Sub-μWRComm: 415-nW 1–10-kb/s Physically and Mathematically Secure Electro-Quasi-Static HBC Node for Authentication and Medical Applications

Shovan Maity, *Graduate Student Member, IEEE*, Nirmoy Modak, *Graduate Student Member, IEEE*, David Yang, *Graduate Student Member, IEEE*, Mayukh Nath, Shitij Avlani, Debayan Das, *Graduate Student Member, IEEE*, Josef Danial, Parikha Mehrotra, and Shreyas Sen, *Senior Member, IEEE*

***Abstract*— Low-power secure communication is one of the key enablers of applications, such as secure authentication and remote health monitoring. Radio wave-based communication method, such as Bluetooth, suffers from high-power requirements and physical signal leakage. Electro-quasi-static human body communication (EQS-HBC) utilizes the conductivity of the human body to use it as a communication medium and confine the signal within a close proximity of the body and enable low power consumption through low-frequency operation. This makes EQS-HBC an attractive alternative for such low-power, low-data-rate secure communication. In this article, we present the first >1 kb/s Sub-μW WeaRable Communication (Sub-μWRComm), a secure EQS-HBC node, which uses EQS-HBC for physical security and an AES-256 engine for mathematical security and operate at sub-μW power budget. The signal confinement property of EQS-HBC is demonstrated through finite element method (FEM) simulations and leakage measurements, establishing its security property. The Sub-μWRComm system consumes only 415-nW total power, with 108-nW active power at the lowest power mode, operating at a data rate of 1 kb/s with −64-dBm sensitivity making it suitable for authentication and remote monitoring applications. This work presents a 100× improvement compared with state-of-the-art HBC implementations while providing simultaneous physical and mathematical security for the first time.**

***Index Terms*— Electro-quasi-static human body communication (EQS-HBC), low power AES-256, mathematical security, physical security, physiological monitoring, secure authentication.**

I. Introduction

SECURE low power communication for wearable devices is critical for applications, such as secure authentication and physiological signal monitoring for connected healthcare/medical applications (see Figs. 1 and 2). These applications typically require data rates in the range of tens of kilobit per second, as shown in Fig. 1. For example, transmitting a 1024-bit secret key with a latency of 500 ms requires a data rate of 2.048 kb/s. Similarly, a one-channel electromyography (EMG) data acquisition with a 16-bit resolution and at a rate of 500 sps requires a data rate of 8 kb/s. For these devices to become battery-less or have years of lifetime with small batteries, it is essential for them to operate with sub-μW power. It is also necessary to simultaneously ensure the end-to-end secure communication for these security-critical applications. These require a low-power secure communication method. Currently, wireless radio wave-based communication, such as Bluetooth, is commonly used among wearable devices. However, Bluetooth suffers from higher power consumption [1] and the inherent property of widely radiating the transmitted signal, making it accessible to a nearby attacker. Human body communication (HBC) is a promising alternative communication method, which uses the conductive property of the human body to communicate among these devices in close proximity to the body.

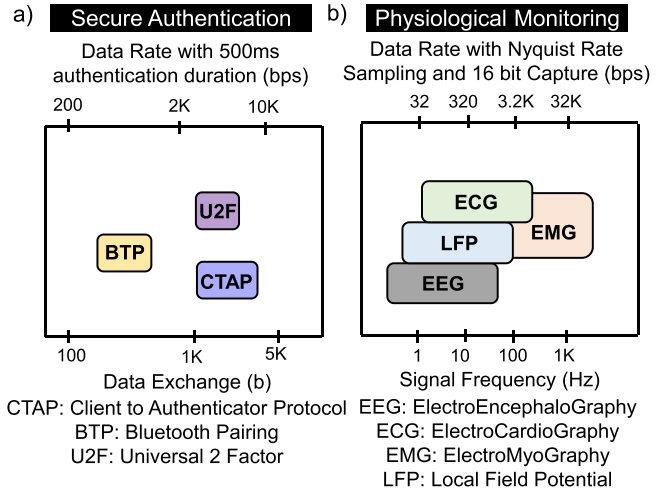


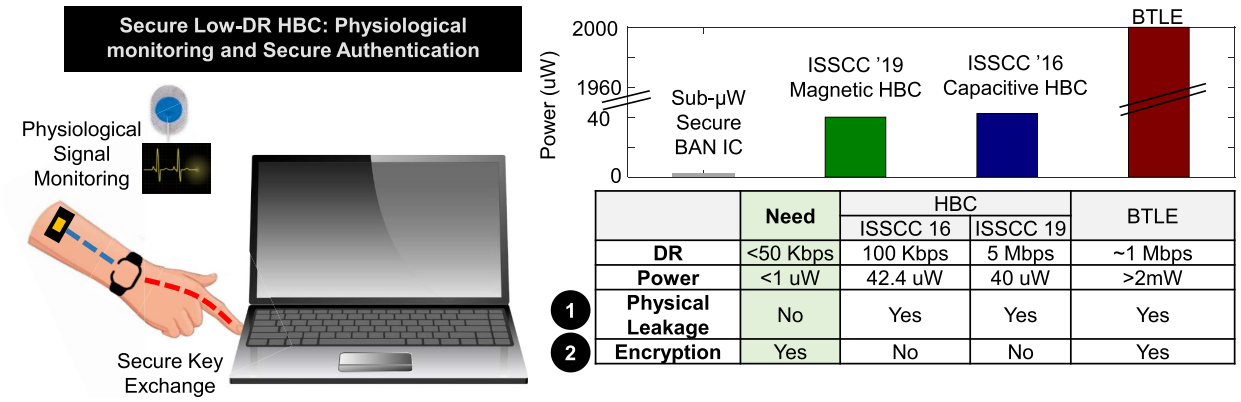
Fig. 1. Data rate requirement for (a) common authentication protocols and (b) physiological signal monitoring applications. Most of these applications require a data rate <10 kb/s making it suitable to be implemented with Sub-μWRComm system.

Manuscript received June 9, 2020; revised August 13, 2020 and October 14, 2020; accepted November 9, 2020. Date of publication January 20, 2021; date of current version February 24, 2021. This work was supported in part by the Air Force Office of Scientific Research YIP Award under Grant FA9550-17-1-0450 and in part by the National Science Foundation CRII Award under Grant CNS 1657455. This article was approved by Guest Editor Mark Oude Alink. *(Corresponding author: Shovan Maity.)*

The authors are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: maity@purdue.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JSSC.2020.3041874.

Digital Object Identifier 10.1109/JSSC.2020.3041874



	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. 2. Application of low-data-rate secure communication: secure authentication and physiological signal monitoring for medical applications.

In HBC, the signal is coupled to the body through an electrode and is communicated utilizing the body as the communication channel. The signal is received either through a wearable or by a device that is touched by the user. HBC can be primarily classified into two categories: capacitive and galvanic HBC. The signal is coupled into the body and also received through a single electrode in capacitive HBC [2]–[8]. The body provides the forward path of communication and the return path is formed through the parasitic capacitances between the device ground planes and the surrounding environment. In galvanic HBC [9], the signal is applied differentially into the body and received through differential termination. In this case, the body provides both the forward and the return path of communication. Magnetic HBC [10] has also been demonstrated, which couples magnetic fields into the body for communication.

HBC achieves an order of magnitude lower power consumption than radio wave-based communication, primarily by operating at a significantly lower frequency. Most previous HBC implementations operate in the frequency range of 10–100 MHz. The HBC channel has been widely characterized as a high-pass channel with the lowest loss beyond 20 MHz [3]–[7]. Most circuit implementations use this frequency range and are designed using narrowband modulation techniques [11]–[16], leading to: 1) >40-μW power and 2) lack of physical security, i.e., signals are snoopable by nearby attackers, as the human body acts as an radiative antenna at these frequencies. Although these implementations are lower power and more energy efficient than Bluetooth, still, it does not utilize the full potential of body as a private, wire-like communication channel. The high-pass channel response can be attributed to the low-impedance, resistive termination used for these measurements. It has been shown that a high-impedance capacitive termination makes the channel response flat band down to sub-MHz frequencies and enables the body to be used as a broadband communication channel [2], [17]–[19]. This has opened up the low-frequency range to be utilized through https://www.ted.com/talks/shreyas_sen_how_your_body_will_play_an_integral_role_in_the_future_of_wearable_security electro-quasi-static human body communication (EQS-HBC) [20]. EQS-HBC uses single-ended excitation and termination-like capacitive HBC. However, it operates at lower frequencies compared with capacitive HBC to minimize signal leakage and uses a high-impedance capacitive termination at the receiver end, unlike 50 Ω or low-impedance termination used in capacitive HBC. The operating frequency of HBC has a strong effect on the signal leakage out of the body and, hence, the vulnerability of communication to a nearby attacker. Recent advancements in the physical understanding of HBC have shown that operating in the EQS regime around the MHz frequency range enables signal confinement within a few centimeters around most of the body and < 15 cm near the transmitting device [20]. This provides physical security by denying an attacker physical access to the transmitted signal. Hence, low-frequency operation enables: 1) physical security by operating in the EQS regime and 2) sub-μW power consumption due to low-carrier frequency operation. Traditionally, body area network (BAN) nodes employ lightweight authentication techniques for mathematical security [21]–[26]. While encryption provides strong-resistance against brute-force attacks, they can still be broken if an attacker has physical access to the signal. Any such remote phishing attack can be thwarted if the attacker is denied access to the physical signal itself. In this article, we present Sub-μW WeaRable Communication (Sub-μWRComm), which demonstrates an end-to-end secure communication node at sub-μW power through a combination of AES 256 providing mathematical security and EQS-HBC providing physical security. The complete system consumes 415-nW total power in the lowest power mode for a 1-kb/s data rate, leveraging the low-frequency operation of EQS-HBC.

A. Motivation

Secure authentication [27] and physiological signal monitoring applications require low-power secure communication in wearable devices at low data rates, often less than 10 kb/s. For example, a data rate of 7.5 kb/s is sufficient for secure authentication using FIDO2 protocol even with 50% communication overhead. Similarly, data acquisition using a Maxim Integrated MAX30102 heart rate/SpO2 sensor will need a data rate of around 5 kb/s. The low-power and physical security property of EQS-HBC makes it an ideal communication method for

these devices to communicate with off-body device at low data rates. As a result, these devices can have long battery lifetime or even be battery-less with energy harvesting. The signal confinement property also enables physical security, not present in radio wave propagation or current HBC implementations.

