Backscatter Ex-Nihilo: Single-component, Fully-passive Backscattering for Microcontrollers

Stewart J. Thomas
Dept. of Electrical and Computer Engineering
Bucknell University
Lewisburg, PA, 17837 USA
stewart.thomas@bucknell.edu

Brian P. Degnan, Cristel Callupe Chavez, and Billy Culver
White River Technologies, Inc.
Lebanon, NH 03766 USA
degnan@whiterivertech.com

***Abstract*—This paper investigates the harvesting of RF power using the existing electrostatic discharge (ESD) protection circuits of most ICs. Because of the internal diode configuration, a single off-chip capacitor is enough to create a charge pump circuit for rectifying and storing sufficient DC power to passively operate a microcontroller. This paper explores ESD circuitry and shows the feasibility of ESD-based power harvesting. A proof-of-concept device demonstrates a fully-passive backscatter link created using a MSP430. Backscatter communication is achieved through modulation of the internal configuration of a General Purpose Input Output (GPIO) pin on a microcontroller. This type of circuit enables two types of communication: zombie-links in which data is able to be transferred after a device has had its battery removed, as well as a mechanism for hidden identification or verification data, such as chip dielets.**

I. Introduction

The Internet of Things (IoT) continues to be an ever present economic force and demands that radio links be ever examined. Current market predictions estimate that IoT is ushering in a 4th industrial revolution centered around data-driven decisions with 75B devices in use by 2025 [1]. With data serving as the raw material necessary for this new industry makeup, efficient means to transport sensed and collected information are paramount to improving device lifetime and successful deployments.

To operate in this low-power communication space, the IoT field has adopted many technologies developed by RFID practitioners. Since the first complete RFID tag was developed [2], research within RFID has closely examined efficient wireless power transfer [3]–[5], protocol efficiency [6], generalized RFID-based platforms [7]–[9], and backscatter communication [10]–[13], among other topics. The result has been a large variety of low-power applications [14]–[18] that rely fundamentally on the backscattering techniques first introduced in the middle of the 20th century [19].

One central theme to RFID research has been the expansion and diversification of backscattering systems beyond the mere transfer of a 96-bit EPC identification code [20]. At least with regard to the academic literature, the dream of a "wireless barcode" technology has shifted to a focus on low-power, efficient wireless sensing and collection of data. It is no coincidence that this has happened alongside the rise of IoT and ubiquitous sensing. Recent work has examined ways to combine low-power backscatter with the extant devices that speak traditional protocols. The Ensworth BLE modulator [17] is one example of this device expansion. Further work has shown that all modern digital devices with general purpose input/output (GPIO) pins are capable of backscattering information in a UHF context [21] as well as a fully-passive LF tag [22].

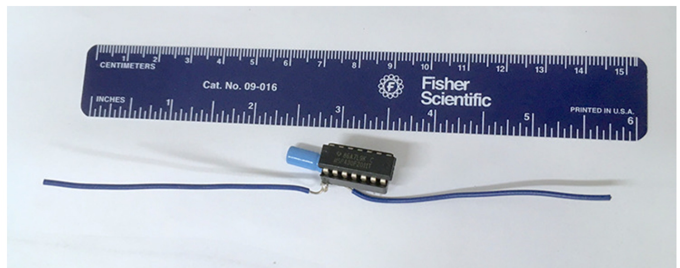

Fig. 1. Photograph of a single-component backscattering device.

In this work, we expand upon Zeroscatter modulation [21], and present a proof-of-concept device that is capable of fully-passive UHF backscatter communication using a commercial, off-the-shelf (COTS) microcontroller and a single, off-chip component. We see single-component, fully-passive backscattering from COTS digital devices directly benefiting two main areas. Firstly, single-component microcontroller backscattering allows for so-called "zombie links" that can extend device lifetime well beyond the limitation of a battery storage element. Once drained of power, an IoT device with a zombie link will still be capable of being powered wirelessly, allowing for stored data or sensed data to be wirelessly telemetered. For deployments where physical access to the IoT device is difficult, if not impossible, this link allows a device to still sense or transmit information and maintain some utility functions well after battery storage elements have been depleted or removed. Secondly, remotely powering devices can allow for wireless verification of Integrated Circuits (ICs) in the supply chain. DARPA kicked off the Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program in 2015 with the purpose of embedding RFID SHIELD dielets for insertion into the packaging devices for verifying component source integrity. As ICs already have a diode-capacitor structure in

