Real-time Analysis for Wireless Power Transfer Observation and Recognition (RAWPTOR)

Shannon Beck
United States Air Force Academy
Shannon.Beck@afacademy.af.edu

Jordan Scott
University of Colorado Colorado Springs
jscott21@uccs.edu

Manohar Raavi
Kennesaw State University
mraavi3@kennesaw.edu

Caleb Dale
United States Air Force Academy
C24Caleb.Dale@afacademy.af.edu

Kaija Weishalla
United States Air Force Academy
C24Kaija.Weishalla@afacademy.af.edu

Brennan Worrell
United States Air Force Academy
C24Brennan.Worrell@afacademy.af.edu

***Abstract*—The Qi wireless charging protocol exposes electo-magnetic field (EMF)-based side-channel information. We share our lower-cost approach, discussing tools and techniques used to sniff and analyze information exchanged between the Qi charger and the charging device such as a mobile phone. We can detect devices at a distance that far exceeds the Qi protocol's specification of up to 4 cm (1.6 in), seeing signals as far away as 30.5 cm (12 in) in a noisy, uncontrolled environment, regardless of the device charging being powered on or off. This extended detection range enables adversaries to eavesdrop, hijack, and interfere with the wireless charging process, even when the receiver device is turned off.**

Our analysis reveals that the Qi communications leak unique device identifiers, such as manufacturer and device IDs, which can be leveraged for tracking and profiling users' behavior patterns. We discuss the challenges faced in directly demodulating the Qi signal, which is necessary for deeper protocol inspection and dynamic attack development.

Despite these difficulties, our research highlights the significant security and privacy risks introduced by the widespread adoption of Qi wireless charging technology. The accessibility of the required equipment, costing less than $2,500, underscores the need to increase user awareness of these vulnerabilities.

I. Introduction

Our research began with a replication of experiments from [1], where eavesdropping and hijacking attacks were performed. Replication was used to understand the communications between a Qi charger and a charging device, in our case, a mobile phone. Unable to directly demodulate the communications, we were able to use the Qi Sniffer by Avid to inspect the demodulated signals between the charging pad and the phone. Through the Qi Sniffer device, our team learned of the unique Qi ID values. The Qi ID is similar to the networking Media Access Control (MAC) address, where both indicate the device manufacturer and a device ID. Through intercepting the Qi protocol communications, this leakage of Qi ID is a possible side channel that can be used for detecting and tracking a device, detectable at a far distance greater than the specification, as discussed below.

During the replication of the eavesdropping and hijacking, we were able to craft and inject signal noise to perform a denial of charge (DoC) with the knowledge gained, using a waveform generator with packets with incorrect checksum values.

We are pursuing the direct demodulation of the Qi communication signals to be able to inspect the Qi communications for dynamic hijacking and injection, as well as getting the Qi ID to use for device tracking and possible pattern of life information.

Even without demodulation, we have shown we can detect charging devices, even when powered off, at a distance far greater than the charging specification. We have been pushing the limits of our signal detection of the Qi signal in the range of 2.5-30.5 cm (1-12 in) away from the Qi charging pad with success. This can be ideal in security scanning for sensitive environments where personal electronic devices are prohibited. Qi communications are active when paired with a pad, even when the device is powered off.

A. Background

Wireless power transfer (WPT) technology has seen a significant increase in adoption and development in recent years. The ability to charge electronic devices without the need for physical wired connections has enabled greater convenience and mobility for users. WPT systems typically operate by using an electromagnetic field to induce an electric current in a receiver device, allowing it to be charged wirelessly.

Wireless power transfer systems rely on the generation and coupling of electromagnetic fields to enable the wireless charging process. The transmitter in a system generates a time-varying magnetic field, which induces a voltage in the receiver's coil through electromagnetic induction. This induced voltage can then be used to charge the receiver's battery.

The strength and characteristics of the electromagnetic field play a critical role in the efficiency and range of wireless power transfer. Factors such as the frequency, amplitude, and spatial distribution of the field can impact the overall system performance. Additionally, the presence of conductive or magnetic materials near the charging system can potentially distort the electromagnetic field and affect the power transfer.