The key contributions of this article are as follows.

1) This article shows the first demonstration of a sub-μW wearable communication (Sub-μWRComm) node for low-data-rate applications, such as secure authentication and physiological health monitoring. The Sub-μWRComm node consumes 415-nW power at the lowest power mode, making it 100× more power efficient than state-of-the-art implementations.
2) First demonstration of physically and mathematically secure communication through EQS-HBC and AES 256-based encryption.
3) Establishing the security property of EQS-HBC through finite element method (FEM)-based simulation and signal leakage measurements.

The rest of this article is organized as follows. Section II discusses the signal confinement and security aspect of EQS-HBC through simulations and measurements. Section III discusses about the choice of operating frequency and transceiver architecture based on communication channel and signal leakage characteristics. Section IV discusses the detailed design of the transmitter, receiver, and AES 256 blocks. Section V discusses about the measurement results and secure key transfer demonstration with conclusion in Section VI.

II. EQS-HBC: Physical Security

The operating frequency of HBC plays a critical role in the safety of HBC. In HBC, the body acts as the communication channel due to its conductivity property. However, the same finite conductivity of the human body also provides it with an antenna-like radiative property [15], [28]. The optimum frequency of radiation is dependent on the height of the person and is around 40 MHz for a person of 6-ft height (for a ($\lambda/4$) antenna). When the body shows antenna-like radiative property, it operates in the electro-magnetic regime. In this case, the operating wavelength is comparable to the size of the body and the electric (E) and magnetic fields (H) are interrelated to each other through Maxwell's equations [see Fig. 3(a)] and both of them have non-zero time derivatives. On the other hand, in the electro-quasi-static regime, the wavelength of communication is significantly larger than the size of the HBC channel, as shown in Fig. 3(b). In terms of fields, the time derivative of H-field is zero and the E-field is independent on H, making the communication electro-quasi-static [see Fig. 3(a)]. Similarly, for a magneto-quasi-static scenario, the E-field is not time varying, and hence, the H-field is not dependent on it. For an electrostatic scenario, both the E and H fields are time-invariant and independent of each other. The dependencies of E and H fields on each other during the different modes of operation are shown in Fig. 3(a).

The validity of the electro-quasi-static approximation can be determined by the approximation error introduced by ignoring the time-varying H-field on the overall E-field calculation.

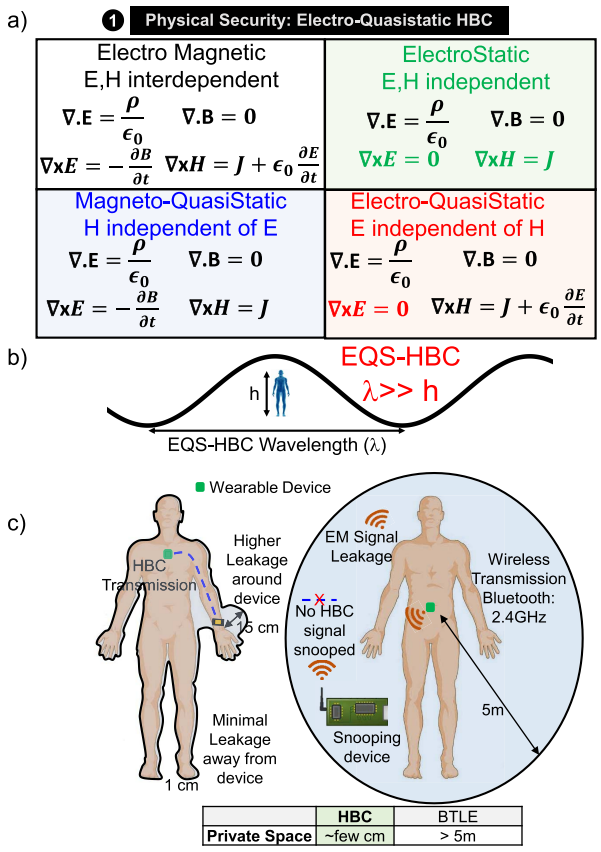


Fig. 3. (a) Maxwell's equations for electric and magnetic fields for electromagnetic, electrostatic, magneto-quasi-static, and electro-quasi-static scenario. (b) These equations in the electro-quasi-static scenario translate to a significantly larger wavelength compared with the channel length, i.e., the size of the human body. (c) EQS-HBC provides physical security by confining the signal within a close proximity of the human body.

For a 1% approximation error the electro-quasi-static approximation holds true for frequencies up to 2.23 MHz [20]. When operating in the electro-quasi-static regime, the signal is primarily confined within a close proximity of the human body. As a result, it is not possible for an attacker to snoop the signal remotely, away from the body. In contrast, in case of Bluetooth, the signal is available up to 5–10 m away from the body [29], making it vulnerable to remote snooping. EQS-HBC enhances the private space of communication significantly compared to radio wave communication techniques, as shown in Fig. 3(c). This section builds on the concepts from [20] and looks into the signal leakage properties of EQS-HBC and its dependence on operating frequencies through FEM-based simulations and experimental measurements.

A. FEM Simulations of Leakage

Simulations are carried out in Ansys High Frequency Structure Simulator (HFSS), an FEM-based simulator, to understand the electric and magnetic field distribution in and around the body while applying excitation into the body at different frequencies. The NEVA Electromagnetics LLC VHP-Female v2.2 model of a 162-cm tall, 60-year-old female subject is

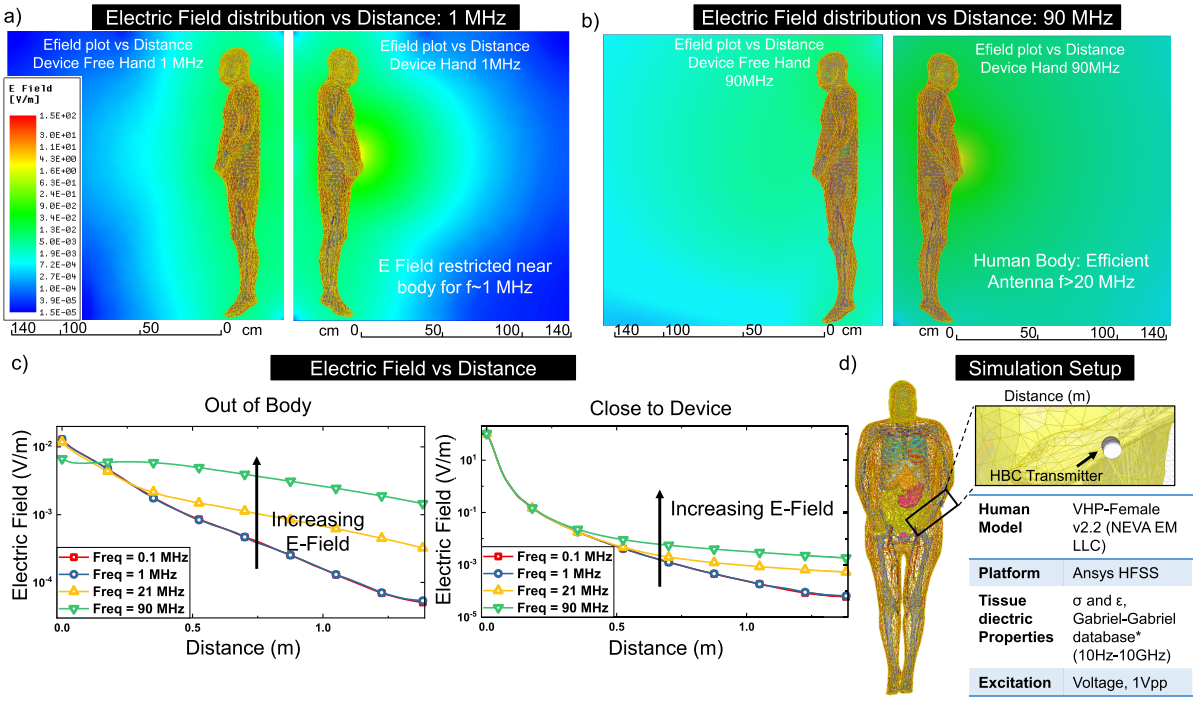


Fig. 4. Simulation results for physical security evaluation of EQS-HBC. (a) Electric field intensity versus distance at an excitation frequency of 1 MHz along a plane across the device and non-device hand obtained from HFSS simulations. (b) Similar plot for an excitation frequency of 90 MHz. (c) Electric field versus distance plot for different frequencies, showing increasing field leakage with increasing frequency. (d) Details of the HFSS simulation setup.

used for the HFSS simulations. There are 26 tissue materials and 184 individual tissue parts in the model and the continuity between the tissue layers were maintained within the model. The dielectric properties of the model are amended with the experimental data from [30] for the sub-10-MHz frequency range, as the original model did not have the appropriate material properties for this frequency range. The signal excitation is provided through a disk-shaped conductor into the body near the wrist. The radius of both the signal electrode and the ground plate is 1.5 cm, the thickness of the signal electrode is 2 mm, and the thickness of the ground plate is 3 mm. The plates are separated from each other by 1 cm with air dielectric. The ground plate of the transmitter is left floating. An alternating potential difference is applied between these two conductors to act as the excitation source. The simulation setup and the details of the model and signal excitation are shown in Fig. 4(d). Fig. 4(a) shows the electric field distribution versus distance from the body for an excitation frequency of 100 kHz. The field intensities on the plane across device hand are larger than the device free hand as also seen from the electric field intensity versus distance plots in Fig. 4(c). These plots show that the signal leakage is maximum close to the device hand. The electric field intensity for an excitation frequency of 90 MHz is shown in Fig. 4(b), showing significantly higher field intensity compared to 100-kHz excitation. The electric field plots in 4(c) shows increasing electric field for the same distance with increasing frequency. The field intensities are also higher close to the device hand. The field intensities in this case are representative of this particular posture and in an open environment away from big conductive objects.