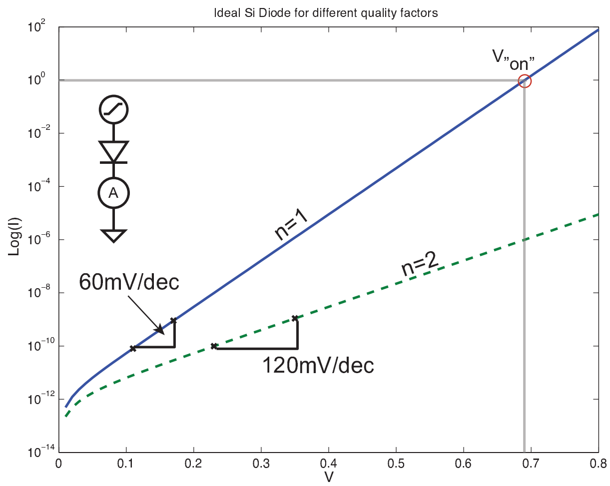

Fig. 2. The image presents the boundary conditions for the current of a silicon diode. For $n_q = 1$, one can see that the "turn on" voltage is lower than that of a diode with lower quality. Furthermore, by changing to a direct band-gap material with a narrower band, one would expect that the diode would "turn on" with less voltage.

the ESD protection, the same security that is available via a SHIELD dielet can be envisioned by the addition of circuitry to the existing silicon of a die, instead of a separate die integrated into the package of an IC, which was the approach in the SHIELD program.

In this paper, we present the theoretical background for harvesting wireless power from COTS circuits in Section II. Section III presents the proposed system for ESD-based power harvesting with simulation results. The proof-of-concept measurements are shown in Section IV. Section V provides a discussion followed by a conclusion.

II. Theory and Background

In passively-powered RFID systems, the minimum necessary blocks are power capture and reflection modulation. Power capture can be simplified to a diode with a capacitor to hold charge, and reflection can be achieved by a FET device that shorts the antenna to a reference.

A. Diode and Charge Pump Basics

The current of a diode is generalized as

$$I = I_S \left(e^{\left(\frac{V}{nU_t}\right)} - 1 \right), \tag{1}$$

with I_S as the zero-bias current where

$$I_s \propto e^{-E_G/(2n_q U_T)}, \tag{2}$$

and where E_G is the band gap, n_q is the diode "quality" and U_T is the thermal voltage. The value for n_q is expected to be between 1 and 2 and is a function of fabrication. Eqn. (2) is the slope of an extrapolated line between the measured minimum drain currents at each temperature for a diode. The effective band gap changes between materials that will thereby alter the "turn on" voltage, which historically was the voltage across the diode what was required to pass 1 A of current. The "quality" factor will also change the diode behavior. An illustration of the boundary conditions for a typical silicon diode is presented in Fig. 2. The rectifier that will act as a charge pump is simply a diode and a capacitor, and this configuration is illustrated in Fig. 4.

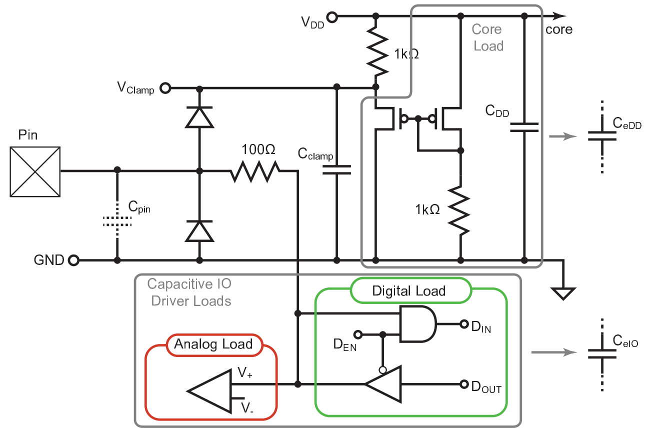

Fig. 3. The illustration depicts the I/O structure of the Microchip PIC12F1822 [23]. The ESD diodes are like isolated from VDD line, and this is suggested by the measured currents. This also suggests that the ESD diodes could be used as a rectifier with the digital load as a modulator under the appropriate conditions.

