

Received 11 August 2022; revised 10 October 2022 and 15 November 2022; accepted 4 December 2022. Date of publication 16 December 2022; date of current version 7 April 2023.

Digital Object Identifier 10.1109/OJSSCS.2022.3230000

Batteryless, Wireless, and Secure SoC for Implantable Strain Sensing

MOHAMED R. ABDELHAMID¹ (Member, IEEE), UNSOO HA¹, UTSAV BANERJEE² (Member, IEEE),
FADEL ADIB¹, AND ANANTHA P. CHANDRAKASAN¹ (Fellow, IEEE)

(Invited Paper)

¹Electrical Engineering and Computer Science Department, Massachusetts Institute of Technology, Cambridge, MA 02139, USA

²Electrical, Electronics, and Computer Sciences Department, Indian Institute of Science, Bengaluru 560012, India

CORRESPONDING AUTHOR: M. R. ABDELHAMID (e-mail: mrhamid@alum.mit.edu)

ABSTRACT The past few years have witnessed a growing interest in wireless and batteryless implants, due to their potential in long-term biomedical monitoring of in-body conditions, such as internal organ movements, bladder pressure, and gastrointestinal health. Early proposals for batteryless implants relied on inductive near-field coupling and ultrasound harvesting, which require direct contact between the external power source and the human body. To overcome this near-field challenge, recent research has investigated the use of RF backscatter in wireless micro-implants because of its ability to communicate with wireless receivers that are placed at a distance outside the body (~ 0.5 m), allowing a more seamless user experience. Unfortunately, existing far-field backscatter designs remain limited in their functionality: they cannot perform biometric sensing or secure data transmission; they also suffer from degraded harvesting efficiency and backscatter range due to the impact of variations in the surrounding tissues. In this article, we present the design of a batteryless, wireless and secure system-on-chip (SoC) implant for in-body strain sensing. The SoC relies on four features: 1) employing a reconfigurable in-body rectenna which can operate across tissues adapting its backscatter bandwidth and center frequency; 2) designing an energy efficient 1.37 mmHg strain sensing front-end with an efficiency of 5.9 mmHg-nJ/conversion; 3) incorporating an AES-GCM security engine to ensure the authenticity and confidentiality of sensed data while sharing the ADC with the sensor interface for an area-efficient random number generation; 4) implementing an over-the-air closed-loop wireless programming scheme to reprogram the RF front-end to adapt for surrounding tissues and the sensor front-end to achieve faster settling times below 2 s.

INDEX TERMS Backscatter, bandwidth reconfigurability, batteryless, biometrics, core pressure, cross-tissue adaptation, far-field, glucose levels, human body, implantable, organ movements, pressure, RF, security, sensing, strain, system-on-a-chip, wireless.

I. INTRODUCTION

THE EVER-GROWING Internet of Things (IoT) and the rise of new biomedical applications is generating an increased demand for energy efficient wireless systems. Conventional wireless biomedical systems optimize their energy efficiency by targeting the different layers of their designs, whether it is energy harvesting, sensor front-end,

encryption engines, or wireless protocols. Optimizing each of these layers has led to tremendous advances in biomedical systems and ushered in the rise of wireless and batteryless micro-implanted systems [1], [2], [3]. However, existing layered designs are inherently limited to the performance bounds of their individual layers. This limitation makes it difficult for them to operate across practical real-world

environments where they need to adapt to changing conditions, such as the available wireless power, bandwidth, and channel conditions.

This article takes a new approach to developing wireless and batteryless implants by co-designing all the subsystems that comprise the end-to-end wireless sensing stack. A key strength of our design is its cross-layer reconfigurability that spans energy-harvesting, wireless communication, security, and analog biometric sensing.

We present the design, implementation, and evaluation of a batteryless wireless and secure SoC for implantable sensing. Our design extends our previously proposed SoC [4] by introducing innovations along two key fronts: 1) a fully integrated security-sensing-communication stack: which shares blocks along the stack for an area and power efficient design; 2) over-the-air closed-loop wireless programming: which leverages the asymmetric wireless link to break the tradeoff between energy-efficiency and latency. Our SoC incorporates a reprogrammable rectenna for integrated and adaptive energy harvesting and backscatter communication, a low-power security engine, and an efficient sensing front-end for biometric sensing.

We demonstrate our SoC's ability to perform pressure sensing for applications in long-term monitoring of gastrointestinal (GI) motility. Such monitoring can be achieved by sensing the internal pressure along the GI tract [5], and is used to understand digestive system disorders and the development of obesity. The reasons why our design is particularly desirable for this application are multifold. First, our batteryless design eliminates the need for surgical replacement, mitigates the health hazards due to battery depletion risks for in-body implants, and reduces the overall size of the implant (since batteries can consume up to 50% of the volume of GI sensor) [1], [6] while directly integrating the power management with energy harvesting. Second, our built-in security builds on past work [7], [8] to bring privacy, confidentiality, and authentication to sensed in-body biometrics. Third, our programmable RF front-end allows our sensing to adapt to different in-body tissues, which is particularly beneficial for a sensor traveling along the GI tract [6]. Finally, our sensor's ability to communicate with far-field wireless transceivers outside the body makes it more desirable than prior approaches that require direct contact with the human body [3], and paves the way for more seamless future biomedical and bionic systems.

II. IN-BODY STRAIN SENSING

This section describes the design of the strain sensing node, circuit-level implementation, over-the-air programming to reconfigure the chip, and the logic controlling the whole operation while guaranteeing system security.

A. SYSTEM OVERVIEW

The in-body strain sensor, shown in Fig. 1, incorporates a built-in security engine to securely transfer data between an

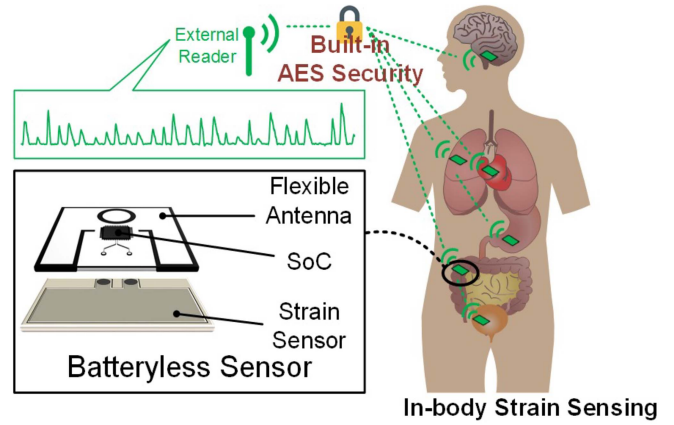


FIGURE 1. Secure, batteryless, and wireless in-body strain sensing.