B. Measurements: Signal Leakage

Signal leakage measurements are carried out for different excitation frequencies to quantify the private space in case of EQS-HBC. A wearable transmitter is worn on the wrist and excites a 3.3-V signal into the body. A spectrum analyzer is used to measure the signal leakage out of the body. The experiments are carried out in an anechoic chamber to minimize external sources of interference affecting the measurements. The measurements are also carried out away from the wall to minimize any effect of a large object affecting signal leakage. The posture of the participants is also kept similar to the simulation model with arms by the side of the torso. Averaging is done at the spectrum analyzer to achieve a low noise floor and emulate the best case scenario for an attacker trying to snoop signals of a particular frequency through averaging. Similar to the simulations, one set of measurements is done along a plane with the transmitting device [see Fig. 5(b)]. The other set of measurements is done along the non-device wearing hand [see Fig. 5(a)]. The measurements show that the signal leakage near the non-device hand is nearly 20 dB less compared to the device wearing hand, particularly for low frequencies. The signal leakage also increases with the excitation frequency. The IEEE 802.15.6 standard, which uses a 21-MHz frequency band, shows almost 40 dB more leakage compared to frequencies in the EQS regime. With a 3.3-V

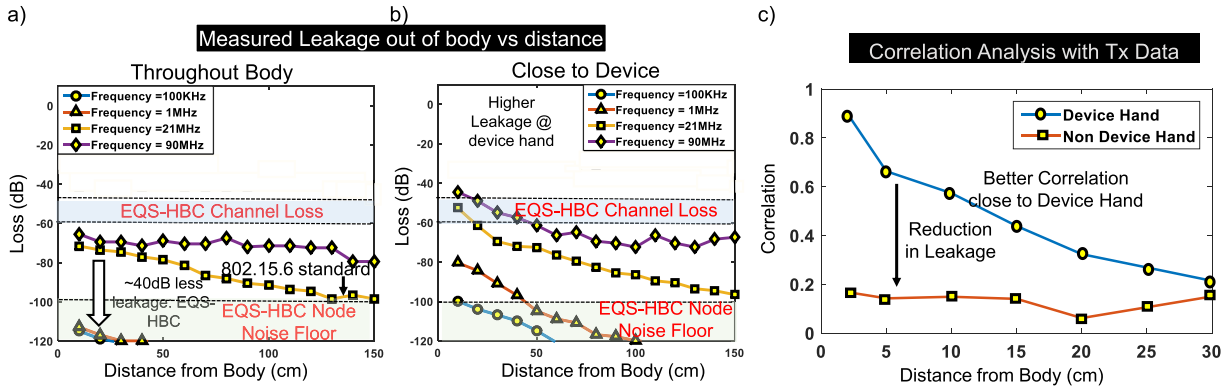


Fig. 5. Signal leakage measurement results: signal loss versus distance plot along (a) non-device wearing hand and (b) device wearing hand. (c) Measured correlation of leakage at different distances with the transmitted data for a transmitted frequency of 1 MHz.

excitation, it is possible to sense signals for up to 120-dB loss. With a transmitted voltage of 0.4 V, the sensitivity limit will be corresponding to 100-dB loss. Hence, it is possible to snoop the signal up to 40 cm away from the body near the device wearing hand when operating at a frequency of 1 MHz. However, for any other part of the body, the signal leakage is below this noise floor even for a distance of 10 cm. For a 100-kHz operation, the signal falls below the noise floor for a distance >10 cm even near the device hand. These experiments corroborate with the simulation results and shows increasing leakage with frequency and higher leakage close to the device. Fig. 5(c) shows the correlation of the leakage signal with the transmitted signal at different distances away from the body. The time-domain leakage signal is captured with an oscilloscope. The correlation falls to 0.4 at a distance of 15 cm from the body even near the device hand. These results show that by operating in the EQS domain, it is possible to enhance the private space of HBC significantly and ensure physical security by denying an attacker from snooping the transmitted signal. It is interesting to note that reducing only the transmit power can also reduce the signal leakage out of the body. However, in that scenario, the received signal will reduce for both the intended and the unintended receiver (attacker), whereas EQS-HBC reduces signal only for the unintended receiver, keeping the signal for the intended receiver unchanged.

III. System Architecture

A. System Design Choices

1) Operating Frequency: The communication frequency is primarily determined by the frequency response of the human body as a communication channel, the signal leakage response out of the body and the circuit power consumption.

Fig. 6(a) shows the simplified bio-physical circuit model of the human body as a communication channel. The human body channel response is strongly dependent on the receiver input impedance, i.e., the channel termination impedance (R_L and C_L). A resistive termination at the receiver end will result in a high-pass frequency response due to the capacitive return path, with a cutoff frequency of

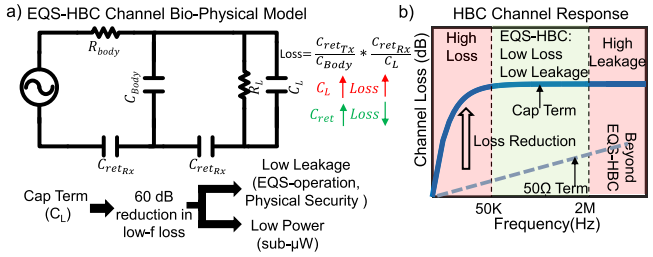


Fig. 6. (a) Simplified circuit model of human body as a communication channel at these low frequencies. (b) Capacitive high-impedance termination at the receiver end enables flat-band channel response down to 50 kHz, enabling secure EQS-HBC. The range of EQS operation is determined by assuming a 1% approximation error to be tolerable for electric field estimation.

$f = (1/R_L C_G)$. Most previous implementation of HBC systems use a low-impedance 50-Ω termination at the receiver end [11]–[15], [31], very similar to radio frequency circuit implementations. The return path capacitance for a wearable device of watch form factor is in the range of 1–2 pF [32]. Hence, a 50-Ω termination results in a channel response with a low-frequency roll-off in the range of tens of megahertz, as shown in Figs. 6(b) and 7(a) and (b). As a result, previous HBC implementations primarily operated in the 10–100-MHz range. However, a capacitive termination at the receiver end [2], [6], [17], [19], [33] instead of resistive termination will result in a frequency response, which is independent of frequency. The channel loss in this case will be determined by the return path capacitances (C_{retTx}, C_{retRx}), the load capacitance (C_L), and the parasitic capacitance between the body and the surrounding environment (C_{Body}). Solving the simplified circuit model shown in Fig. 6(a) for a purely capacitive termination (C_L) will provide us with a channel loss of $(C_{\text{retTx}}/C_{\text{Body}})(C_{\text{retRx}}/C_L)$. Hence, it is possible to achieve a flat-band frequency response by having a purely capacitive input impedance at the receiver end. However, in reality, there will be a resistive component of the receiver input impedance. This will create a low-frequency roll-off dependent on the resistive component. For a receiver impedance of 5 MΩ and a return path capacitance of 2 pF, the cutoff frequency will be 160 kHz. Hence, a primarily capacitive termination with a very high resistive component

can enable us to achieve a channel response, which is almost constant until sub-100-kHz frequencies [see Fig. 7(b)]. Hence, from a channel loss perspective, any frequency >50 kHz is suitable for communication.

The discussion in Section II showed that operating in the electro-quasi-static regime of <2 MHz enables the HBC transmission to be confined within a few centimeters of the body, providing physical security. This limits the upper range of the communication frequency, as any communication beyond this frequency range will result in significant signal leakage out of the body. Hence, an operating frequency in the range of 50 kHz–2 MHz is necessary to satisfy the requirement of security and optimum channel response, as shown by the green shaded region in Fig. 6(b). From the receiver power consumption perspective, it will be optimal to operate at the lowest possible frequency. This will reduce the dynamic power consumption of the digital circuits and also reduce the bias current requirements of the analog circuits by relaxing bandwidth requirements. It is also possible to operate at low supply voltages by reducing the operating frequencies and leakage power consumption significantly.

2) Narrowband Versus Broadband: The data rate requirement for applications, such as secure authentication and remote physiological monitoring for medical applications, is in the range of tens of kilobits per second. A broadband implementation of such communication will result in operating in the tens of kilohertz frequency range, which is not optimum as discussed before. Hence, it is necessary to up-convert the transmitted signal to a higher frequency through modulation. This makes the overall system narrowband as opposed to broadband. An ON–OFF keying (OOK)-based modulation is chosen for low-power implementation. It is not necessary to have any higher order modulation for spectral efficiency since there is enough bandwidth available for these low data rates. The carrier frequency is dependent on the carrier, baseband frequency separation needed at the receiver for down-conversion. An envelope detector (ED)-based non-coherent demodulation scheme is used at the receiver end to minimize power consumption. To achieve high sensitivity at low power, a carrier-to-baseband ratio of 100 is sufficient for the highest sensitivity mode. This makes a carrier frequency of 1-MHz optimum for a data rate of 10 kb/s. Hence, to satisfy the constraint of low-power and secure operation, a narrowband OOK communication link is implemented with a nominal carrier frequency of 1 MHz. In addition, mathematical security is provided by incorporating an AES-256 engine in the design.

3) Low Power Versus Low Energy/Bit: We also focus on optimizing the design for low power instead of lower energy/bit. These applications have incoming data, which can be continuous (physiological signal monitoring) and not short bursts of event-driven data. Hence, there are two design choices using a high data rate, high energy efficiency, relatively higher power, duty-cycled transceiver, or using a low data rate, low power, lower energy efficiency, continuously on the transceiver. A high-data-rate transceiver will need to be turned on and off periodically, which will reduce energy efficiency. Moreover, such a system will require additional memory to store intermediate samples and a wake-up receiver to turn the main receiver on. The communication latency will also increase. Operating at low energy/bit also generally requires operating at a higher data rate and hence at a higher operating frequency. This will also hamper the physical security due to increased signal leakage. Hence, we focus on optimizing the design for low-power low-data-rate operation instead of low energy/bit operation.

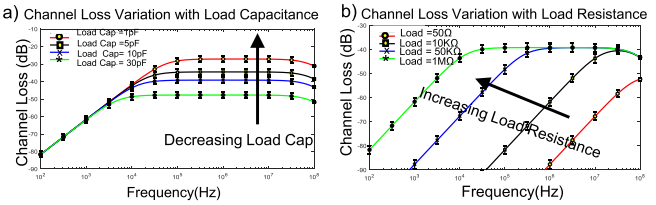


Fig. 7. (a) and (b) Simulation results showing channel loss variation with changing load capacitance and resistance, respectively. A high-resistance, lower capacitance load termination enhances the low-frequency channel loss. The error bars on the simulation results correspond to ±20% variation of the return path capacitance.