Understanding the electromagnetic field properties and protocols of WPT systems is essential for developing techniques to detect, monitor, and potentially exploit the side-channel

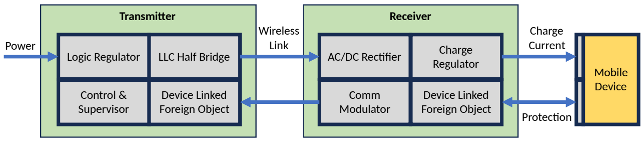

Fig. 1: Architecture of wireless charging

information leakage that may occur during wireless charging operations.

II. Qi Wireless Research - 2 pages

This project is built on 2023 Cadet's senior research work and includes further progression and in-depth reviews of WPT.

A. *Qi Protocol*

The Qi protocol is a wireless charging standard developed by the Wireless Power Consortium (WPC). The research in this paper is for the most part in regard to version 1.3 of the Qi protocol, however Qi 2.0 was recently announced in April of 2023. Version 1.3 of the Qi protocol uses a differential bi-phase encoding scheme in order to modulate data bits. This means that instead of signifying 1s and 0s with corresponding high and low transitions, Qi instead uses 0s to correspond to constant high and constant low states when transitions occur during the rising and falling edges of a clock signal. This means 1s correspond to a change from high to low or low to high within the middle of a single transition state period. The Qi protocol has four phases which are ping, configuration, initialization, and completion.

B. *Qi Wireless Consortium and Costs*

Founded in 2008, the Wireless Power Consortium is a group of over 300 companies that work together to define standards for wireless power. Many companies, such as Apple, Sony, Google, and others, are members of the Wireless Power Consortium. The group's goals include evolving alongside technological advances and other IoT devices outside the scope of small handheld devices. As of 2024, the annual membership fee is 30,000 dollars.

C. *Qi Sniffer*

The Qi Sniffer and the software associated with it were very helpful in the beginning stages of research as the team investigated the basic principles, bounds, and traits of Qi. In order to use the Qi Sniffer, the team downloaded the software and hooked up the Qi Sniffer to a laptop. In order to begin collecting information, the team learned that placing the Qi Sniffer near the charger and starting the Qi Sniffer first before placing the phone on the charger was needed in order to capture all four phases of the Qi protocol. The Qi Sniffer is able to provide unique manufacturer codes for each device, operating frequencies, charging power, error codes, and basic packet information.

D. *Moku*

The Moku is a device with many different capabilities. It simplified our lab setup and experimentation processes by compressing multiple of our devices into one and even into a much more intuitive and user-friendly format. One of the most useful functions to our team was the oscilloscope function, which can measure voltage over time. This function was key to the majority of our early research, especially in achieving an understanding of the process and components of Qi.

E. *HackRF*

The HackRF One is a device that is made to collect radio signals and output radio signals. It was made to work alongside the Pothos Flow. Pothos Flow is software that allows for analyzing of a radio signal in multiple ways, namely demodulation or amplification, and also allows for then outputting that signal.

F. *Nooelec SDR*

The Nooelec SDR was a program that was meant to pick up radio waves. It worked together with equipment that could be acquired with the software but did not need its own specific hardware. The software focused on displaying what frequencies are picked up by the hardware and displaying their strength. We planned to use this software in conjunction with another to narrow down what frequency the charger and phone communicate on, as well as attempt to demodulate the signal.

G. *Qi Chargers*

We have multiple different chargers and phones to perform tests with. We focused on only using one phone and one charger for the experiments detailed in this paper. The charger that we used was a Yootech wireless charging pad model F500 that was acquired from Walmart with the outer housing removed.

III. Research Process

There is scant published research on Qi attacks and information leakage. Some notable papers are [1]–[4]. We extend the current research by investigating the detection range and confirming the ability to detect when the device is powered off. We also performed extensive research into demodulating a Qi signal. However, this has proved much more intricate and difficult than originally thought.