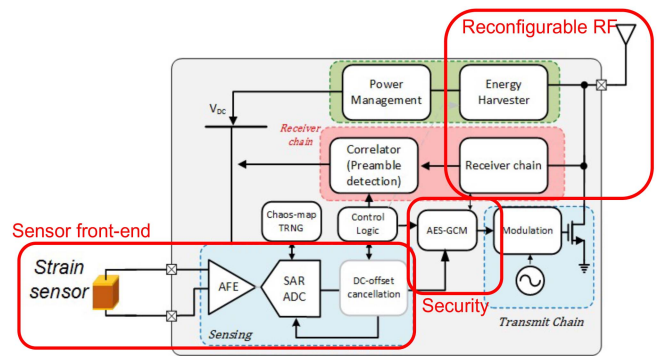


FIGURE 2. In-body strain sensor block diagram highlighting the reconfigurable wireless RF, security engine, and sensor front-end.

external reader and the in-body sensors. The SoC is integrated with a flexible antenna and laminated on a batteryless sensor to extract internal biometric data.

The SoC design includes four main subsystems: 1) a power management unit (PMU) with energy harvesting; 2) a transceiver for wireless communication; 3) a sensor front-end for data acquisition; and 4) a security engine for authentication and encryption as illustrated in Fig. 2. The RF energy harvester is designed as a 6-stage rectifier while the PMU has a voltage limiter to protect the internal devices from being overstressed at high RF input power, a comparator which turns on the LDO when the stored voltage is above 0.5 V, and a power-on reset circuit to initialize the internal registers. The transceiver is made up of a receiver chain and a backscatter transmitter. The receiver employs an envelope detector to downconvert the RF input signal, then an integrate-and-dump filter resolves the incoming bits which use pulse interval encoding (PIE). However, the transmitter utilizes a ring oscillator and digitally modulates its frequency to backscatter an FM0-encoded bitstream back to the reader. The sensor interface acquires the strain signal through the analog front-end (AFE) which incorporates a low-noise amplifier (LNA) followed by a programmable gain amplifier (PGA) then a 10-bit ADC. A security engine based on [8] is implemented on-chip to provide authenticity

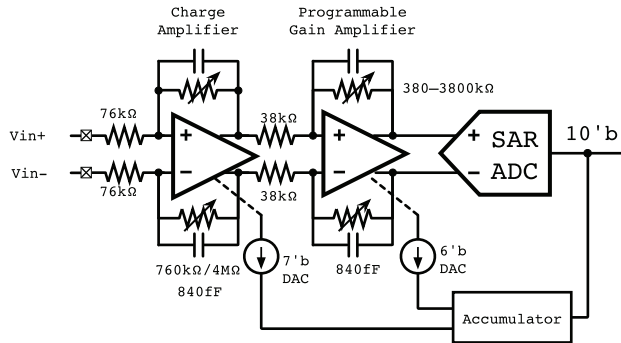


FIGURE 3. AFE schematic with amplification, quantization, and an offset cancelation loop.

and confidentiality through the use of advanced encryption standard in Galois-Counter Mode (128-bit AES-GCM). In addition, the counter mode initialization is performed via a true random number generator (TRNG) implemented as a switched-capacitor chaos map sharing the ADC with the sensor front-end.

B. CIRCUIT-LEVEL IMPLEMENTATION

1) SENSOR FRONT-END

The sensor AFE consists of an LNA directly interfacing with the pressure sensor, a PGA scaling the signal to the full dynamic range, a SAR ADC to provide 10-bit data samples, and an accumulator-based offset cancelation loop shown in Fig. 3. The input stage of the LNA incorporates a 7-bit binary weighted units of pMOS differential pairs for programmable offset. The input pair sizing is then selected by the dc cancelation loop where a larger effective area produces a smaller offset. Once the cancelation loop settles, the sampled data is fed to the SAR ADC to be processed by the encryption engine, and finally, backscattered to the base station.

Over-the-air programming creates a closed-loop system with the base station where the internal states of the sensor front-end are backscattered through the uplink packet. Therefore, the base station can use the “Reconfigure” command to set the initial state of the accumulator and provide a faster settling time to the dc cancelation loop.

2) RECONFIGURABLE WIRELESS RF FRONT-END

In-body sensing requires placing the SoC with its antenna inside the human body. The main problem, however, is that the antenna impedance and efficiency are affected by the surrounding tissues. An antenna optimized to measure the strain on the stomach is not optimum when used to measure the strain on the bladder. As each tissue has different electrical properties (conductivity and permittivity), then antennas of identical dimensions would have different current density distributions and, subsequently, electromagnetic fields.

To overcome this challenge, we designed a reconfigurable RF front-end where the node can be programmed to operate across a wide range of tissues. Our reconfigurable rectenna

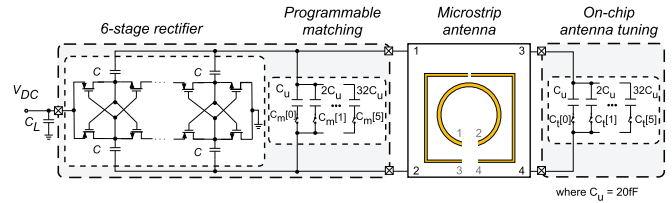


FIGURE 4. Reconfigurable rectenna design allows for programming the center frequency and bandwidth.

is shown in Fig. 4 where a high-Q antenna is conjugate-matched with a capacitive 6-stage rectifier. A 6-bit capacitor bank tunes the input impedance of the rectifier to match the antenna across tissues, while another capacitor bank is used as a programmable load coupled to the loop antenna to program its current distribution and, hence, radiation properties.

The antenna design builds on our previous work on programmable rectennas for RF backscatter [6]. In comparison to this previous work, which only tunes the center frequency, the SoC presented here can be optimized in a high-Q high-efficiency mode or adapt to scale its bandwidth by a factor of 8 for higher bandwidth datarate. This is based on two design features: first, designing a bandwidth-programmable antenna with programmable matching; second, in contrast to the existing designs, our system can utilize closed-loop over-the-air programming to adapt and reconfigure its RF front-end.

A programmable-bandwidth antenna is implemented by designing a loop antenna which is coupled with an outer loop terminated by a tunable capacitive load. The tunable capacitive load modifies the effective electrical length of the outer loop controlling how much the fields of both loops can add up around the frequency of interest. When the resonance frequencies of each loop with the capacitive rectifier are staggered by tuning them to be slightly different, a wider bandwidth is achieved as both resonances combine to produce almost one effective wider peak.

As adding tunable resistors to the harvesting chip would only increase the losses and ultimately reduce the system’s energy harvesting efficiency, we only tune the capacitive part of the harvester’s input impedance. As for the real part, the antenna’s outer loop is loaded by a tunable capacitor bank which couples with the inner loop tuning the radiation resistance and the bandwidth of the antenna without considerable degradation to the harvesting efficiency. Therefore, the real part is tuned via the antenna’s outer tunable capacitor bank (C_t) while the rectifier’s input capacitance is programmed through the input matching capacitor bank (C_m).

Since the node is batteryless, the antenna does not know how and when to change its programming. Here, we leverage the asymmetric link by having the reader do a configuration-space search to find the optimum configuration for the required mode of operation. Each configuration is then

stored on the reader and sent to the node in the form of a Reconfigure downlink command.

3) POWER MANAGEMENT AND COMMUNICATION

The PMU has a voltage limiter to protect the internal devices from being overstressed at high RF input power, a comparator which turns on the LDO when the stored voltage is above 0.5 V, and the power on reset (PoR) circuit to initialize the internal flip flops. The LDO is implemented with a feedback error amplifier and a Miller-compensated pMOS pass transistor to generate a regulated voltage at different current loads.