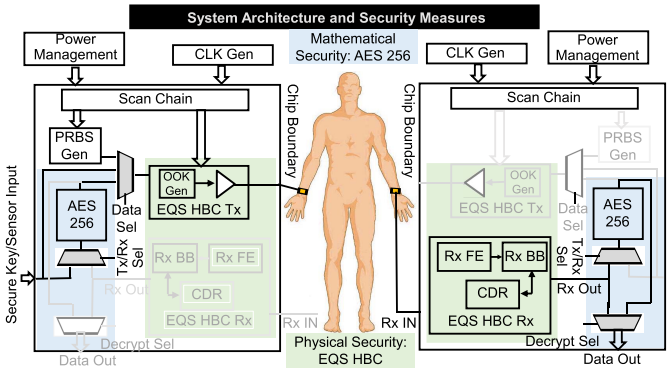


Fig. 8. Overall architecture with the physical and mathematical security measures highlighted (green: physical security and blue: mathematical security).

B. Circuit Design Choice

The circuit architecture is designed primarily taking the low power constraint into account. A passive ED is chosen as the demodulation element due to its low-power operation, as well as its lack of need for a local carrier. However, it will result in a sensitivity hit, which is alleviated by two-stage amplification before the ED. An integrator is used to act as a low power gain element. Since the OOK demodulation results in a constant amplitude signal, time-domain integration can be used to provide gain. Since the carrier frequency is significantly larger than the baseband data rate, time-domain integration will also cancel most of the carrier feedthrough at the output of the ED. The integrator also acts as a filter along with providing low-power, low-frequency gain. Finally, a sampler is used to digitize the output into bits for its low-power operation.

IV. SUB-μWRCOMM NODE DESIGN

The Sub-μWRComm node has a digital transmitter, an AES-256 core, and a mixed-signal receiver (see Fig. 8).

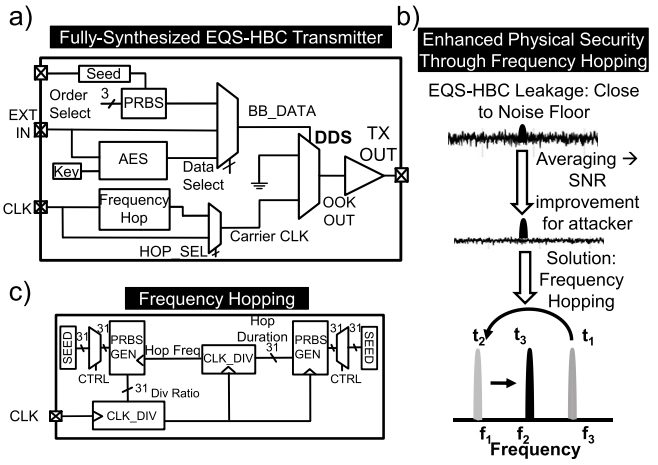


Fig. 9. (a) Detailed architectural block diagram of the EQS-HBC transmitter. (b) FH enhances the physical security of EQS-HBC by varying the carrier frequency and denying an attacker the opportunity to recover the signal leakage through narrowband filtering and averaging. (c) FH block generates the carrier frequency depending on a division factor determined by a PRBS generator.

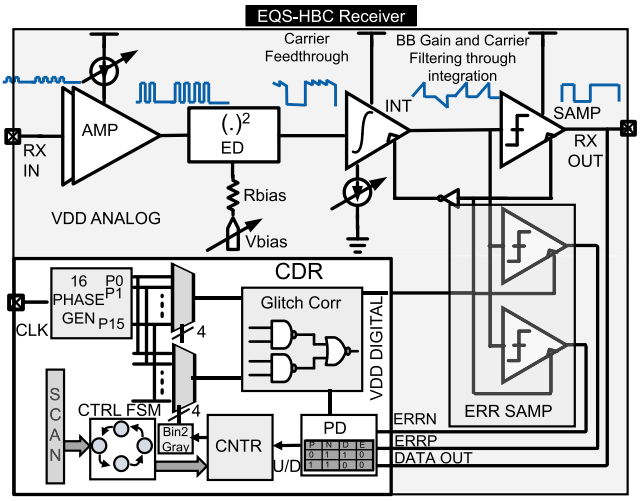


Fig. 10. Receiver architecture with the analog front end consisting of amplifier, ED, integrator, and sampler. The CDR loop requires two extra samplers. The control logic is synthesized.

As discussed in Section III, a narrowband OOK-based transceiver with a carrier frequency in the range of 50 kHz–2 MHz provides the best tradeoff in terms of physical security, receiver sensitivity requirements, and circuit power consumption. An AES-256 encryption core is used to provide mathematical security along with the physical security already provided by EQS-HBC, enabling strong end-to-end security. The physical security feature is further enhanced by employing frequency hopping (FH) at the transmitter. The constant change in frequency at the transmitter end will make it more difficult for an attacker to employ a narrowband averaging-based approach to recover the leakage signal, which is very close to the noise floor. Non-coherent detection is used at the receiver end to demodulate the transmitted signal with varying carrier frequency due to FH. The overall system architecture along with the different security measures is shown in Fig. 8

A. Synthesizable Transmitter Design

The transmitter is designed to be fully synthesizable and is shown in Fig.9. The transmitted data can be generated from a programmable pseduo random bit sequence (PRBS) generator or can be loaded from an external data source. The input serial data are converted to 128-bit data blocks and applied to the AES-256 engine for encryption. The encrypted output data are again serialized before being OOK modulated and transmitted. The OOK modulation is chosen for its simplicity of modulation/demodulation and low-power operation. The OOK modulation is done through direct digital synthesis (DDS) by utilizing the baseband data as a control signal to a multiplexer for selectively passing the carrier clock.

The carrier clock is generated from an input clock by dividing it. The division factor is varied in a pseudorandom manner to enable FH at the transmitter. The duration of operation at a particular frequency is also variable and is determined through a 32-bit pseudorandom generator. This enables FH with a variable hop duration. The two pseudorandom generators for clock frequency generation and determining the hop duration are independent of each other and can be initialized with their own independent seed values. The FH scheme enhances the physical security aspect of EQS-HBC. Although the signal leakage is low in EQS-HBC and falls below the noise floor for distances >40 cm from the device hand, it is still possible for an attacker to use narrowband filtering and averaging techniques to enhance the received SNR when the transmission frequency is known. With FH, since the carrier frequency is constantly changing, it is not possible for an attacker to use such averaging techniques to enhance SNR, as shown in Fig. 9(b).

The primary source of power consumption at the transmitter is from the output buffer driving the signal into the body. A multi-stage buffer with smaller unit slices is used to optimally drive the signal into the body depending on the operating frequency. This helps minimize the power by utilizing the optimum amount of buffer drive strength.

B. Integrating Receiver Design

The EQS-HBC receiver consists of an analog front end, sampler, and a baud rate clock data recovery (CDR) circuit (see Fig. 10). The analog front end has a current starved amplifier, a tunable bias ED for demodulation, and a resettable integrator to provide carrier feedthrough rejection and improve SNR at the sampler input. The regenerative latch-based sampler samples the integrator output. A clocked sampler and integrator is used to reduce power consumption. The proper phase alignment between the data and the clock is obtained through the CDR circuit. A baud rate Mueller–Muller CDR (MM-CDR) is used to minimize power consumption.

1) Amplifier: The front-end amplifier is necessary to provide sufficient sensitivity to the receiver to decode the received signal. A higher sensitivity will enable the input signal amplitude to be smaller, allowing the transmitter to operate at a lower supply voltage. This has a strong impact on the overall system power consumption. The required sensitivity

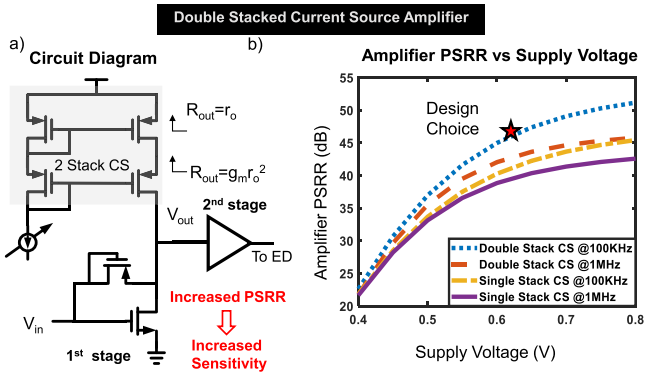


Fig. 11. (a) Circuit diagram of the front-end amplifier. (b) PSRR of the amplifier versus supply voltage for a single- and double-stacked current source-based architecture at 100 kHz and 1 MHz. A double-stacked current source-based architecture provides higher PSRR compared with single-stacked architecture, making it the preferable design choice.

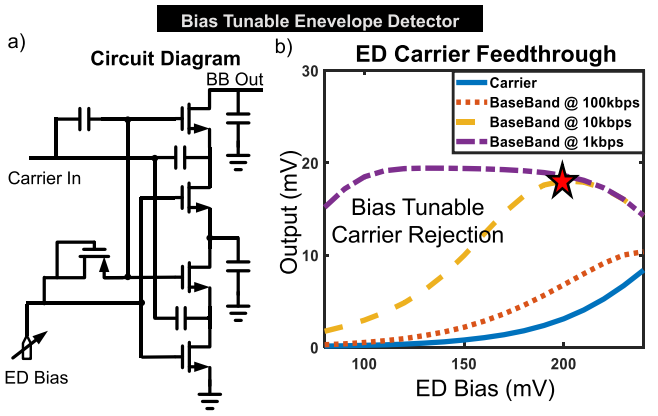


Fig. 12. (a) Circuit diagram of the bias tunable ED used for non-coherent detection at the receiver end. (b) Baseband and carrier (1 MHz) output versus tunable bias shows that the optimum bias for a data rate of 10 kb/s is around 200 mV.