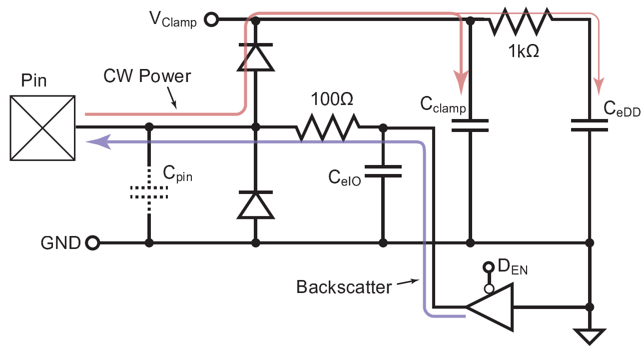

Fig. 4. The illustration depicts a simplified ESD structure where an ESD diode is used to place charge on capacitor. The GPIO driver enable line is then used as a backscatter load.

B. ESD architectures

ESD mitigation structures vary between pins as the structures are designed to protect the circuits that a pin contains. High current can destroy the device or decrease its reliability. The existence and magnitude of the current depend on the I/O type and the ESD protection device it contains. In the purely analog case, they are often as simple as passing the signal through a resistor to diodes tied to the voltage rails [24]. For purely digital pins, the ESD protection is often a simple diode and a voltage clamp. The general purpose GPIO pins of a MCU are more complex, with both types of ESD structure. This structure is illustrated in Fig. 3 with its simplification illustrated in Fig. 4.

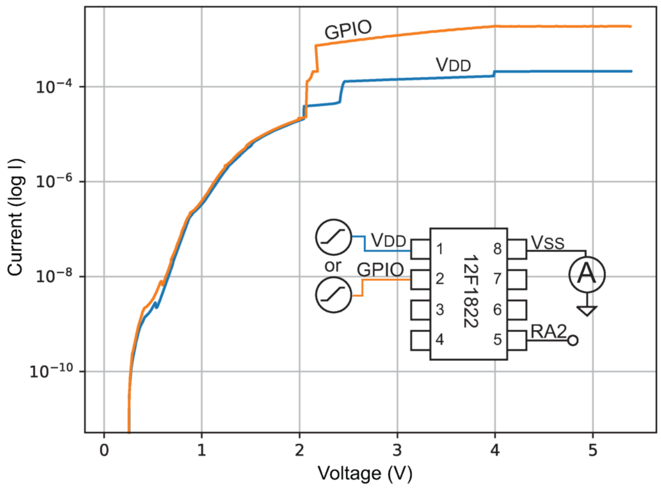

Fig. 5. The graph reports for the measured current data for a sweep of the VDD pin and a GPIO (RA5) pin on a logarithmic scale. The illustration depicts the test setup for a Microchip PIC12F1822 that was used to measure currents to ground through a picoammeter. The GPIO pin, as well as power, were ramped from 0 V to 5.5 V through the pins shown in the illustration.

C. MCU measurements

To show the broad application of ESD power harvesting, the work presented uses two microcontrollers: a Texas Instruments MSP430 series device and a Microchip PIC12 series device. Owing to availability, the MSP430 was characterized in an RF context. The current to the PIC12F1822 was measured by a sweep from 0 V to 5 V on both a power pin and a GPIO pin. The results are reported in Fig. 5. The data supports the conjectured ESD and IO structures that are presented in Fig. 3.

III. Proposed System

The proposed single-component, far-field, backscatter system consists of a microcontroller with a large capacitor connected between DC ground and the VDD supply pin combined with an antenna whose feed points are connected to the VDD supply pin and a GPIO pin. Because the antenna can be embedded in the associated circuit board traces (or even completely lacking in the case of a connectorized, cabled setup), this is not considered an extra component.

To show the connection between the ESD circuitry and a typical charge pump, a simplified circuit model for this system is shown in Fig. 6. Note that the RF return (i.e., ground) is separate from the DC circuit ground. This model shows the ESD diode configuration for a single GPIO pin. Items in gray (antenna connector and external capacitor) represent off-chip components. This circuit resembles a single-stage charge pump, or voltage multiplier, although it lacks the series capacitor [4].