Blending cybersecurity research with a physical layer is challenging. Hardware design has become so small that it is challenging to crack into boards to access information as it flows through a system. Figure 2 shows a transmission packet can be encrypted, encoded, and modulated prior to transmitting over a free space signal. A receiver would then demodulate, decode, and decrypt that signal before using the packet. When considering the reconnaissance of wireless signals, raw wireless signals hold very little useful information without the ability to demodulate, decode, and decrypt them. For Man in the Middle (MitM) attacks or even spoofing, the attacker has to be able to intercept, demodulate, decode,

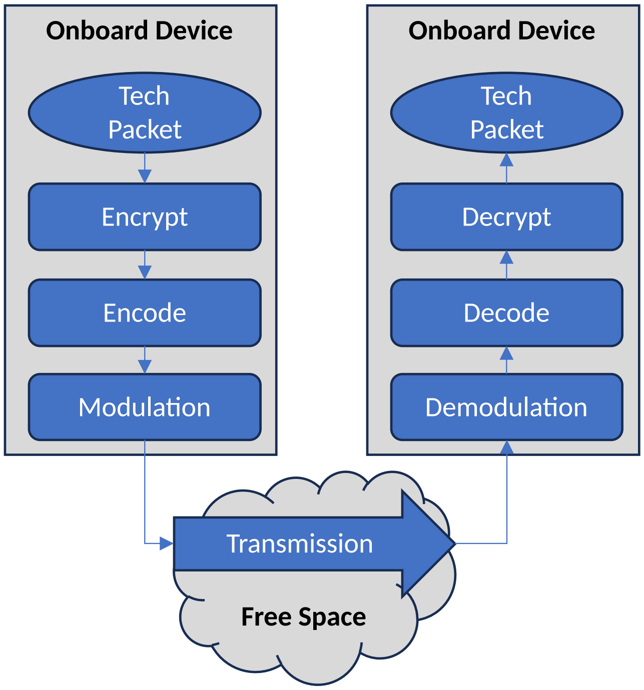

Fig. 2: Research design of wireless security

decrypt, manipulate the packet, then re-encrypt, re-encode, and re-modulate signals.

To accomplish this in near real-time is not an easy feat.

- Expensive Lab Equipment -
- On-board Probe Points -
- Daisy Chain Lab Equipment -
- Choose Alternative Attack Vectors -

IV. Experiment

A. Design

We wanted to create a realistic scenario to accomplish our low-cost-to-entry security research on Qi while including real-world considerations. Since today's security stations include passing bags through x-ray machines, it would be realistic to consider adding detection of Qi to detect a phone that has been turned off. Being able to detect phones turned off would significantly benefit security within secure areas where personal electronic devices are not permitted.

As shown in Figure 5, a phone that is turned off is placed into a bag. That bag is passed over a conveyor belt with embedded Qi chargers. The coils of the chargers are connected to an oscilloscope to monitor the voltage levels. A spectrum analyzer uses magnetic antennas to monitor signals sent from the Qi charger and device.

B. Tools

1) Nooelec NESDR SMArt v5 SDR - HF/VHF/UHF (100kHz-1.75GHz) RTL-SDR. RTL2832U & R820T2-Based Software Defined Radio: This device is used in conjunction with software and antennas that come with the product. It allows the user to detect radio waves across a spectrum (based on the antenna used) and the strength of the signal received. The antenna connects to the USB device that plugs directly into the computer.

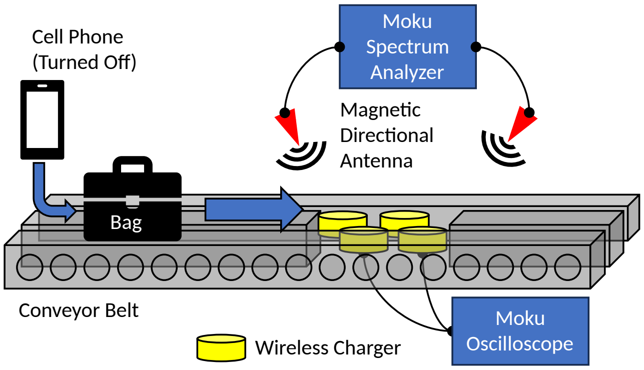

Fig. 3: Experiment design of Qi Active Detection

2) Liquid Instruments Moku:Go M1: The Moku:Go is a device that consolidates a lot of functions into one device. It has 10 basic functions, with 3 other functions that can be added to it along with an increase in the cost of the device. Some of the functions this team used the most were the oscilloscope and spectrum analyzer functions. Both Moku's have:

- Oscilloscope
- Spectrum Analyzer
- FIR Filter Builder
- Waveform Generator
- Frequency Response Analyzer
- Arbitrary Waveform Generator
- Data Logger
- PID Controller
- Digital Filter Box
- Logic Analyzer

White Top Moku only:

- Demodulation Tool

3) Keysight 33522B - Trueform Waveform / Function Generator with Arbitrary Capability (30 MHz / 2 Channel): This device allows the user to produce a waveform of varying frequency, amplitude, and type. Our team mostly used the sine waveform, a frequency around 150kHz, and 10V peak-to-peak amplitude. It can produce two signals at one time.