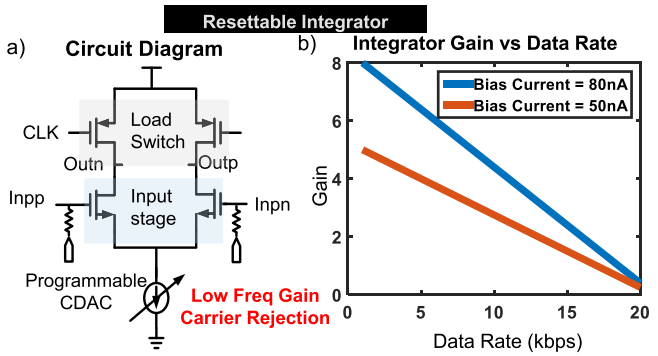


Fig. 13. (a) Circuit diagram of the resettable integrator with a tunable tail current source. (b) Variation of integrator gain versus data rate for different values of tail current source. Low data rates enable higher gain by providing longer integration duration, as long as the input stage stays in saturation.

can be estimated from the channel loss and the minimum reliable operating voltage at the transmitter end. Assuming a 60-dB channel loss and a 400-mV supply voltage at the transmitter end for 65-nm technology operating at 1-MHz clock frequency, the sensitivity requirement at the receiver end is 400 μV. The gain necessary from the amplifier stage is also dependent on the sensitivity of the demodulation stage, which is a passive ED in this case. We have used two-stage amplification to have sufficient signal at the ED input even for the worst case input signal. A current starved architecture [see Fig. 11(a)] is used for the amplifier to minimize power consumption and tune bandwidth and gain according to the requirements. One of the primary design goals in this case was to minimize the power supply noise effect on the amplifier output to enhance receiver sensitivity. Comparing a single- and double-stacked current source-based design shows that a double-stacked architecture provides a better power supply rejection ratio (PSRR) as can be seen from the simulation results in Fig. 11. The PSRR also improves with increasing supply voltage and decreasing operating frequency. The amplifier bandwidth requirement is determined by the OOK carrier frequency. The low carrier frequency of 1 MHz makes it possible to operate at a supply voltage as low as 0.5 V even for a double-stacked architecture.

2) Envelope Detector: The amplified signal is demodulated using a passive ED [see Fig. 12(a)] with a tunable gate bias [34]. An ED is chosen instead of a mixer to enable low-power operation, although it has lower sensitivity. Since the transmitter employs FH to increase physical security, an ED-based demodulation is preferable as it does not require generating a local carrier clock. A four-stacked ED is used in this scenario to enable demodulation for a carrier-to-baseband ratio of 100. The tunable bias determines the relative rejection between the carrier and the baseband data. A higher bias increases the carrier feedthrough, as the time constant reduces due to the decreasing resistance of each individual transistor. However, it also increases the baseband output, as shown in Fig. 12(b). At the optimum bias point, the baseband output is sufficient to meet the integrator sensitivity with minimal carrier feedthrough. The ED determines the minimum tolerable carrier frequency for a particular data rate to meet the required bit error rate (BER) constraints. The carrier frequency sets the bandwidth requirement of the front-end amplifiers and their power consumption. Hence, choosing the optimum bias point for the ED operation has a strong effect on the overall power consumption.

3) Integrator: A resettable clocked integrator is used at the output of the ED to improve the SNR of the signal applied to the sampler and also provide carrier feedthrough rejection through low-pass filtering. The integrator has an NMOS input stage, and two PMOS switches act as the load [see Fig. 13(a)]. It has two phases: 1) evaluate and 2) reset. During the reset phase (clk = 0), both the PMOS switches are ON and the output nodes are pre-charged to Vdd. During the evaluate phase (clk = 1), both the switches are turned off and the output load capacitance is discharged due to the tail current source. The discharge current on a particular branch is dependent on the ac input signal and the difference in discharge current creates a differential output. The differential output voltage is dependent on the integration of the discharge current over the integration duration. Since the ac discharge current is

proportional to the differential ac input voltage, the differential output voltage is dependent on the integration of the ac input voltage over the integration duration. This relation holds as long as the input stage is in saturation. Too high a bias current will result in the input transistors entering linear region making the differential output 0. The clock frequency of the integrator is equal to the baseband data rate, and the integration is done during the high phase of the clock. For a fixed bias current, a longer integration duration will result in higher differential output voltage and, hence, a higher integrator gain, as shown in Fig. 13(b). This is true as long as the integrator input stage does not go out of saturation. Since the carrier frequency is significantly larger than the baseband data rate, integrating it over the baseband duration results in almost zero output. As a result, any carrier feedthrough at the ED output is nullified by the integrator. The output of the integrator is applied to a sampler for digitization. The sampler, which is also clocked, and the integrator work on alternate phases such that the sampler evaluates after the evaluation phase of the integrator.

4) Clock Data Recovery: As discussed in Section IV-B, the receiver uses a clocked integrator and sampler for low-power operation. The integrator clock needs to be aligned with the data to ensure that the data remain constant over the integration evaluation phase and there is no data transition. Any misalignment will reduce the integrator output amplitude and hurt the overall receiver sensitivity. An integrating MM-CDR [35] is used to extract timing mismatch information between the incoming data stream and the integrator clock and provide phase alignment between them. A baud rate CDR enables low-power operation as it does not require any oversampling. Two additional samplers are required to provide voltage error information, which can be used to extract timing information. The CDR utilizes the different phases from a digitally synthesized 16-phase clock generator, which uses off-chip crystal-based reference without PLL, suitable for low carrier frequency operation. The CDR takes a decision to choose a leading/lagging phase depending on the extracted timing information. FH can create extra latency due to the CDR losing the lock condition and requiring extra time to settle. This can result in increased energy consumption, a tradeoff to consider while enabling FH as an extra security measure. Since the clock is generated externally, the power measurements do not include the clock generation power but include the clock division and distribution power.

C. AES 256 Encryption Core

EQS-HBC helps provide physical security by minimizing signal leakage and enhancing the private space of communication compared with previous HBC implementations and radio wave-based communication such as Bluetooth. Encrypting the transmitted data will provide mathematical security on top of this physical security and will require an attacker to break the encryption in the low probability scenario of physical access to the transmitted signal.

Hence, to provide security in case of an attacker physically contacting a person to snoop data, mathematically secure encryption algorithm AES 256 is implemented. The architecture of the parallel AES 256 with 14 rounds is shown in Fig. 14. It is a parallel 128-bit data-path implementation to provide high performance and requires 14 cycles for each encryption. The AES key is programmed externally into a register.

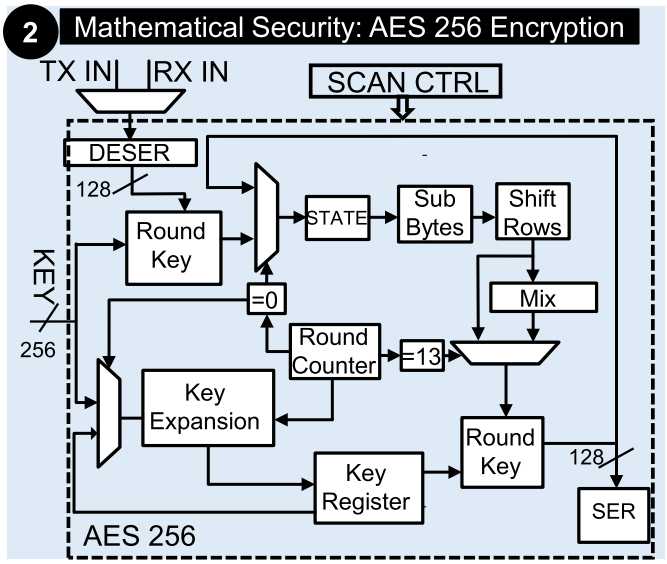


Fig. 14. AES 256 block diagram showing the different stages of encryption. The data are encrypted at the transmitter end and serialized before transmission. The received serial data are de-serialized into 128-bit blocks for decryption.

Since AES is a block cipher, it is necessary to convert the input serial data to parallel before encryption at the transmitter end or decryption at the receiver end. The AES module alternates between 128 cycles of data load phase and 14 cycles of encryption phase. At the transmitter end, the 128-bit output ciphertext is again converted to serial data before transmission. The parallel-to-serial conversion at the output and the serial-to-parallel conversion at the input are done simultaneously. A control unit is designed to set the different phases in the AES module, handle the serialization/de-serialization process, and also control the PRBS data generation at the transmitter end.

V. Measurement Results

The Sub-μWRComm node is fabricated in TSMC 65nm LP CMOS technology and has an active area of 0.17 mm^2, making it suitable for wearable devices. We measure the power consumption of the different physical and mathematical security features as well the sensitivity and BER performance of the receiver under different operating modes. We also demonstrate the transfer of a secure key from a watch-like wearable to a receiver connected to a laptop.

A. Transmitter Performance

The transmitter power is dominated by the switching power of the output buffer and varies from 38 nW (Data Rate = 1 kb/s and f_c = 100 kHz) to 240 nW (DR = 10 kb/s and f_c = 1 MHz), as shown in Fig. 15(a). The AES core runs at the baseband clock. Hence, its power consumption is dominated by leakage power for such low data rates and this leakage

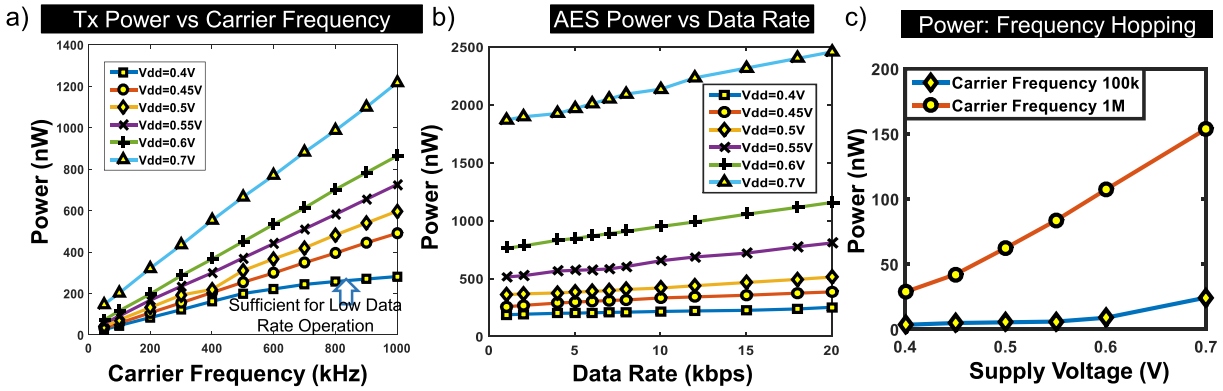


Fig. 15. Measurement results from the EQS HBC Transmitter and AES module. (a) Transmitter power consumption across different supply voltages. The transmitter operates at 0.4-V Vdd, which is sufficient for these low data rates. (b) Mathematical security: AES power consumption with frequency for different supply voltages. (c) Physical security enhancement: FH module power consumption versus voltage for different carrier frequencies.