The transmitter chain incorporates an FM0 encoder, a continuous phase frequency encoding scheme, to modulate a pair of antenna switches which modulate the node's reflection coefficient between a reflective state and absorptive state. A current-starved ring oscillator generates the clock necessary to frequency modulate the backscattered bitstream.

The receiver extracts the RF envelope through ac-coupling the output of the (N-1)th output of the N-stage rectifier to the input of a cascade of differential amplifiers. The amplified signal is quantized through a Schmitt-trigger comparator then an analog integrate-and-dump decodes the pulse-interval-encoded (PIE) input stream to extract the packet's content.

C. SECURITY AND LOGIC

The core of the security engine consists of an energy-efficient hardware accelerator for advanced encryption standard (AES) [9] in Galois counter mode (GCM) [10] for authenticated encryption and decryption. The two main components of the AES-GCM module are the AES block cipher (the forward cipher mode is used for both encryption as well as decryption) and the GHASH hash function (which uses Galois field multiplications for authentication). The AES block cipher is implemented as a 128-bit data-path with a parallel architecture leveraging larger active area to provide an energy-efficient design operating for only short periods of time [8]. The AES implementation consists of 20 parallel instances of the S-Box (substitution function) which is not only the most important nonlinear component of the AES function but also accounts for majority of the area and power consumption. Out of these 20 S-Boxes, 16 are used for the encryption and the remaining four are used for the key schedule computation. The GHASH implementation consists of four Galois multiplication stages which are executed iteratively and provides the perfect a balance between area and energy efficiency [8]. The AES module takes 11 cycle per block encryption and the GHASH module takes 32 cycles per Galois field multiplication. Fig. 5 shows a block diagram of the overall architecture of the AES-GCM engine.

The on-chip AES-GCM security engine ensures node authenticity and data confidentiality. It is employed to authenticate the downlink commands as well as encrypt the uplink biometric data being transmitted via RF backscatter. The AES-GCM engine utilizes a counter-mode encryption

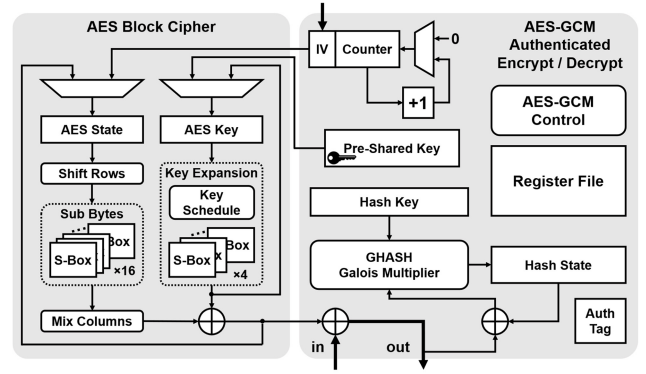


FIGURE 5. Block diagram of AES-GCM security engine.

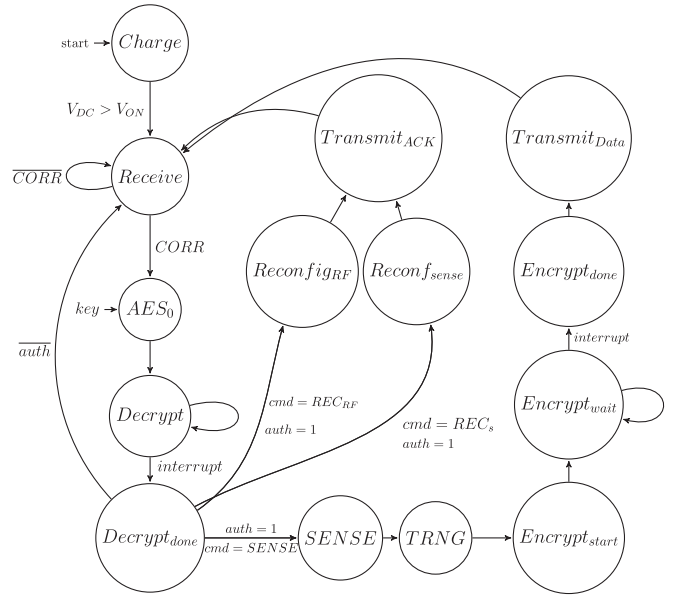


FIGURE 6. System-level finite-state machine controls the node operation from charging to reconfiguration, sensing, and communication.

algorithm which requires a unique initialization vector (IV) to be used with each new block of data. A switched-capacitor chaos map is designed as a TRNG to generate the IV for the security engine. Such TRNG comes at a 2% power overhead only as it shares the ADC with the sensor front-end to quantize the TRNG output for each block-cipher.

The SoC finite-state machine is illustrated in Fig. 6 starting with the *Charge* state where the RF harvester stores the input RF energy on an off-chip storage capacitor. The chip keeps charging till the stored dc voltage V_{DC} is higher than the PMU turn on threshold V_{ON} . Then, the LDO is powered up and regulates the supply for the receiver chain (*Receive* state) to decode the input bits until the correlator detects a 20-bit preamble signifying the beginning of the packet. The 280-bit downlink packet is stored, with a custom structure illustrated in Fig. 7, and the encrypted command is passed on to the AES-GCM engine along with the IV and authentication tag for authentication and decryption.

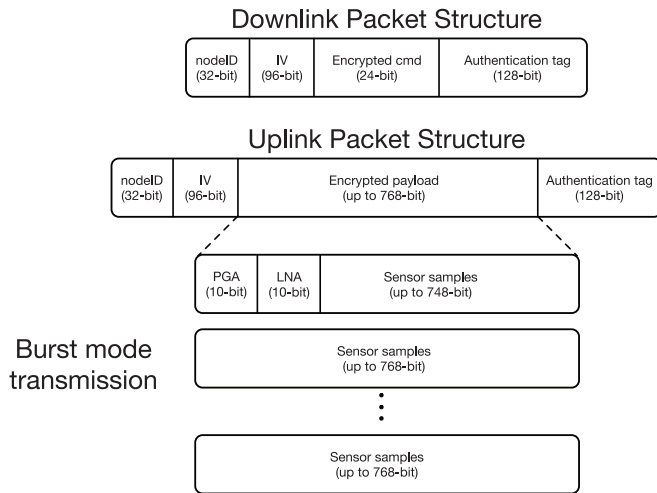


FIGURE 7. Custom packet structure allows for over-the-air programming, authentication, and burst-mode communication.

The AES-GCM engine is then turned on with a 128-bit hardwired preshared key. The chip remains in the *Decrypt* state till the engine triggers an interrupt signal along with the authentication result. An unauthenticated packet returns the chip to the *Receive* state while an authenticated one is decrypted into a downlink command to reprogram the chip over-the-air (Reconfig_{RF} or Reconf_{sense} states) or to begin in-body strain sensing in the *SENSE* state.

For the *SENSE* state, the chip progresses by turning on the AFE and ADC along with the dc offset cancelation loop. After the front-end settles, the ADC is multiplexed to the TRNG to generate the IV and buffer it for encryption. Finally, in-body strain sensing starts with the data being encrypted, buffered, and backscattered to the reader. The internal accumulator states and gain configurations of the LNA and PGA are concatenated in the first 20 bits of the uplink packets, as illustrated in Fig. 7.