To characterize the RF power harvesting performance, nonlinear harmonic balance simulations were performed in AWR Design Environment (formerly "Microwave Office") using the circuit in Fig. 6. The results from sweeping RF input power from a 915 MHz input signal are shown in Fig. 7. Simulations were carried out using both the standard SPICE diode model as

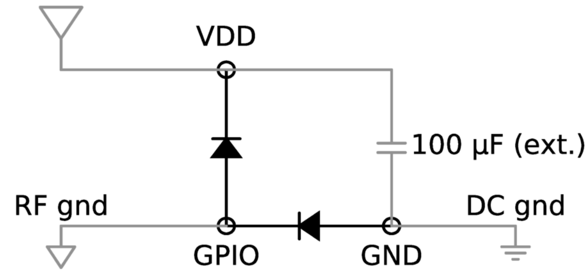

Fig. 6. Simplified schematic of ESD power harvesting circuit with off-chip components shown in gray used for nonlinear harmonic balance simulation.

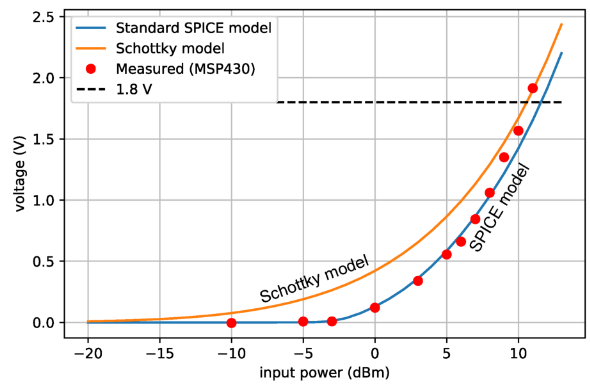

Fig. 7. Simulated and measured harvested voltage at 915 MHz.

well as a low-threshold Schottky model. With simplicity as an ultimate goal, no attempt in matching (whether in simulation or in experimental data) was performed. Although the 1.8 V turn-on logic level was reached at the relatively high value—as compared to RFID ICs—of approximately +10 dBm, further improvements can be gained by both inclusion of a matching network or inclusion of a series capacitor in the charge pump.

For experimental data, the microcontroller was programmed to perform one of two tasks, selected at power-on-reset. By reading the logic value of a designated GPIO pin at startup, the software determined if it was in an active state or a "zombie" state. Execution was then passed to the appropriate task. The active state allows for normal operations of the device. If the appropriate logic level was not detected at startup, the device assumes it is in the zombie state, and all clocks are slowed to conserve power and the GPIO pin with the antenna connected is used to wirelessly telemeter data. This dual-mode also allows the device to be powered by the harvested power by providing time for the capacitor to accumulate sufficient charge for operation.

IV. Measurements

A. Cabled setup

The simplified circuit from Fig. 6 was assembled using a Texas Instruments MSP430F2011 and a 22 μF capacitor, as shown in Fig. 1. To measure the harvested voltage, the

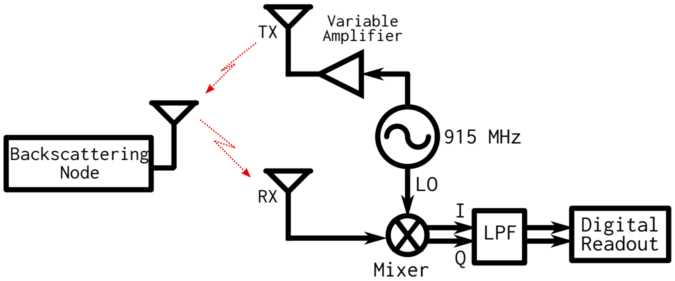

Fig. 8. Block diagram of the bistatic reader setup.

TABLE I
MEASURED CURRENT DRAW FOR CPU TASKS

	Current (at 3.3 V)		
	mean	min.	max.
Active	307 μA	306 μA	307.7 μA
"Zombie"	38 μA	422 nA	56.7 μA

antenna was replaced with a SMA connector and connected to a Agilent E4438C RF signal generator through a 50 Ω cable. A continuous wave 915 MHz MHz signal was sent to the device under test. As RF power was varied, DC voltage across the capacitor was recorded. This data is shown in Fig. 7 and closely follows the simulation data. The device's measured sensitivity was +10 dBm.

Current draw for the two microcontroller tasks was then measured. This data is presented in Table I. The measured data only represents the microcontroller itself and not other external peripherals. As expected, the zombie task draws significantly less current as it operates at a much lower clock frequency and communication duty cycle. It is also worth noting that the measured current draw is below the recommended 2 mA continuous current limit of the ESD protection diodes [25].