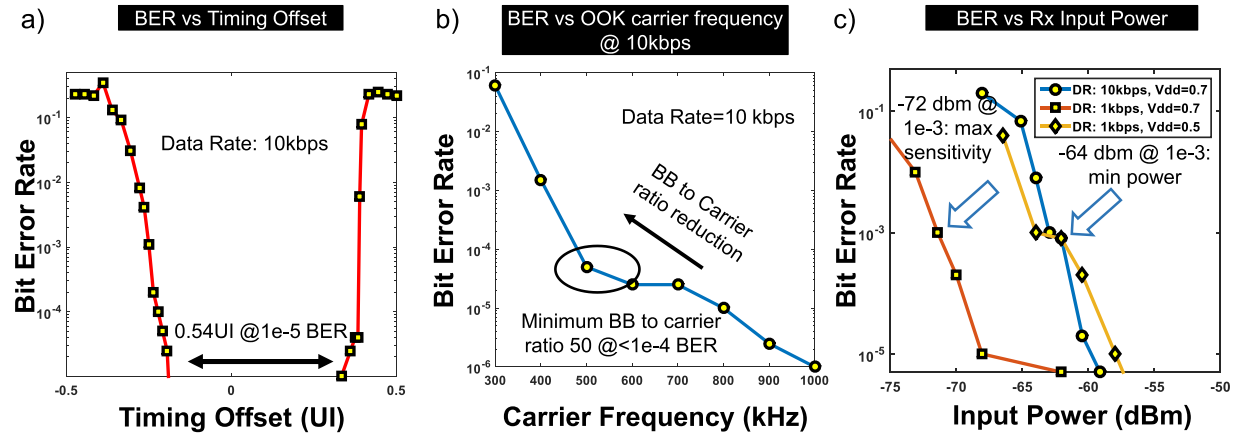


Fig. 16. EQS HBC receiver performance. (a) Bathtub curve at the receiver showing 0.54-UI opening at 10^{-5} BER. (b) BER performance keeping the data rate fixed at 10 kb/s and varying the carrier frequency. (c) Sensitivity analysis of the receiver showing −72-dBm sensitivity at the highest sensitivity point.

power accounts for a significant portion of the overall system power. The measured power for different data rates shows little variation in power consumption, particularly for low operating supply voltages [see Fig. 15(b)], showing the strong leakage power component. Hence, minimizing the operating supply voltage is a key requirement in reducing the overall system power. The FH circuit consumes a significantly small portion of the overall transmitter power, particularly for a carrier frequency of 100 kHz [see Fig. 15(c)].

B. Receiver Performance

The BER performance of the EQS-HBC receiver for a data rate of 10 kb/s under different clock and data timing offsets are shown in Fig. 16(a). It shows a 0.54-UI timing margin for a BER of 10^{-5}. Fig. 16(b) shows the performance of the receiver for a fixed data rate of 10 kb/s and varying carrier frequency. This can help determine the minimum carrier frequency that can be used for a particular data rate to meet a certain BER performance. Minimizing the carrier frequency for a given data rate will help reduce the overall system power and depends on the carrier rejection achieved through the ED and the integrator. Measurements show that BER increases as the carrier frequency is reduced and a BER of 10^{-4} can be obtained even for a carrier frequency as low as 500 kHz. The sensitivity of the receiver under different conditions is shown in Fig. 16(c). The receiver has a sensitivity of 400 μVp-p (−64 dBm for a 50Ω impedance) for a BER requirement of 10^{-3} in the minimum power mode of operation with a data

TABLE I
BLOCK LEVEL AREA AND POWER BREAKDOWN

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	

TABLE II
COMPARISON WITH STATE OF THE ART

	This Work	H. Cho ISSCC '15	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	**237nW (>75X)**	21uW	0.87mW	1.7mW	18uW	1.85mW
Rx Power	**178nW(>125X)**	42.5uW	1.1mW	8mW	24uW	9.02mW
Total Power	**415nW (>100X)**	63.5uW	1.97mW	9.7mW	42uW	10.87mW
Sensitivity (Voltage)#	398μV @10^{-3} BER	632μV @10^{-5} BER	44μV @10-3 BER	6.324mV @10^{-5} BER	1mV @10^{-3} BER	796μV @ <10^{-5} BER
Sensitivity (dbm)*	-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
Area (mm^2)	0.17	5.93	0.54	1.6	0.12	1.12
Operating Frequency	50KHz-1 MHz	10/13.56 MHz	20-120 MHz	20-60 MHz 140-180 MHz	40 MHz	40-80 MHz
Encryption Implementation	AES-256	-	-	-	-	-
Physical Security	**Yes**	No	No	No	No	No

#Sensitivity provided in v_{p-p} for high impedance termination *dBm sensitivity, calculated assuming 50Ω termination

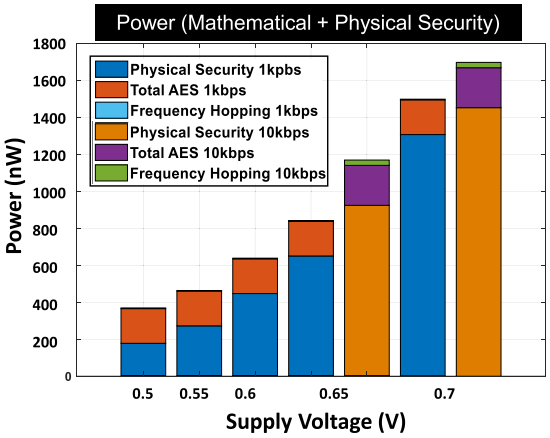


Fig. 17. Overall system power consumption showing the contribution of each type of security measure for different data rates.

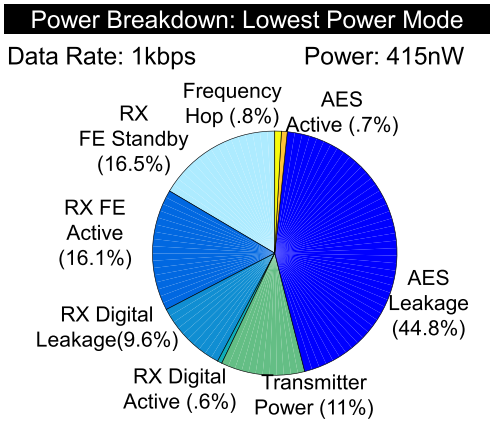


Fig. 18. Power breakdown of different blocks at the lowest power mode.

rate of 1 kb/s and supply voltage of 0.5 V. This sensitivity is sufficient even for a transmitted voltage of 400 mV undergoing a 60-dB loss through the channel. The receiver can achieve a sensitivity of 158 μVp-p (−72 dBm for a 50-Ω impedance) under the maximum sensitivity mode operation with a data rate of 1 kb/s and a receiver supply voltage of 0.7 V. The BER performance is limited by the carrier frequency (for physical security) and the minimum tolerable baseband-to-carrier ratio. Inter-person and environmental variation in channel loss does not affect BER for these low data rates.

C. Power Breakdown: Physical Versus Mathematical Security

Fig. 17 shows the power breakdown for mathematical and physical security at different receiver Vdd and data rates. The minimum operating transmitter Vdd is 0.4 V. At receiver supply voltages below 0.65 V, it is not possible to operate at 10 kb/s with tolerable sensitivity. At low supply voltages (<0.6 V), the overall power is dominated by the AES leakage power. Operating at the lowest power mode requires 227 nW for physical security, with an additional 188 nW for mathematical security through encryption. Increasing supply voltage and data rate increases power consumed by the EQS-HBC receiver to provide physical security. The physical security power stays almost constant with data rate as it is dominated by the leakage power. At the lowest power mode with a data rate of 1 kb/s, the transmitter consumes 233.6-nW Tx, and Rx consumes 178-nW Rx (including leakage power) and 108-nW overall active power for both the physical and the mathematical security (see Table I). The power breakdown at this mode (see Fig. 18) shows that the leakage power from AES consumes most of the power and only about 25%

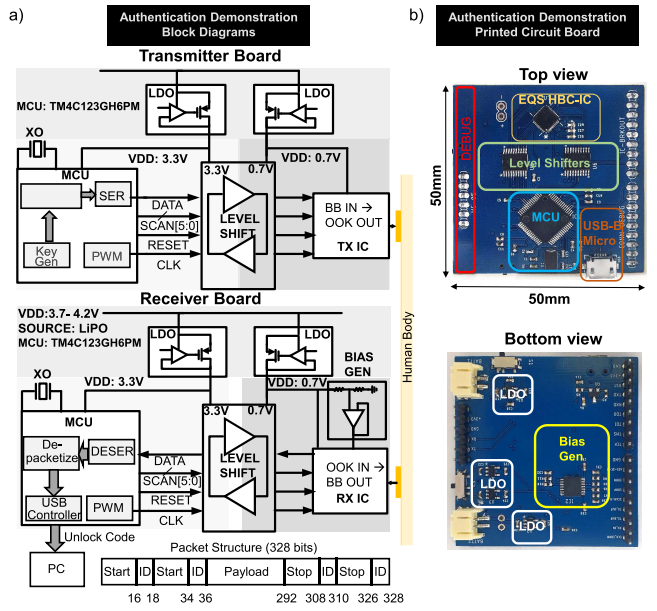


Fig. 19. Secure authentication demonstration setup. (a) Block diagram of the transmitter and receiver board and the transmitted packet structure. (b) Top and bottom views of the demonstration PCB showing the different components.