In principle, a nonvolatile memory can be used to store the optimum configurations for the chip. However, non-volatile memories require a higher voltage for their read and write cycles compared to the subthreshold regime of 0.5 V that the implant utilizes. Over-the-air programming mitigates increasing the node's supply voltage, and power, by taking advantage of the power asymmetry between the reader and the node.

D. ADC-SHARING AND TRNG

The generation of the IV for the AES-GCM engine at a low area and power overhead can be achieved by sharing the SAR ADC between the sensor front-end and the TRNG circuit.

The TRNG is implemented as a discrete-time chaos-map, utilizing a residue amplifier which is similar to a 1.5-bit stage of a pipeline ADC but the residue is fed back to the input [11], [12]. With a random initial sample based on the circuit noise, the output bifurcates into a range of random numbers covering the voltage range of the whole amplifier.

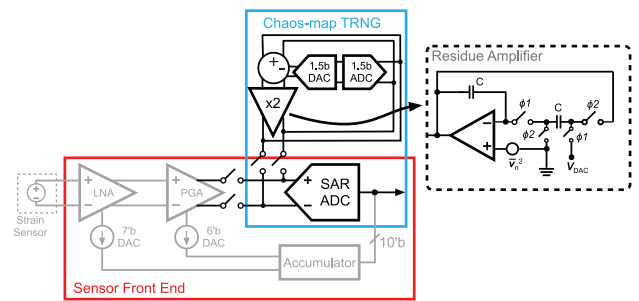


FIGURE 8. TRNG schematic highlighting how the sensor front-end shares the ADC with the TRNG.

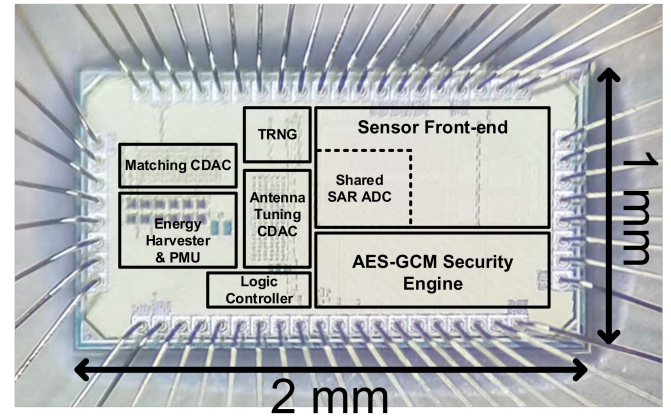


FIGURE 9. Magnified die photo of the 2-mm² strain sensing SoC.

The random discrete output is then sampled by the SAR ADC as it is multiplexed to take its input from the TRNG as shown in Fig. 8 during the TRNG state of the system-level finite-state machine before beginning encryption in the Encrypt_{start} state.

III. MEASUREMENT RESULTS

The chip was fabricated using a TSMC 65-nm CMOS process occupying a 2 mm×1 mm active area as shown in the die photo of Fig. 9 which illustrates the main building blocks of the SoC. A commercial strain sensor is interfaced with the sensor node SoC which is mounted on a PCB with a printed microstrip antenna.

The active power consumption of the chip varies from one state of operation to the other. The maximum power is consumed when the security engine is on and draining 4.8 μ W contributing to 43.7% of the total active power, as shown in Fig. 10. In contrast, during other states the power is dominated by the PMU which provides a stable supply for the logic, AFE, transmitter, and receiver.

A. WIRELESS HARVESTING AND COMMUNICATION

The strain-sensing SoC is evaluated in a wireless setup where an RF signal generator is configured as a custom base station.

The SoC powers up by harvesting the incoming RF energy through its reconfigurable rectenna, storing it over an off-chip capacitor, and generating an LDO-regulated supply of

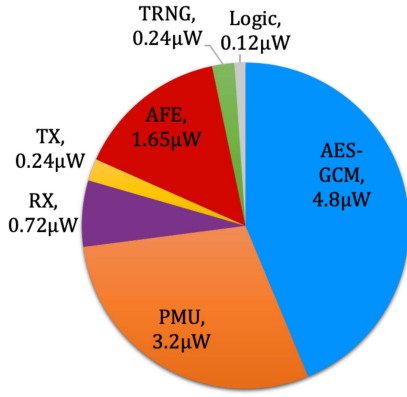


FIGURE 10. Breakdown of the active power consumption of key blocks.

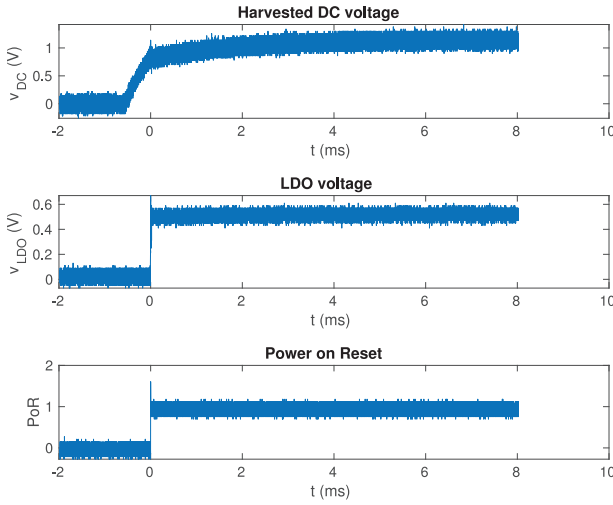


FIGURE 11. Voltage measurements versus time showing the energy harvesting operation.

0.55 V for the remaining baseband and communication circuits. Then, the PMU generates a PoR signal to initialize all internal states of the finite state machine to their default values as shown in Fig. 11.

The downlink packet can be a Reconfigure command used to reprogram the sensor and the RF front-ends, or a “Sense” command used to acquire biometric data. When a Sense packet is received, the SoC turns on the sensor interface to sample the strain input. The time-domain measurements of the uplink operation are shown in Fig. 12 in which the security engine triggers an *interrupt* signal once an authentication result is ready. An authenticated packet progresses to power up the sensor interface and the ADC starts buffering its samples serially. Then, the AES-GCM engine encrypts the data and the payload is framed with the header to be backscattered to the reader.