After programming the microcontroller, a wire dipole antenna was connected to the communications pin and VDD pin. Passive backscatter modulation is achieved through the zeroscatter modulation method by switching a GPIO pin's input/output direction register [21].

B. *Over-the-air measurements*

The single component backscattering device was then tested in an over-the-air (OTA) scenario in an indoor lab environment using a bistatic receiver. A block diagram of the reader is shown in Fig. 8. A +27 dBm, 915 MHz, CW source was transmitted to the device through a +6 dBi horizontally-polarized patch antenna (yielding a +33 dBm EIRP signal). The signal received by the RX antenna (+6 dBi, horizontally polarized patch antenna) was mixed with the local oscillator (LO) to perform direct to baseband conversion. The baseband I and Q signals were filtered and then captured using a benchtop oscilloscope. A photograph of the experimental setup is shown in Fig. 9.

Using this setup, the backscatter device was placed approximately 0.5 m away from the source. A simple resistive divider network connecting a voltage source to a GPIO pin allowed

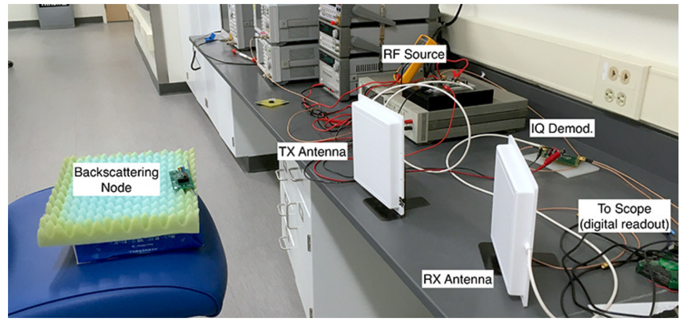

Fig. 9. Photograph of over-the-air bistatic experimental setup.

for the microcontroller to be switched between the so-called "active" modes and the "zombie" modes. By powering off the voltage source—mimicking a power source that has failed open—the microcontroller rectified the incoming RF signal through its ESD protection diodes, and powered the device, selecting the zombie task to execute. In this scenario, the MCU initialization code detects the presence or lack of a voltage source by reading the appropriate pin, and then hands off execution to either the normal task or an ultra-low-power task. For this prototype, the normal task or "active" mode consists of backscattering a payload. The ultra-low-power task or "zombie" mode reduces all clocks to minimal speed, and backscatters a second, shorter payload at a slower modulation rate.

Captured data is shown in Fig. 10. A packet consists of a short pilot tone, a Barker code, and the data payload containing data stored in memory. Fig. 10 shows the full packet (top) along with zooms of the three sections of the packet (bottom). In the bottom row, both the raw data is shown, along with the digitally processed data consisting of the sign of the normalized signal.

In this example, the air encoding for the bits consisted of a binary FSK encoding scheme with logic '1' encoded using a high frequency symbol (transition in the middle and end of a bit period) and logic '0' encoded with a low frequency symbol (transition only at the end of a bit period). Data recovery was performed using a zero crossing detector. In the packet shown, there were zero bit errors.

V. DISCUSSION

As we show in this work, in the simplest sense, it is possible to turn every existing IC into a fully-passive backscatter link with minimal additional components. However, there remains the question of power. The primary limitation is the ability for the ESD diodes to act as a rectifier, combined with the power-on-reset circuitry in the ICs. If the voltage and current requirements can be satisfied, a low-power method for IC communication or remote verification can indeed be realized based on the data presented in this work. It remains open question whether an MCU can act as a fully-passive device with no additional components. This would require sufficient internal capacitance allowing either a significant reduction of

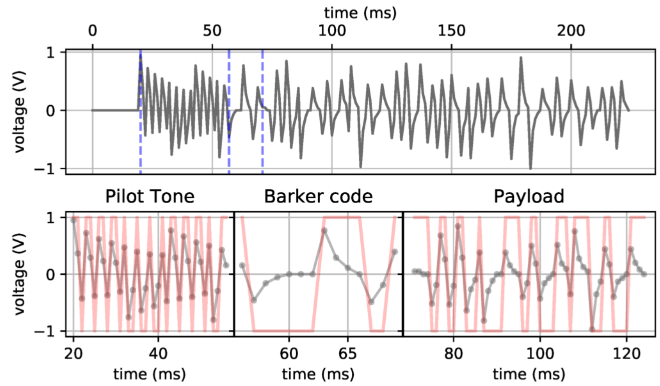

Fig. 10. Measured, over-the-air data from the fully-passive link with pilot tone, Barker code, and segment of data shown in the second row (respectively).