4) Tektronix TBS2000 Series Digital Oscilloscope: This device allows the user to see, monitor, and measure signals. The team used this device prior to acquiring the Moku:Go. This device was the team's primary means of monitoring and measuring signals.

5) Nooelec HackRF One Software Defined Radio: The HackRF One is a device that is mostly used to detect signals, but it also has additional functionalities such as analyzing and even demodulating. Our teams attempted to use the device to demodulate but found that demodulating Qi was too complex for the HackRF One's functions.

6) AVID Technologies, Inc Qi Sniffer V1.2: The Qi Sniffer is a device that is made to detect a signal sent between a wireless charger and phone. It can detect the communication

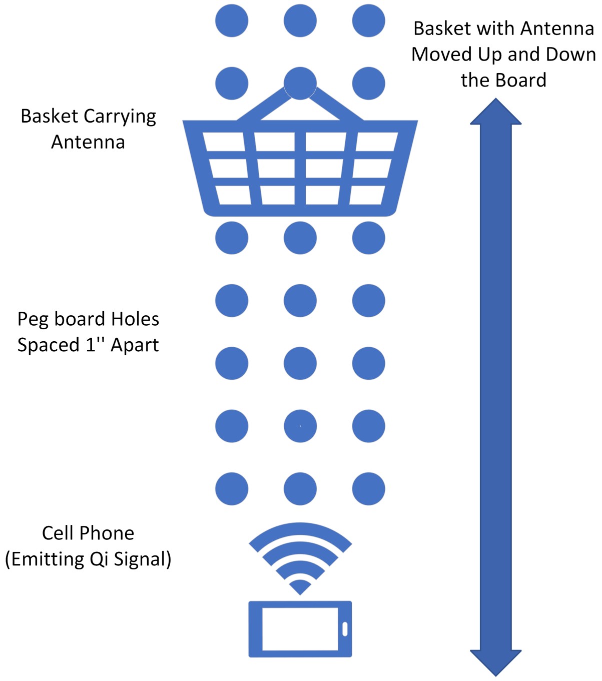

Fig. 4: Experiment design of Qi Distance Experiment

frequency, power level, and certain bits of information from the phone itself. Our team used this device mostly to detect the frequency a phone and charger were communicating with, and the power levels sent from the charger to the phone.

7) 5Pcs Magnetic Field Probes Set EMI EMC Near Field Probe: Only 2 probes are listed here, as they were the only ones we used. These are basic probes used to detect signals in conjunction with the Moku:Go. They were also used during our team's distance and speed tests.

8) Magnetic Field Probes: These devices both have different frequency ranges but operate the same. The yellow antenna has a range of 3-300kHz, while the pink antenna has a range from 100kHz-20MHz. They are probes that are made to detect radio waves and were used in conjunction with the Moku:Go. They were also used in the team's distance and speed tests.

C. Experiment Set-Up

In order to achieve the desired results of this experiment, the team prototyped a few different contraptions in order to measure both distance and speed from which a Qi signal could still be detected. The team decided to focus efforts on the distance experiment first and eventually landed on a set-up that allowed for an antenna to be fastened to a wire shelf. This wire shelf was attached to a peg board that allowed for hooks to be moved one inch at a time up and down the peg board and moved the antenna different distances away from a charging phone that was located below the fastened antenna. The phone was placed on top of the charger and was not moved throughout the entirety of the experiment, this was because if the phone was taken off then a new handshake would be initiated and potentially affect the power output even if the affect would be minuscule.