The measured uplink bitstream is magnified in Fig. 13, showing the packet composition. The packet header contains a 32-bit node ID to select the sensor as well as a 96-bit IV used by the security engine. Then, the payload carries a variable-length data followed by a 128-bit authentication

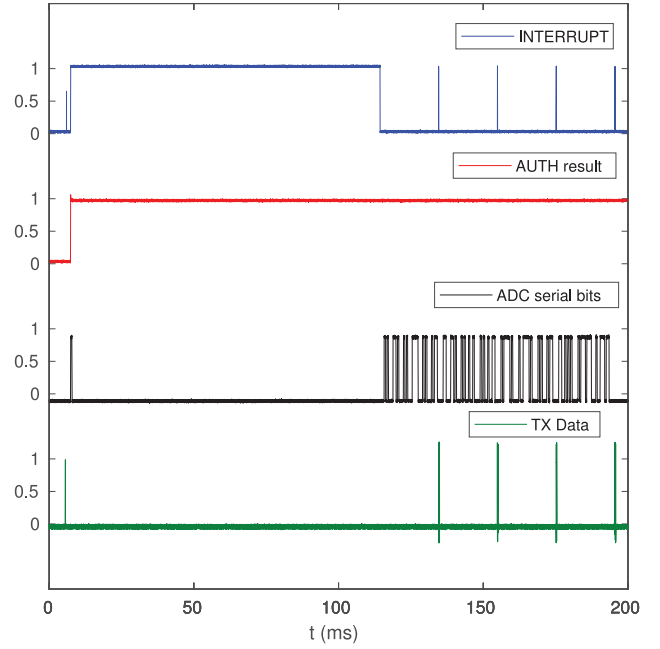


FIGURE 12. Downlink and uplink measurements showing the decryption operation, sensor data sampling, and backscattering data.

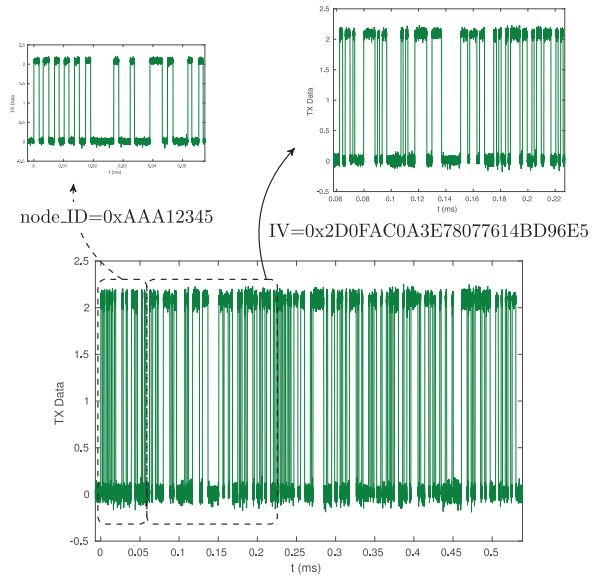


FIGURE 13. Zoomed-in measurement of the uplink packet showing the packet structure with the node_ID and IV by the TRNG.

tag. The bursts of packets are then buffered, FM0 encoded, and backscattered to the base station.

B. CROSS-TISSUE ADAPTATION

To characterize how the SoC adapts across different tissues, the rectenna is programmed across its range of bandwidths and center frequencies showing its full range of coverage. To tune the bandwidth and center frequency, we varied the tuning capacitance C_t and the matching capacitance C_m and the antenna’s programmable architecture described earlier.

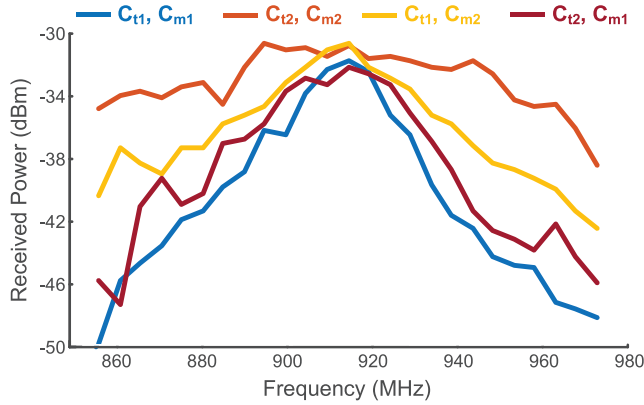


FIGURE 14. Reconfigurable RF bandwidth across different configurations scaling from 10 to 80 MHz.

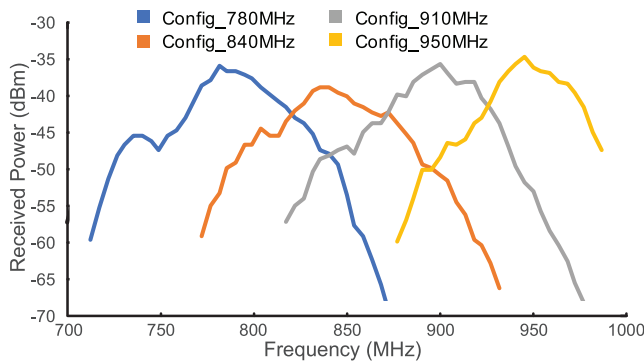


FIGURE 15. Reconfigurable center frequency covering a 300-MHz tuning range.

1) BANDWIDTH ADAPTATION

The first adaptation experiment focused on evaluating the bandwidth reconfigurability. To measure the bandwidth, we transmitted an RF carrier frequency from an external source and programmed the SoC to backscatter at different frequencies. The RF signal generator starts by transmitting a constant frequency signal to power up the node. The node then backscatters at different frequencies and a spectrum analyzer is used to measure and record the magnitude of the backscattered power at different frequencies around the RF carrier. Such measurement is then repeated across different configurations for the antenna programming and the optimum configurations for different bandwidths are plotted.

The measured RF bandwidth is shown in Fig. 14 where the rectenna can be reconfigured from a high-Q 10-MHz configuration to an 80-MHz bandwidth according to the available channel conditions.

2) RESONANCE ADAPTATION

The second adaptation experiment focused on evaluating the system's resonance reconfigurability. Similar to the above experiment, we transmitted an RF carrier frequency from an external source and programmed the SoC to backscatter at different frequencies. We measured the backscatter response using a spectrum analyzer.

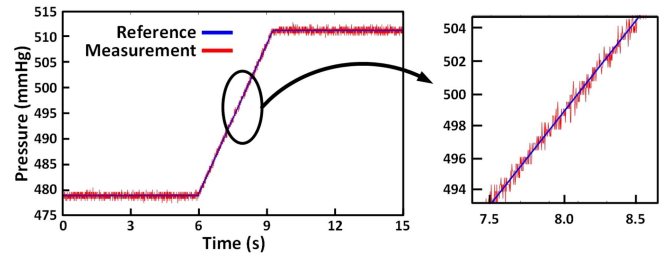


FIGURE 16. Measured digital output pressure versus time where the input steps across different values.

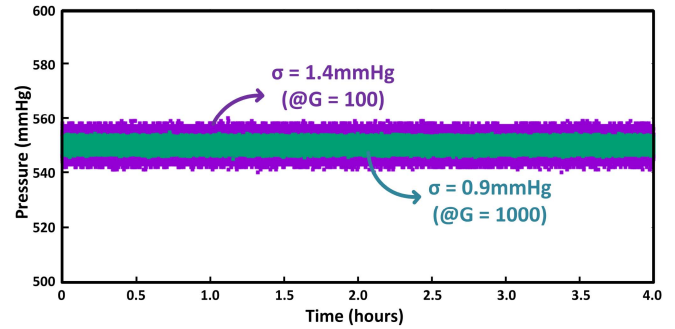


FIGURE 17. Measured long term pressure with time for different gain configurations with a resolution as low as 0.9 mmHg, respectively.