the off-chip capacitor, or its complete removal. Further modification of the standard ESD structures themselves may yield improved performance from a power harvesting perspective, while maintaining the intended protection function. Intentionally using power-harvesting-friendly ESD structures leaves open the possibility for wireless verification of ICs without a need for additional dielets introduced at the packaging stage.

However, it is also worth considering the possibility that these power harvesting structures may leave open a new avenue for malicious attacks. The possibility exists for a malicious agent to send high-powered RF signals with intent to either destroy or harm vulnerable circuits. Further, by sending a large RF signal and monitoring the return side-channels, it may be possible to extract sensitizing information from the ICs.

In this study, we have shown that it is possible for a microcontroller (or other digital device) to both harvest UHF power and wirelessly backscatter information. This demonstration shows an example of data uplink from a battery-free device. Such a system is primarily limited by a few factors. Firstly, the current limitations of the protection diodes. This provides an upper limit of the power consumption of the task—including sensors and computation. As mentioned, Texas Instruments specifies the diodes can sustain a continuous DC current of 2 mA [25] Secondly, the choice of capacitor, which serves as the energy reservoir during fully-passive operation, limits the task options. In this study, a 22 µF capacitor was used. Lastly, the protocol of choice will affect device performance. Faster modulation (and therefore switching) rates require faster clocks and ultimately higher power consumption. Protocols involving long sequences of pilot tones or other preambles, can rapidly drain the stored energy. The latter limitations can be overcome through use of a larger storage capacitor and duty-cycling the data rate to keep the time spent harvesting much greater than the time spent communicating. With increasing capacitor size comes an increased dwell time to allow for the capacitor to sufficiently charge. However, given the relatively high power levels in this study, such a long dwell time is not expected to significantly impact performance. Dynamic power consumption related to capacitor selection is not included in this study. Protocols that include transport mechanisms for framing data can help reduce the transmission duty cycle while also putting further power and complexity burden on the device to appropriately frame and transport the data. For large transmissions, this also extends the total time that the device must be illuminated and powered by RF. Concerning protocol, it should also be noted that this work does not examine the reader-to-tag downlink. This work considers the downlink to transmit a single bit encoded as RF presence or lack. While randomized time delay protocols [6] could allow for simultaneous time-divisioned transmissions, a further study of the demodulation capabilities of the protection diodes is needed.

With regard to the expanding IoT device infrastructure, this study yields promising results that integration of IoT devices with the low-power communication means well-known to the RFID community is possible. Enabling IoT devices to hold "dual-mode" functionality has promise to greatly extend device lifetime well beyond the utility of a single battery charge.

VI. Conclusion

In this paper, we have examine the feasibility of harvesting wireless power through the ESD protection structures that are present in existing microcontrollers. We present a theoretical basis for the operation of the ESD structures as a charge pump and measured data using a PIC12F1822 and MSP430F2011 MCU.

We also present an over-the-air demonstration of a fully-passive backscatter device consisting of an MSP430F2011 microcontroller with a single off-chip capacitor. This device is capable of operating as a zombie-link when no voltage source is present and wirelessly telemetering data from 0.5 m from a +27 dBm source.

References

[1] "Internet of Things (IoT) connected devices installed base world-wide from 2015 to 2025," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed: 2020-02-03.

[2] U. Karthaus and M. Fischer, "Fully integrated passive UHF RFID transponder IC with 16.7-μW minimum RF input power," *IEEE Journal of Solid-State Circuits*, vol. 38, no. 10, pp. 1602–1608, October 2003.

[3] D. Arnitz and M. S. Reynolds, "Wireless power transfer optimization for nonlinear passive backscatter devices," in *2013 IEEE International Conference on RFID*, Orlando, Florida USA, May 2013, pp. 245–252.

[4] C. Valenta and G. Durgin, "Harvesting wireless power," *IEEE Microwave Magazine*, pp. 108–120, June 2014.

[5] A. Sample and J. Smith, "Experimental results with two wireless power transfer systems," in *IEEE Radio and Wireless Symposium, 2009. RWS '09.*, January 2009, pp. 16–18.