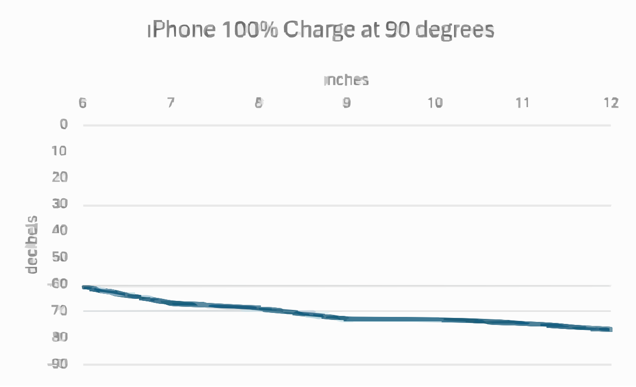

Fig. 5: Graph

D. Challenges and Limitations

Most of the difficulties encountered in our research were directly demodulating the Qi signals. We were able to collect voltage signals from an oscilloscope and the magnetic signal from the probe. We could not identify the details in communication packets without a demodulation capability. We attempted to use the Moku, a HackRF, and a Nooelec SDR to create a demodulation process in our workflow but were unsuccessful. We have looked at other research that describes demodulation but not the hardware or configurations they used. We recommend that manufacturers offer probe-friendly boards with their products so we could have access to the onboard circuits, which include analog-to-digital and digital-to-analog converters, as well as the steps in between. This would overcome the limitations of non-RF security research that approaches wireless domains.

If we could demodulate the signal, we could access the key information within the packets. This would greatly impact man-in-the-middle attack vectors via the wireless path. We also could validate that the signal we receive at a distance contains the information per the spec. Being able to affect transmissions in real-time offers a signals intelligence angle and a stronger indication of cyber attack potential.

V. Findings

Through incremental exploration and experimentation, we have uncovered multiple findings.

1) The demodulation is critical for any specific RF based attack. Last years research team was able to inject noise into the Qi protocol, disrupting charge, but not as they intended. Without a demodulation capability, we were unable to man in the middle anything or even evaluate possible attacks via that concept.

2) The Qi protocol, as seen through Pulse View, is not consistently decoded. This could be due to noise, software bugs, hardware bugs, or measurement tool error. We were

unable to isolate without the ability to demodulate. An RF assurance assumption is too bold.

3) Qi Charger antenna pattern was different than expected. The ”donut” was lopsided.

4) Distance and speed between the charger and phone were not forgiving enough to allow movement.

A. Distance and Angle

Considering the simplistic resources used in accomplishing this conveyor belt experiment, it was a significant success in identifying the Qi signal from up to 14 inches away. Assuming stronger antennas, larger antennas, and better noise elimination software, there is much room to scale this concept for real-world applications involving secure areas.

This experiment was meant to test how far away the communication signal between the phone and charger could be detected and how the angle affected the signal reception. The signal could be accurately recognized from 30.5 cm (12 in) away from the 3KHz-300KHz magnetic probe when directly above the device, perpendicular to the phone. We then tested using the probe at a 45° angle to the phone, from 15.24 cm (6 in) and 30.5 cm (12 in) away. We found that the signal was stronger at 45° angle than the signal perpendicular at a distance of 15.24 cm (6 in), meaning the signal can likely be detected from an even greater range than directly above the phone. We plan to expand our testing of the limits but meet our hypothesis of Qi protocol communication detection at a distance of up to 30.5 cm (12 in).

B. Identification

For this experiment, we attempted to see how much information we could gather from a phone that is powered off but still charging. The only tests that we are currently able to check for this are charge levels and the Qi sniffer. When the phone is powered off, the information that can be found is the exact same as when the phone is on or just asleep, and the charge levels are the same as when the phone is asleep.

Observation and Recognition - We also tested the signal strength when the phone was powered on and off at different power levels. We discovered that the Qi Sniffer displays the exact same amount of information when the phone is either powered on, powered off, or the phone screen is active or off, meaning that even a dead phone on a Qi charger can leak the same information and be detected once paired to a charger.

C. Speed

One limitation of our research was the inability to effectively measure the speed at which a Qi-enabled device could be detected while in motion. Our initial goal was to test how quickly a phone could be detected as it moved across a simulated security screening setup, such as a conveyor belt or mantrap. However, we could not implement a controlled experiment to accurately measure this speed due to lacking a motor system with fine enough speed controls.

Without the ability to maintain a constant, measurable speed of the device passing over the Qi charger, we could not reliably determine the minimum time required for detection. This parameter is crucial for understanding the practical application of Qi signal detection in real-world security scenarios, where individuals may be quickly passing through a monitored area.