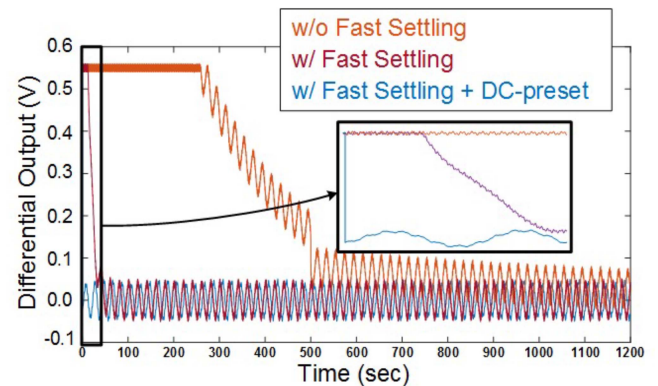


FIGURE 18. Measured transient settling of the sensor front-end showing 100× faster settling with over-the-air programming.

The measured RF bandwidth, plotted in Fig. 15, shows that the system's programmability extends to tuning the center frequency to adapt for different tissue environments where the optimum frequency of operation can be tuned covering a range of 300 MHz demonstrated in the figure.

C. IN-BODY PRESSURE SENSING

The main function of the sensor front-end is to amplify the strain signal to the full dynamic range of the 10-bit ADC while canceling the offset to prevent saturation. The measured time-domain digital output is plotted in Fig. 16 for a continuous pressure measurement setup. The figure demonstrates how the 10-bit samples track the input reference pressure during a fixed-value pressure and as it progresses inside its dynamic range. Additionally, Fig. 17 plots the long

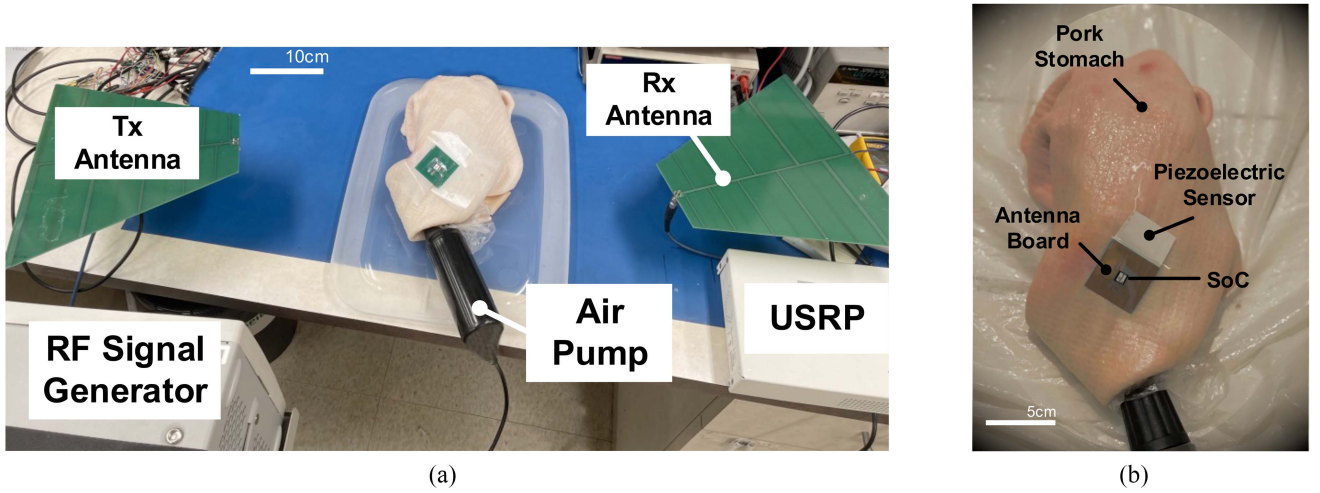


FIGURE 19. Ex-vivo measurement setup for in-body strain sensing. (a) Wireless measurement setup with an air pump mimicking stomach fluid flow. (b) Sensor laminated over pork stomach.

TABLE 1. Comparison of the sensor front-end with the state of the art.

Specification	This Work	[13]	[3]	[14]	[15]
Supply Voltage (V)	0.55	3.6-4.2, 1.2	1.9	1.2, 3.6	1.35
Power (μ W)	1.65	8.52	100	2.65	35.6
Energy/Conversion (nJ/conv.)	4.29	68.1	100	10.6	8290
Resolution (mmHg)	1.37	0.3	0.78	1.1	0.67
FoM (mmHg-nJ/conv.)	5.9	20.43	78	11.66	5554.3
Pressure range (mmHg)	0-2000	90-900	400-1200	100-900	0-60

term accuracy by measuring the dc output for a fixed pressure input over a 4-h period. The measurement is performed at a low-gain configuration ($G = 100$) achieving a resolution with a standard deviation of $\sigma_{G,low} = 1.37$ mmHg, whereas a high-gain configuration ($G = 1000$) provides a resolution of $\sigma_{G,high} = 0.9$ mmHg deviation.

The PMU provides a 0.55-V supply to the sensor front-end which consumes 1.65 μ W, achieving a conversion efficiency of 4.29 nJ/conv. step. With a 1.37-mmHg resolution, the system achieves a figure of merit (FoM) of 5.9 mmHg-nJ/conv. step, where a lower FoM ($FoM = [Power/f_s \cdot resolution]$) represents higher accuracy and energy efficiency for the design. Our sensor front-end is compared to the state-of-the-art pressure sensor front-ends in Table 1 showing our lower power consumption and, subsequently, FoM.

D. OVER-THE-AIR PROGRAMMING

Closing the loop with the base station takes advantage of the power asymmetry between the node and the reader providing a way to store internal states and program the node for optimum performance.

To evaluate the benefit of our design, we measured the settling time of the sensor front-end under three different settings. Our baseline setting does not incorporate any method for fast settling. The second setting involves turning on the fast settling capability of the design. The third setting incorporates setting the dc-preset to previously determined value,

which can be obtained from an earlier settling period and transmitted over the air to the wireless node.

Fig. 18 plots the differential output of the front-end as a function of time for each of these three settings. The figure shows that the baseline without fast settling (orange plot, takes about 500 s) to settle. In contrast, with our front-end's fast settling, the voltage settles within 20 s. Finally, our entire design (which would include both fast-settling and over-the-air programming with the stored internal state), the settling time drops to only 2 s. This result shows that our design reduces the settling time by two orders of magnitude, which yields very low latency and higher overall energy efficiency by eliminating the settling time overhead of the front-end.

E. EX-VIVO MEASUREMENTS

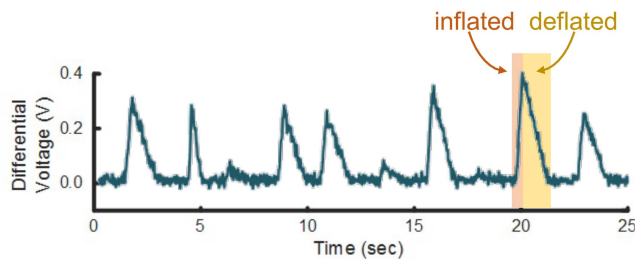
The full system is evaluated in an ex-vivo setup demonstrated in Fig. 19(a). An RF signal generator is used to provide the RF signal to power up the node. The transmit power is around 10 dBm and the node is at a distance of 15–30 cm from the TX antennas. The reader employs a similar log-periodic antenna connected to a software radio (USRP) as a reader to decode and extract the backscattered biomedical data, while an air pump is used to mimic the flow of fluids in tissues. The chip with the microstrip antenna are mounted on a piezoelectric sensor and laminated on a pork stomach as shown in Fig. 19(b).