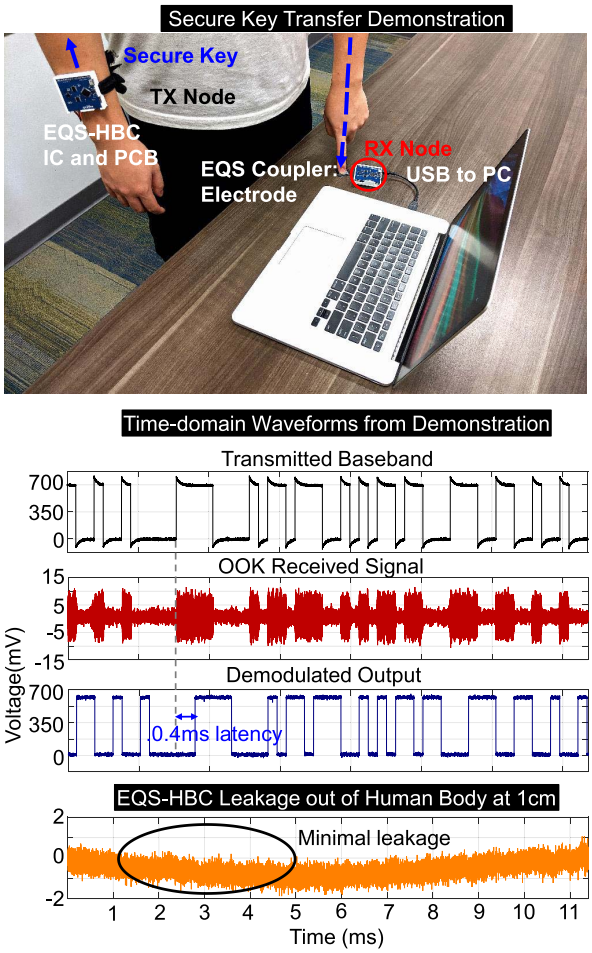


Fig. 20. Demonstration of secure key transfer using EQS-HBC. The user transmits a key, which is securely transmitted through EQS-HBC to the receiver. Captured time-domain waveforms showing the transmitted voltage, the received waveform, and the demodulated output. Signal leakage measurements showing signal leakage below the noise floor.

of overall power is active power. The dominance of leakage power and low data rate makes the energy efficiency of the Sub-μWRComm system low.

The power measurements are done on a chip in the typical process corner. Slow corner chips will require higher supply voltage, which can affect overall leakage. Moreover, when operating as a transceiver, an on-chip regulator will be necessary for both Rx and Tx to operate at the optimum power point, which can add to the overall power. Applications requiring dedicated Tx or Rx operation will not have this additional power overhead.

D. Demonstration: Secure Key Transfer

The feasibility of EQS-HBC is shown through a demonstration of secure key transfer between a wearable and a laptop. The wearable device acts as the transmitter, sending a 128-bit key, and the receiver is connected to the laptop through a serial interface. The user has the transmitter on one hand and touches the receiver electrode with the other hand. The receiver will communicate to the computer only when the correct key is received, which can then unlock the computer. The block diagram of the PCB is shown in Fig. 19(a). A TM4C123GXL MCU is used to program the scan bits, providing clock, reset, and input to the transmitter, and get the output signal from the receiver. The MCU works at a supply voltage of 3.3 V, whereas the EQS-HBC node operates at a supply voltage of 0.7 V. Therefore, a level shifter (LSF0108) is used to connect the signals between the MCU and the IC. A lithium-ion battery is used as supply for the board, and the supply voltages for the MCU and EQS-HBC node are generated using two LDOs (TPS73633 and TLV73310). The actual PCB implementation is shown in Fig. 19(b). The data are transmitted in a packet format for error correction and synchronization purposes. Each packet has a start and stop delimiter and a data payload, as shown in Fig. 19(a). The signal waveforms and the actual demonstration for the secure key transfer are shown in Fig. 20. The transmitted signal is sent at a baseband rate of 5 kb/s with an OOK modulation carrier frequency of 500 kHz. The signal is demodulated at the receiver with a tolerable latency of 0.4 ms. The out-of-body leakage at a distance of 1 cm away from the nondevice hand is negligible and very close to the noise floor. This further demonstrates the security aspect of EQS-HBC. The received data are sent to the laptop through serial communication. This demonstration shows a method of communicating a private key in a secure manner between a wearable and a computer.

E. Comparison

Fig. 21 and Table II show the comparison of the Sub-μWRComm node with other state-of-the-art implementations. The *Sub-μWRComm* node consumes 415-nW power at the lowest power operating mode, making it $>100\times$ power efficient compared to previous HBC transceivers.

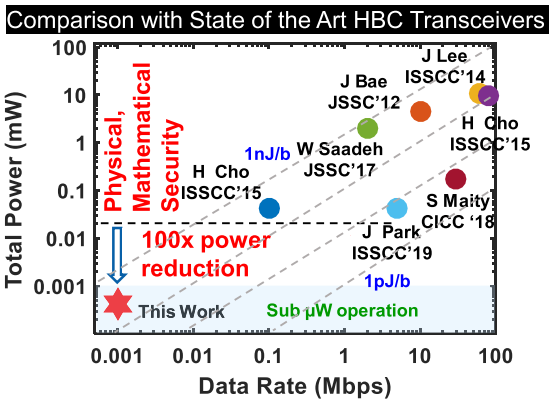


Fig. 21. Comparison of the EQS-HBC SoC with other state-of-the-art HBC implementations showing lowest power physically and mathematically secure operation with $>100\times$ improvement in power consumption.

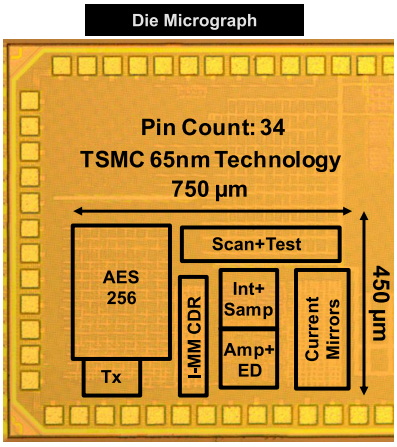


Fig. 22. Die micrograph of the Sub-μWRComm system.

Most previous transceivers are designed for higher data rate applications and are not the most optimum for security-sensitive low-data-rate applications. This also provides physical and mathematical security, which is not present in any other state-of-the-art implementations. The low data rate makes the energy efficiency lower compared to previous high-data-rate HBC implementations. However, it is not the focus of the targeted applications and low-power operation is the primary goal. The die micrograph of the IC is shown in Fig. 22.

VI. Conclusion

This article presents Sub-μWRComm: the first sub-μW wearable communication for low-data-rate, security-sensitive applications, such as secure authentication and remote physiological monitoring. It utilizes EQS-HBC and operates around the 1-MHz frequency range. This provides physical security by confining the signal within a few centimeters of the body, stopping any malicious attacker from remotely snooping the transmitted signal. An AES 256 engine provides mathematical security through encryption. An OOK-based EQS-HBC transceiver is used to enable secure low-power operation. The Sub-μWRComm node operates at 415-nW power for the lowest power mode, a $100\times$ improvement compared to state-of-the-art HBC transceivers, for a data rate of 1 kb/s and sensitivity of -64 dBm. A secure key transfer demonstration also shows minimal signal leakage out of the body. This can potentially enable the design of battery-less wearable patches in future.

References

[1] S. Sen, "Invited: Context-aware energy-efficient communication for IoT sensor nodes," in *Proc. 53nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Dec. 2016, pp. 1–6.

[2] S. Maity, M. He, M. Nath, D. Das, B. Chatterjee, and S. Sen, "Bio-physical modeling, characterization, and optimization of electro-quasistatic human body communication," *IEEE Trans. Biomed. Eng.*, vol. 66, no. 6, pp. 1791–1802, Jun. 2019.

[3] J. Park, H. Garudadri, and P. P. Mercier, "Channel modeling of miniaturized battery-powered capacitive human body communication systems," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 2, pp. 452–462, Feb. 2017.

[4] Z. Lucev, I. Krois, and M. Cifrek, "A capacitive intrabody communication channel from 100 kHz to 100 MHz," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf.*, May 2011, pp. 1–4.

[5] Ž. Lucev, I. Krois, and M. Cifrek, "A capacitive intrabody communication channel from 100 kHz to 100 MHz," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 12, pp. 3280–3289, Dec. 2012.

[6] S. Maity, K. Mojabe, and S. Sen, "Characterization of human body forward path loss and variability effects in voltage-mode HBC," *IEEE Microw. Wireless Compon. Lett.*, vol. 28, no. 3, pp. 266–268, Mar. 2018.

[7] J. Bae, H. Cho, K. Song, H. Lee, and H.-J. Yoo, "The signal transmission mechanism on the surface of human body for body channel communication," *IEEE Trans. Microw. Theory Techn.*, vol. 60, no. 3, pp. 582–593, Mar. 2012.

[8] S. Maity, M. Nath, G. Bhattacharya, B. Chatterjee, and S. Sen, "On the safety of human body communication," *IEEE Trans. Biomed. Eng.*, vol. 67, no. 12, pp. 3392–3402, 2020.

[9] M. S. Wegmueller, M. Oberle, N. Felber, N. Kuster, and W. Fichtner, "Signal transmission by galvanic coupling through the human body," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 963–969, Apr. 2010.

[10] J. Park and P. P. Mercier, "Magnetic human body communication," in *Proc. 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Aug. 2015, pp. 1841–1844.

[11] J. Park and P. P. Mercier, "A sub-40 μW 5Mb/s magnetic human body communication transceiver demonstrating trans-body delivery of high-fidelity audio to a wearable in-ear headphone," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2019, pp. 286–287.

[12] J. Jang *et al.*, "4-camera VGA-resolution capsule endoscope with 80Mb/s body-channel communication transceiver and sub-cm range capsule localization," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2018, pp. 282–284.

[13] W. Saadeh, M. A. B. Altaf, H. Alsuradi, and J. Yoo, "A 1.1-mW ground effect-resilient body-coupled communication transceiver with pseudo OFDM for head and body area network," *IEEE J. Solid-State Circuits*, vol. 52, no. 10, pp. 2690–2702, Oct. 2017.

[14] H. Cho, H. Kim, M. Kim, J. Jang, J. Bae, and H.-J. Yoo, "A 79 pJ/b 80 Mb/s full-duplex transceiver and a 42.5 μW 100 kb/s super-regenerative transceiver for body channel communication," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2015, pp. 1–3.