VI. Future Work

In order to expand this experiment, the implementation of consistent Geometry orientation and a switch from M/H field to E field could improve results. In addition

- M/H field to E field for increased distance
- Geometry to account for poor orientation
- Vertical Man Trap implementation
- Demodulation for decoding identifications
- Phased Array Magnetic Antenna for beam steering

In addition to additional distance measurements, we plan to test how quickly the phone and charger can connect when the phone is constantly moving or stops for a short time. This goal is a proof-of-concept for device detection, imitating a person walking through a mantrap or walk-through detector equipped with a Qi-detecting device or across a security screening conveyor belt. We continue working toward successfully demodulating Qi signals to access dynamic information, including the Qi ID as a form of information leakage that can be used for tracking.

We can consider additional threat attacks with real-time demodulation, but the distance enables varying delivery options. At a low frequency in the 100-200 KHz range, we could utilize advanced antenna designs, including phased arrays, to increase the sensing ranges. With the right transmission capability, we could trigger devices to broadcast their Qi responses, even when devices are turned off. We believe more potential vulnerabilities need additional countermeasures when the demodulated signals are accessed.

We need increased user awareness and potential new mitigation strategies to address the security and privacy risks highlighted by our research. The Wireless Power Consortium is addressing issues we discuss, but users are unaware of the potential security problems similar to using public WiFi or USB chargers at conferences.

Outline specific areas for future research, such as developing more robust Qi signal demodulation techniques, exploring additional attack vectors, and investigating countermeasures.

Ultimately, devices with Qi charging have no control over their Qi hardware, enabling an attack vector they cannot disable or control.

VII. Conclusion

Our research has revealed significant security and privacy risks associated with the widespread adoption of Qi wireless charging technology. We have demonstrated the ability to detect Qi signals at distances far exceeding the protocol’s specification, even when the charging device is powered off. This extended detection range enables potential adversaries to eavesdrop, hijack, and interfere with the wireless charging process.

Our analysis of the Qi communications has uncovered the leakage of unique device identifiers, which can be leveraged for tracking and profiling user behavior. Despite the challenges faced in directly demodulating the Qi signals, this capability is crucial for deeper protocol inspection and developing more sophisticated dynamic attacks.

The accessibility of the required equipment, costing less than $2,500, underscores the need to increase user awareness of these vulnerabilities. As the Qi wireless charging technology continues to proliferate, it is imperative that the Wireless Power Consortium and device manufacturers address these security and privacy concerns through robust countermeasures and improved user control over Qi hardware.

Future research should focus on developing more reliable Qi signal demodulation techniques, exploring additional attack vectors, and investigating effective mitigation strategies. By addressing these issues, the benefits of wireless charging can be realized without exposing users to unacceptable risks. Ultimately, this work aims to enhance the security and privacy of Qi-enabled devices, empowering users and fostering a more secure wireless charging ecosystem.

Acknowledgment

The authors would like to thank Lt Col Neil Rogers, Lt Col David Hancock, Dr. Steven Fulton, Mr. Delbert Christman, Dr. Carlos Salazar, and Mr. Robin Wright.

References

[1] Y. Wu, Z. Li, N. Van Nostrand, and J. Liu, “Time to Rethink the Design of Qi Standard? Security and Privacy Vulnerability Analysis of Qi Wireless Charging,” in *Annual Computer Security Applications Conference*. Virtual Event USA: ACM, Dec. 2021, pp. 916–929. [Online]. Available: https://dl.acm.org/doi/10.1145/3485832.3485839

[2] D. Yang, G. Xing, J. Huang, X. Chang, and X. Jiang, “QID: Robust Mobile Device Recognition via a Multi-Coil Qi-Wireless Charging System,” *ACM Transactions on Internet of Things*, vol. 3, no. 2, pp. 1–27, May 2022. [Online]. Available: https://dl.acm.org/doi/10.1145/3498904

[3] X. Gao, “Demodulating communication signals of qi-compliant low-power wireless charger using mc56f8006 dsc,” *NXP Freescale Semiconductor Application Note, Document No. AN4701, Rev. 0*, 2013.

[4] Y. Qu, W. Shu, Y.-C. Kuan, S.-H. W. Chiang, Y. Li, Z. Zheng, and J. S. Chang, “A 12-W 96.1%-Efficiency eFuse-Based Ultrafast Battery Charger Supporting Wireless and USB Power Inputs,” in *2021 IEEE Custom Integrated Circuits Conference (CICC)*. Austin, TX, USA: IEEE, Apr. 2021, pp. 1–2. [Online]. Available: https://ieeexplore.ieee.org/document/9431525/