To test the system functionality, the measured differential voltage from the sensor front-end is plotted against time as an external pump inflates and deflates the pork stomach. The measured voltage tracks the pressure variations, shown in Fig. 20 showing clear regions of inflation and deflation along the time axis as the fluid is pumped into the stomach.

Table 2 compares the SoC to existing batteryless sensing nodes. This work uses far-field to power up and communicate with a distance of up to 30 cm from tissues and consumes a

TABLE 2. Comparison of the state-of-the-art batteryless sensor nodes.

Specification	This Work	[16]	[6]	[17]	[2]	[18]	[19]
Technology	65nm	180nm	65nm	65nm	180nm	130nm	1.5 μ m
Distance from Tissues	15-30cm	1cm	-	Contact	<5cm	<5cm	<5cm
Energy Harvesting	Far-field (900MHz)	Near-field (250MHz)	Far-field (900MHz)	Ultrasound (2MHz)	Near-field (27MHz)	Near-field (433MHz)	Near-field (4MHz)
Voltage	0.55V	1.3V	0.55V	1.2V	1.5V	1.5V/2.75V	2V
Power Consumption	11 μ W	926-2105 μ W	0.6-2.5 μ W	140 μ W	2700 μ W	16.1 μ W	300 μ W
Communication	RF Backscatter	UWB	RF Backscatter	Ultrasound	RF Backscatter	RF Backscatter	Active RF
Datarate	DL: 40kbps UL: 6Mbps	DL: 2.5Mbps UL: 150Mbps	6Mbps	400kbps	27Mbps	DL: 125kbps UL: 125kbps	48kbps
Center frequency adaptation	300MHz	-	200MHz	-	-	-	-
BW adaptation	10-80MHz	-	-	-	-	-	-
Security	128-bit AES-GCM	-	-	-	-	Keccak auth.	-
Sensor Front-end	Strain	-	-	Oxygen	-	-	Pressure
Area	18.4cm ²	0.05cm ²	7.2cm ²	0.135cm ²	0.04cm ²	0.81cm ²	0.32cm ²


FIGURE 20. Measured sensor front-end voltage with time as the air pump inflates and deflates the pork stomach.

maximum active power of 11 μ W only. Compared to existing nodes, it provides a tunability of 300 MHz in the center frequency with an $8\times$ scaling of BW while guaranteeing security through a 128-bit AES-GCM engine.

IV. DISCUSSION AND CONCLUSION

This article describes an implantable strain sensing node as a fully integrated wireless and batteryless implant enabling far-field with 300-MHz frequency tunability and $8\times$ BW programmability. It incorporates a low-noise sensor front-end achieving a 4.3 nJ/conversion at 1.65- μ W active power consumption. Secure sensing and communication is achieved with a low-power TRNG through ADC-sharing between the security engine and the sensor interface.

One of the key advantages of our design is that it relies on far-field energy harvesting and backscatter, allowing it to communicate with a transceiver at a distance from the human body. Such contactless sensing would result in a qualitative improvement in future healthcare monitoring. In particular, in contrast to existing designs that require body contact (e.g., by requiring the user to wear an inductive coil vest or placing an ultrasound probe on their body), our approach would enable a seamless user experience that is similar to how mobile devices connect to nearby wireless access points today. For example, if an external transceiver is placed near a user's desk or bed, it can automatically

power up and communicate with our far-field microimplants whenever the user is in their vicinity.

More broadly, the ability to perform wireless, batteryless, and secure in-body sensing opens important applications for long-term monitoring of internal biometrics, may allow for early diagnosis and intervention, and paves the way for closed-loop treatment systems (e.g., drug delivery) that continuously monitor and respond to critical vital signs.

REFERENCES

- [1] Y. Ma, Z. Luo, C. Steiger, G. Traverso, and F. Adib, "Enabling deep-tissue networking for miniature medical devices," in *Proc. Conf. ACM Spec. Interest Group Data Commun.*, 2018, pp. 417–431.
- [2] J. Thimot, K. Kim, C. Shi, and K. L. Shepard, "A 27-Mbps, 0.08-mm³ CMOS transceiver with simultaneous near-field power transmission and data telemetry for implantable systems," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2020, pp. 1–4.
- [3] M. J. Weber, Y. Yoshihara, A. Sawaby, J. Charthad, T. C. Chang, and A. Arbabian, "A miniaturized single-transducer implantable pressure sensor with time-multiplexed ultrasonic data and power links," *IEEE J. Solid-State Circuits*, vol. 53, no. 4, pp. 1089–1101, Apr. 2018.
- [4] M. R. Abdelhamid, U. Ha, U. Banerjee, F. Adib, and A. Chandrakasan, "Wireless, batteryless, and secure implantable system-on-a-chip for 1.37mmHg strain sensing with bandwidth reconfigurability for cross-tissue adaptation," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2022, pp. 1–2.
- [5] C. Dagdeviren et al., "Flexible piezoelectric devices for gastrointestinal motility sensing," *Nat. Biomed. Eng.*, vol. 1, no. 10, pp. 807–817, 2017. [Online]. Available: <https://doi.org/10.1038/s41551-017-0140-7>
- [6] M. R. Abdelhamid, R. Chen, J. Cho, A. P. Chandrakasan, and F. Adib, "Self-reconfigurable micro-implants for cross-tissue wireless and batteryless connectivity," in *Proc. 26th Annu. Int. Conf. Mobile Comput. New.*, 2020, pp. 1–14. [Online]. Available: <https://doi.org/10.1145/3372224.3419216>
- [7] S. Maji et al., "A low-power dual-factor authentication unit for secure implantable devices," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2020, pp. 1–4.
- [8] U. Banerjee, A. Wright, C. Juvekar, M. Waller, Arvind, and A. P. Chandrakasan, "An energy-efficient reconfigurable DTLS cryptographic engine for securing Internet-of-Things applications," *IEEE J. Solid-State Circuits*, vol. 54, no. 8, pp. 2339–2352, Aug. 2019.
- [9] "Advanced encryption standard (AES)," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. FIPS PUB 197, Nov. 2001.
- [10] "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. Special Publication 800-38D, Nov. 2007.

