 1cm distance is masked by the noise floor, proving the physical security of EQS-HBC. Comparison with other state-of-the-art HBC implementations show a 100x reduction in power consumption, while providing end-to-end physical and mathematical security(Fig. 8, Fig. 9a). The power breakdown of the different blocks for lowest power operation at 1kbps (Fig. 10b), shows 233.6nW Tx, 178nW Rx operation (including leakage power) and 108nW overall active power for both physical and mathematical security. The die micrograph and the demonstration PCB is shown in Fig. 11.

IV. Conclusion

This paper presents a low power EQS-HBC SoC with a complete transceiver and AES 256 core for applications like

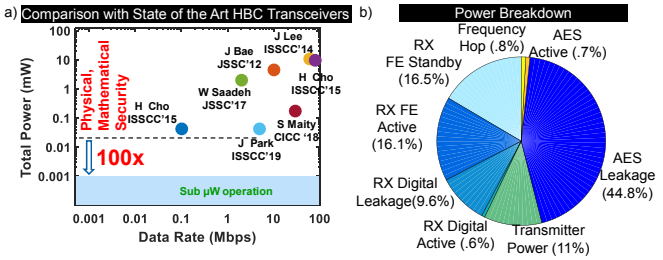
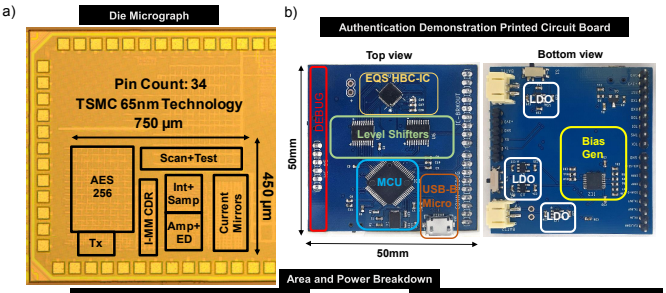


Fig. 10. a) Comparison of the EQS-HBC SoC with other state of the art HBC implementations showing lowest power physically and mathematically secure operation with >100x improvement in power consumption. b) Relative power breakdown of different blocks at lowest power mode.



c) Area and Power Breakdown

Minimum Power Mode: -64dBm @ 415nW | Maximum Sensitivity Mode: -72dBm @ 1.8µW

	Block	Area (μm^2)	Standby Power (nW) $V_{dd_{Tx}}, V_{dd_{Rx}}$ 0.4, 0.5	Active Power @1kbps (nW)	% Standby Power	Total Power (nW)	Standby Power (nW) $V_{dd_{Tx}}, V_{dd_{Rx}}$ 0.4, 0.7	Active Power @10kbps (nW)	% Standby Power	Total Power (nW)
Tx	PRBS Gen + Transmission+Fhop	2025	11.2	34.8	24.30	233.6	11.2	210.8	5.04	435.6
	AES 256	72875	184.4	3.2	98.30		184.4	29.2	86.33	
Rx	Analog Front End	67700	68.5	67	50.55	178	490	770	38.89	1451.8
	Digital : CDR+CLK Gen	24500	40	2.5	94.12		175.7	16.1	91.61	

Fig. 11. a) Die Micrograph of the EQS-HBC IC. b) Top and Bottom view of the demonstration PCB showing the different components. c) Table with the area and power breakdown of the different blocks.

secure authentication, remote health monitoring. The primary design focus has been on providing security (physical, mathematical) and minimizing the total power for low data rate applications instead of energy efficiency (done for higher data rates).The current design achieves 100X lower power while providing stronger security both physically (private space <15cm) and mathematically (AES 256 encryption), opening new possibilities in medical/authentication applications.

References

[1] J. Park *et al.*, "17.6 a sub-40w 5mb/s magnetic human body communication transceiver demonstrating trans-body delivery of high-fidelity audio to a wearable in-ear headphone," in *2019 IEEE ISSCC*, Feb 2019.

[2] J. Jang *et al.*, "4-camera vga-resolution capsule endoscope with 80mb/s body-channel communication transceiver and sub-cm range capsule localization," in *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*, Feb 2018, pp. 282–284.

[3] D. Das *et al.*, "Enabling covert body area network using electroquasistatic human body communication," *Scientific Reports*, vol. 9, no. 1, pp. 169:1–169:29, Mar. 2019.

[4] W. Saadeh *et al.*, "A 1.1-mW Ground Effect-Resilient Body-Coupled Communication Transceiver With Pseudo OFDM for Head and Body Area Network," *IEEE JSSC*, vol. 52, no. 10, pp. 2690–2702, Oct. 2017.

[5] H. Cho *et al.*, "21.1 A 79pj/b 80mb/s full-duplex transceiver and a 42.5W 100kb/s super-regenerative transceiver for body channel communication," in *2015 IEEE ISSCC*, Feb. 2015, pp. 1–3.

[6] V. Mangal *et al.*, "28.1 a 0.42nw 434mhz -79.1dbm wake-up receiver with a time-domain integrator," in *2019 IEEE ISSCC*, Feb 2019, pp. 438–440.