[6] Y. Maguire and R. Pappu, "An Optimal Q-Algorithm for the ISO 18000-6C RFID Protocol," *IEEE Transactions on Automation Science and Engineering*, vol. 6, no. 1, pp. 16–24, January 2009.

[7] A. Sample, D. Yeager, P. Powledge, and J. Smith, "Design of a passively-powered, programmable sensing platform for UHF RFID systems," in *IEEE International Conference on RFID, 2007*, March 2007, pp. 149–156.

[8] S. J. Thomas, "RFID for Everyone: An Easily-Accesible, Experimental UHF RFID Platform," *IEEE Journal of RFID*, vol. 4, pp. 46–54, Mar. 2020.

[9] V. T. Talla, M. Buettner, D. Wetherall, and J. Smith, “Hybrid analog-digital backscatter platform with high data rate, battery-free sensing,” *IEEE Topical Meeting on Wireless Sensors and Sensor Networks (WiSNET)*, January 2013.

[10] P. Nikitin and K. Rao, “Theory and measurement of backscattering from RFID tags,” *IEEE Antennas and Propagation Magazine*, vol. 48, no. 6, pp. 212–218, 2006.

[11] P. Nikitin, K. Rao, and R. Martinez, “Differential RCS of RFID tag,” *Electronics Letters*, vol. 43, no. 8, pp. 431 – 432, April 2007.

[12] S. J. Thomas, E. Wheeler, J. Teizer, and M. S. Reynolds, “Quadrature amplitude modulated backscatter in passive and semipassive UHF RFID systems,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 4, pp. 1175–1182, April 2012.

[13] R. Correia, A. Voaventura, and N. B. Carvalho, “Quadrature amplitude backscatter modulator for passive wireless sensors in IoT applications,” *IEEE Trans. Microwave Theory and Techniques*, vol. 65, no. 4, pp. 1103–1110, Apr. 2017.

[14] S. J. Thomas, R. R. Harrison, A. Leonardo, and M. S. Reynolds, “A battery-free multichannel digital neural/EMG telemetry system for flying insects,” *IEEE Transactions on Biomedical Circuits and Systems*, vol. 6, no. 5, pp. 424–436, October 2012.

[15] V. Talla, B. Kellogg, S. Gollakota, and J. R. Smith, “Battery-free cellphone,” in *ACM Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 2, 2017, p. 105.

[16] J. Ensworth and M. S. Reynolds, “Every smart phone is a backscatter node: Modulated backscatter compatibility with Bluetooth 4.0 low energy (BLE) devices,” in *IEEE International Conference on RFID, 2015*, April 2015, pp. 78–85.

[17] ——, “BLE-backscatter: Ultra-low-power IoT nodes compatible with Bluetooth 4.0 low energy (BLE) smartphones and tablets,” *IEEE Trans. Microwave Theory and Techniques*, vol. 65, no. 9, pp. 3360–3368, 2017.

[18] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, “Wi-Fi backscatter: Internet Connectivity for RF-powered Devices,” in *Proceedings of the 2014 ACM Conference on SIGCOMM*. New York, NY, USA: ACM, 2014, pp. 607 – 618.

[19] H. Stockman, “Communication by means of reflected power,” *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, October 1948.

[20] EPC Global US, “Class 1 Generation 2 UHF RFID protocol for operation at 860MHz-960MHz, version 1.0.9,” Available online, *http://www.epcglobalus.org/*, 2005.

[21] A. Dadkhah, J. Rosenthal, and M. Reynolds, “Zeroscatter: Zero-Added-Component Backscatter Communication Using Existing Digital I/O Pins,” in *2019 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*. IEEE, Jan. 2019, pp. 1–3.

[22] “Using an AVR as an RFID tag,” https://scanlime.org/2008/09/using-an-avr-as-an-rfid-tag/, accessed: 2020-04-17.

[23] *PIC12(L)F1822/16(L)F1823*, Microchip, 4 2015, rev. E.

[24] B. Degnan and J. Hasler, “On the temperature dependence of subthreshold currents in MOS electron inversion layers, revisited,” in *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2016, pp. 2074–2077.

[25] Texas Instruments, “MSP430 system-level ESD considerations (SLAA530),” Texas Instruments, Tech. Rep., Mar. 2012.