- [11] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 12, pp. 3124–3137, Dec. 2010.
- [12] M. Kim, U. Ha, Y. Lee, K. Lee, and H.-J. Yoo, "A 82nW chaotic-map true random number generator based on sub-ranging SAR ADC," in *Proc. 42nd Eur. Solid-State Circuits Conf. (ESSCIRC)*, 2016, pp. 157–160.
- [13] S. Jeong, Y. Kim, G. Kim, and D. Blaauw, "A pressure sensing system with ± 0.75 mmHg (3σ) inaccuracy for battery-powered low power IoT applications," in *Proc. IEEE Symp. VLSI Circuits*, 2020, pp. 1–2.
- [14] S. Oh et al., "A 2.5nJ duty-cycled bridge-to-digital converter integrated in a 13mm³ pressure-sensing system," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2018, pp. 328–330.
- [15] H. Bhamra, J.-W. Tsai, Y.-W. Huang, Q. Yuan, and P. Irazoqui, "21.3 a sub-mm³ wireless implantable intraocular pressure monitor microsystem," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2017, pp. 356–357.
- [16] H. Rahmani and A. Babakhani, "A wirelessly powered reconfigurable FDD radio with on-chip antennas for multi-site neural interfaces," *IEEE J. Solid-State Circuits*, vol. 56, no. 10, pp. 3177–3190, Oct. 2021.
- [17] S. Sonmezoglu and M. M. Maharbiz, "34.4 a 4.5mm³ deep-tissue ultrasonic implantable luminescence oxygen sensor," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2020, pp. 454–456.
- [18] C. S. Juvekar, H.-M. Lee, J. Kwong, and A. P. Chandrakasan, "16.2 A Keccak-based wireless authentication tag with per-query key update and power-glitch attack countermeasures," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2016, pp. 290–291.
- [19] P. Cong, N. Chaimanonart, W. H. Ko, and D. J. Young, "A wireless and batteryless 130mg 300 μ W 10b implantable blood-pressure-sensing microsystem for real-time genetically engineered mice monitoring," in *IEEE Int. Solid-State Circuits Conf. Dig. Tech. Papers*, 2009, pp. 428–429.



MOHAMED R. ABDELHAMID (Member, IEEE) received the B.S. and M.S. degrees in electronics and electrical communications engineering from Cairo University, Cairo, Egypt, in 2013 and 2015, respectively, and the S.M. and Ph.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2017 and 2021 respectively.

He was a Ph.D. student with MIT from 2015 to 2017, where he worked on the design of low-power radio for the Internet of Things and reconfigurable in-body implants. He held internships as an Analog Designer with Texas Instruments, Dallas, TX, USA, in 2017, and with Apple, Cupertino, CA, USA, in 2019.

Dr. Abdelhamid was the recipient of the Endowed Fellowship of the Arab Republic of Egypt at MIT, and the Winner of the International Microelectronics Olympiad at Armenia in 2014.



UNSOO HA received the B.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute for Science and Technology (KAIST), Daejeon, South Korea, in 2012 and 2017 respectively.

He is currently a Research Scientist with the Signal Kinetics Group (Advised by Prof. Fadel Adib), Massachusetts Institute of Technology (MIT) Media Lab, MIT, Cambridge, MA, USA. His primary research interests are in the area of wireless and mobile sensing systems. He is particularly interested in designing and building new low-cost, ubiquitous technologies and systems for human health and wellbeing.



UTSAV BANERJEE (Member, IEEE) received the B.Tech. degree in electronics and electrical communication engineering from the Indian Institute of Technology (IIT) Kharagpur, Kharagpur, India, in 2013, and the S.M. and Ph.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2017 and 2021, respectively.

He was with the Low-Power System-on-Chip Design Team, Qualcomm, Bengaluru, India, from 2013 to 2015, where he was involved in the design and verification of power management architectures for Snapdragon mobile chipsets. Since October 2021, he has been with the Indian Institute of Science (IISc), Bengaluru, where he is currently an Assistant Professor with the Department of Electronic Systems Engineering. His research interests include cryptography, hardware security, digital circuits, and embedded systems.

Dr. Banerjee was a recipient of the President of India Gold Medal from IIT Kharagpur in 2013, the Irwin and Joan Jacobs Presidential Fellowship from MIT in 2015, the Qualcomm Innovation Fellowship in 2016, the Pratiksha Trust Young Investigator Award from IISc in 2022, and the ABB Research Award in 2022.



FADEL ADIB received the B.Eng. degree in computer and communications engineering from the American University of Beirut, Beirut, Lebanon, in 2011, and the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2016.

He has been a Faculty Member with MIT, since 2016, where he is currently an Associate Professor with the Department of Electrical Engineering and Computer Science and the MIT Media Lab.

He is the Founding Director of the Signal Kinetics Group, MIT, which invents wireless and sensor technologies for networking, health monitoring, robotics, and ocean IoT. He is also the Founder and the CEO of Cartesian Systems, a spinoff from his lab that focuses on mapping indoor environments using wireless signals.

Dr. Adib has received various awards and honors for his research. He was named by Technology Review as one of the world's top 35 innovators under 35 and by Forbes as 30 under 30. He is also the recipient of the ACM SIGMOBILE Dissertation Award in 2018, the NSF CAREER Award in 2019, the ONR Young Investigator Award in 2019, the ONR Early Career Grant in 2020, the Google Faculty Research Award in 2017, the Sloan Research Fellowship in 2021, and the ACM SIGMOBILE Rockstar Award in 2022. His research on wireless sensing (X-Ray Vision) was recognized as one of the 50 ways MIT has transformed Computer Science, and his work on robotic perception (Finder of Lost Things) was named as one of the 103 Ways MIT is Making a Better World. His commercialized technologies have been used to monitor thousands of patients with Alzheimer's, Parkinson's, and COVID19, and he has had the honor to demo his work to President Obama at the White House. His papers have won awards for best papers, demos, and highlights at premier academic venues, including SIGCOMM, MobiCom, CHI, and Nature Electronics.



ANANTHA P. CHANDRAKASAN (Fellow, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer sciences from the University of California at Berkeley, Berkeley, CA, USA, in 1989, 1990, and 1994, respectively.

He has been with the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, since September 1994, where he is currently the Vannevar Bush Professor of Electrical Engineering and Computer Science. He was the Director of the MIT Microsystems Technology Laboratories,

MIT from 2006 to 2011, and the Head of the MIT Department of Electrical Engineering and Computer Science from July 2011 to June 2017. He has been Dean of the MIT School of Engineering, MIT since July 2017. He has coauthored the *Low Power Digital CMOS Design* (Kluwer Academic Publishers 1995), *Digital Integrated Circuits* (Pearson Prentice-Hall, 2003, 2nd edition), and *Subthreshold Design for Ultra-Low Power Systems* (Springer 2006). His research interests include ultralow-power circuit and system design, energy harvesting, energy-efficient RF circuits, and hardware security.

Dr. Chandrakasan was a co-recipient of several awards, including the 2007 ISSCC Beatrice Winner Award for Editorial Excellence and the ISSCC Jack Kilby Award for Outstanding Student Paper in 2007–2009. He received the 2009 Semiconductor Industry Association University Researcher Award and the 2013 IEEE Donald O. Pederson Award in Solid-State Circuits, the Honorary Doctorate from KU Leuven in 2016, the UC Berkeley EE Distinguished Alumni Award in 2017, and the 2019 IEEE Solid-State Circuits Society Distinguished Service Award. He was elected to the National Academy of Engineering in 2015 and the American Academy of Arts & Sciences in 2019. He has served in various roles for the IEEE ISSCC, including the Program Chair, the Signal Processing Subcommittee Chair, and the Technology Directions Subcommittee Chair. He served as the Conference Chair for ISSCC from 2010 to 2018. He serves as the Senior Technical Advisor for the Conference starting ISSCC 2019. He was elected as fellow of the Association for Computing Machinery (ACM) in 2020.