[15] N. Cho, L. Yan, J. Bae, and H.-J. Yoo, "A 60 kb/s–10 Mb/s adaptive frequency hopping transceiver for interference-resilient body channel communication," *IEEE J. Solid-State Circuits*, vol. 44, no. 3, pp. 708–717, Mar. 2009.

[16] B. Chatterjee, A. Srivastava, D.-H. Seo, D. Yang, and S. Sen, "A context-aware reconfigurable transmitter with 2.24 pJ/bit, 802.15.6 NB-HBC and 4.93 pJ/bit, 400.9 MHz MedRadio modes with 33.6% transmit efficiency," in *Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC)*, Aug. 2020, pp. 75–78.

[17] S. Maity, B. Chatterjee, G. Chang, and S. Sen, "A 6.3pj/b 30mbps -30 db SIR-tolerant broadband interference-robust human body communication transceiver using time domain signal-interference separation," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2018, pp. 1–4.

[18] S. Maity, B. Chatterjee, G. Chang, and S. Sen, "BodyWire: A 6.3-pJ/b 30-Mb/s -30-dB SIR-tolerant broadband interference-robust human body communication transceiver using time domain interference rejection," *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2892–2906, Oct. 2019.

[19] S. Maity *et al.*, "A 415 nW physically and mathematically secure electro-quasistatic HBC node in 65nm CMOS for authentication and medical applications," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Mar. 2020, pp. 1–4.
[20] D. Das, S. Maity, B. Chatterjee, and S. Sen, "Enabling covert body area network using electro-quasistatic human body communication," *Sci. Rep.*, vol. 9, no. 1, pp. 169:1–169:29, Mar. 2019.
[21] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: A survey," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 171–193, 2011.
[22] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.
[23] M. Wazid, V. B. K, A. V. Vasilakosef, and A. K. Das, "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment," *J. Netw. Comput. Appl.*, vol. 150, Jan. 2020, Art. no. 102496.
[24] M. Wazid, A. V. Vasilakos, and A. K. Das, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, pp. 112–126, Dec. 2018.
[25] A. V. Vasilakos, H. Fang, Z. Zhang, and H. Wang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.
[26] S. Challa, A. K. Das, P. Gope, A. V. Vasilakos, N. Kumar, and F. Wu, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1267–1286, Nov. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17326328
[27] S. Maity, D. Yang, S. S. Redford, D. Das, B. Chatterjee, and S. Sen, "Bodywire-HCI: Enabling new interaction modalities by communicating strictly during touch using electro-quasistatic human body communication," *ACM Trans. Comput.-Hum. Interact.*, vol. 27, no. 6, p. 39, Nov. 2020, doi: 10.1145/3406238.
[28] M. Nath, S. Maity, S. Avlani, S. Weigand, and S. Sen, "Inter-body coupling in electro-quasistatic human body communication: Theory and analysis of security and interference properties," Sci. Rep., 2020.
[29] J. Y. Jung, D.-O. Kang, and C. Bae, "Distance estimation of smart device using Bluetooth," in *Proc. ICSNC*, 2013, pp. 13-1–13-8.
[30] S. Gabriely, R. Lau, and C. Gabriel, "The dielectric properties of biological tissues: II. Measurements in the frequency range 10 Hz to 20 GHz," *Phys. Med. Biol.*, vol. 41, no. 11, pp. 2251–2269, 1996.
[31] N. Cho, J. Yoo, S.-J. Song, J. Lee, S. Jeon, and H.-J. Yoo, "The human body characteristics as a signal transmission medium for intrabody communication," *IEEE Trans. Microw. Theory Techn.*, vol. 55, no. 5, pp. 1080–1086, May 2007.
[32] M. Nath, S. Maity, and S. Sen, "Towards understanding the return path capacitance in capacitive human body communication," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 7, pp. 1879–1883, Oct. 2020.
[33] S. Maity, D. Das, and S. Sen, "Wearable health monitoring using capacitive voltage-mode human body communication," in *Proc. 39th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Jul. 2017, pp. 1–4.
[34] V. Mangal and P. R. Kinget, "A 0.42 nW 434 MHz −79.1 dBm wake-up receiver with a time-domain integrator," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2019, pp. 438–440.
[35] P. Mehrotra, S. Maity, and S. Sen, "An improved update rate CDR for interference robust broadband human body communication receiver," *IEEE Trans. Biomed. Circuits Syst.*, vol. 13, no. 5, pp. 868–879, Oct. 2019.

Shovan Maity (Graduate Student Member, IEEE) received the B.E. degree from Jadavpur University, Kolkata, India, in 2012, the M.Tech. degree in electrical engineering from IIT Bombay, Mumbai, India, in 2014, and the Ph.D. degree in electrical engineering from Purdue University, West Lafayette, IN, USA, in 2019.

He worked as an Analog Design Engineer at Intel, Bengaluru, India, from 2014 to 2016. He is currently working as a Senior Circuit Design Engineer with Qualcomm, San Diego, CA, USA. His research interests lie in the area of mixed-signal circuits and systems for the Internet of Things, and Biomedical and security applications.

Dr. Maity received the Institute Silver Medal from IIT Bombay in 2014, the Purdue ECE fellowship during 2016–2018, the IEEE HOST Best Student Paper Award in 2017, and the CICC 2019 Best Paper Award.

Nirmoy Modak (Graduate Student Member, IEEE) received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 2012, and the M.Tech. degree in electrical engineering from IIT Bombay, Mumbai, India, in 2015. He is currently pursuing the Ph.D. degree in electrical engineering with Purdue University, West Lafayette, IN, USA.

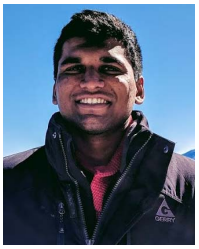
He was an Electrical Design Engineer with Cypress Semiconductor Pvt. Ltd., Bengaluru, India, from 2015 to 2016. He is currently an Assistant Professor with Jadavpur University. His research interests include the design of circuits and systems for human body communication and mixed-signal circuit design.

David Yang (Graduate Student Member, IEEE) received the bachelor's degree in electrical engineering from Purdue University, West Lafayette, IN, USA, in 2019, where he is currently pursuing the Ph.D. degree in electrical engineering.

His work is focused on the development and design of human body communication systems and circuits—in particular, relating to physical security in embedded systems.

Mayukh Nath received the B.S. degree in physics from the Indian Institute of Science, Bengaluru, India, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with Purdue University, West Lafayette, IN, USA.

His research interests include theory and simulation-based formulation of interdevice communications, such as body area network-based medical implants and wearables.



Shitij Avlani received the Bachelor of Engineering degree in electronics engineering from the University of Mumbai, Mumbai, India, in 2017. He is currently pursuing the master's degree in electrical engineering with Purdue University, West Lafayette, IN, USA.

He worked at IIT Bombay, Mumbai, for three years on point of care medical devices and fabrication of MEMS sensors. He has been working on the system design aspect of human body communication at the SPARC lab. He interned at Intel Labs, Hillsboro, OR, USA, in the summer of 2020, where he worked on analog circuit design. His research interests include circuit design and embedded systems.

Debayan Das (Graduate Student Member, IEEE) received the Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, Kolkata, India, in 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Purdue University, West Lafayette, IN, USA, working with Prof. Shreyas Sen.

He worked as an Analog Design Engineer at a start-up based in India. He has interned with the Security Research Lab, Intel Labs, Hillsboro, OR, USA, over the summers of 2018 and 2020. His research interests include mixed-signal IC design and hardware security.

Mr. Das was a recipient of the IEEE HOST Best Student Paper Award in 2017 and 2019 and the 3rd Best Poster Award in IEEE HOST 2018. In 2019, one of his papers was recognized as a Top Pick in Hardware and Embedded Security published over the span of the last six years. During his Ph.D. degree, he has been awarded the ECE fellowship during 2016–2018 and the Bilsland Dissertation Fellowship during the final year (2020–2021) for his outstanding overall achievements.

Josef Danial received the B.Sc. degree in computer engineering from Purdue University, West Lafayette, IN, USA, in 2018, where he is pursuing the master's degree with the SPARC Lab.

He has two years of industry experience in automotive at Fiat Chrysler Automobiles, London, U.K., and IOT at Cisco Jasper, Santa Clara, CA, USA. He is currently a Graduate Research Assistant with the SPARC Lab, Purdue University. His research interests include machine learning, hardware security, and computer vision.

Parikha Mehrotra received the B.E. degree in electrical and electronics engineering from the National Institute of Technology at Hamirpur, Hamirpur, India, in 2017. She is currently pursuing the Ph.D. degree with Purdue University, West Lafayette, IN, USA.

Her research interests include mixed-signal circuit design, human body sensing, and communication.

Shreyas Sen (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Georgia Tech, Atlanta, GA, USA, in 2011.

He is currently an Associate Professor in electrical and computer engineering with Purdue University, West Lafayette, IN, USA. He has over five years of industry research experience at Intel Labs, Hillsboro, OR, USA; Qualcomm, San Diego, CA, USA, and Rambus, Los Altos, USA. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Things (IoT), biomedical, and security. He is the inventor of the Electro-Quasistatic Human Body Communication, for which he was a recipient of the MIT Technology Review top-10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award. His work has been covered by more than 100 news releases worldwide, invited appearance on TEDx Indianapolis, Indian National Television CNBC TV18 Young Turks Program, and NPR subsidiary Lakeshore Public Radio.

Dr. Sen was a recipient of the NSF CAREER Award in 2020, the AFOSR Young Investigator Award in 2016, the NSF CISE CRII Award in 2017, the Google Faculty Research Award in 2017, the Intel Labs Quality Award for industrywide impact on USB-C type, the Intel Ph.D. Fellowship in 2010, the IEEE Microwave Fellowship in 2008, and seven best paper awards, including IEEE CICC 2019 and IEEE HOST 2017, 2018, and 2019. His work was chosen as one of the top-10 papers in the Hardware Security field over the past six years (TopPicks 2019). He has coauthored 2 book chapters, over 135 journal and conference papers, and has 14 patents granted/pending. He serves/has served as an Associate Editor for the IEEE Design and Test, an Executive Committee Member of IEEE Central Indiana Section, and a Technical Program Committee Member of DAC, CICC, DATE, ISLPED, ICCAD, ITC, and VLSI Design, among others.