MAKING A LOW-COST SOFTWARE-DEFINED UHF RFID READER

A PREPRINT

Edward A. Keehr
Superlative Semiconductor LLC
Carlsbad, CA 92009, USA
keehr@super-semi.com

Gregor Lasser
University of Colorado, Boulder
1111 Engineering Dr.
425 UCB, EE 1B55
gregor.lasser@colorado.edu

January 30, 2021

1 Introduction

1.1 Overview

In this article, we discuss how one can make, with modern and low-cost tools, a software-defined UHF RFID reader. Since we have chosen to leave discussion of the top-level reader implementation until the very end, an introductory outline is warranted in order to help guide our audience. We will first provide the uninitiated with some background context by answering the questions: "What is UHF RFID?", "How does it work?", "What happened with UHF RFID?", and finally, "What's next?"; i.e., how do we as the authors envision it evolving in the future with the support of a broad community? Secondly, we describe the fundamental metrics and performance budgeting of RFID readers. Following this, we provide an overview on how to design, make, and automatically tune two critical components of UHF RFID readers: the antenna and transmit leakage canceller. Thirdly, we delve even further into details of the transmit leakage canceller in its own section. Finally, we describe the complete high-level architecture of a proposed low-cost reader.

1.2 What is UHF RFID?

To put it briefly, Ultra-High-Frequency Radio-Frequency Identification (UHF RFID) is a technology in which one can affix a *tag*, often with adhesive backing, to an object, and obtain information from the tag at a distance using a *reader* device with an integrated radio. The tag contains an embedded antenna and a very small microchip which conducts a simple communications protocol with the reader, as depicted in Fig. 1. Tags often also harvest RF energy to power themselves, usually from the reader's radio transmission, and are commonly about the size of a medium-sized adhesive bandage. The maximum range between reader and tag in free space depends on the reader antenna directivity, reader quality, and tag quality, but typically varies from about 2 to 20 meters. As per the dominant EPC Gen 2 specification [1], the most common information to be found on the UHF RFID tag is its electronic product code, or EPC. The EPC functions as a wireless bar code that can in principle be used to uniquely identify the object to which the tag is attached. In addition to the EPC, special tags have been developed that can sense the temperature [2] of the object to which they are affixed, moisture level [3] in a given area, and other environmental parameters, and report that information back to the reader.

1.3 How UHF RFID Works: Backscatter

Of greatest interest are batteryless passive UHF RFID tags due to their minimal cost (≈\$0.05-\$0.10 in bulk) and lack of maintenance requirement. Such tags communicate back to the reader using a low-power technique known as *backscatter*. Backscatter eschews the power and complexity of a full radio transmit chain to send data. Rather, a device communicating with backscatter sends data back to a radio receiver by changing the termination on an antenna when incident radio frequency (RF) power is present, usually with a switch that shorts out the antenna terminals, as depicted in Fig. 2. As the antenna termination changes, its scattering coefficient changes. The portion of the incident signal

1527-3342 ©2021 IEEE. Digital Object Identifier 10.1109/MMM.2020.3042046.

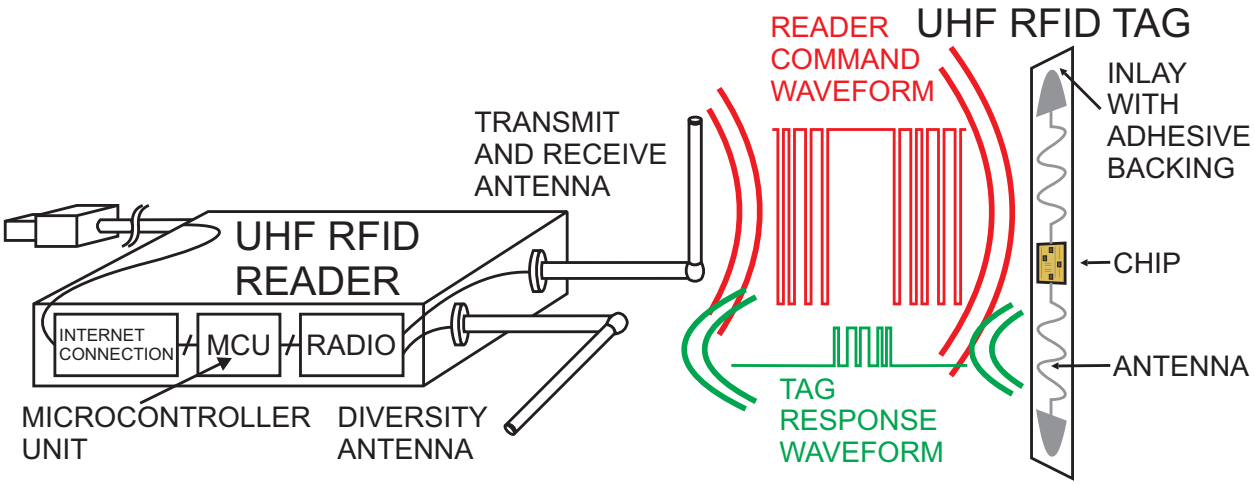


Figure 1: RFID physical layer concept.

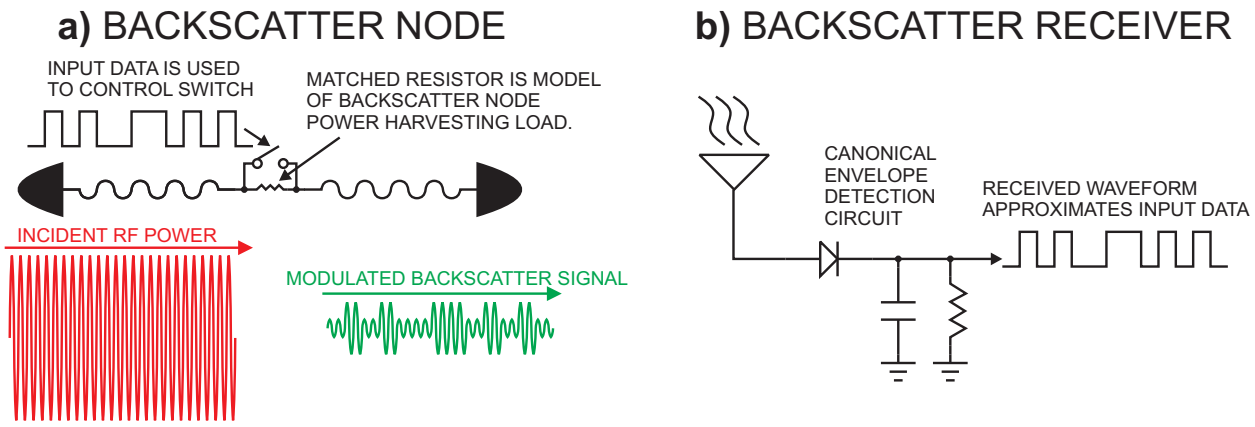


Figure 2: Backscatter concept, with On-Off Keying as an exemplary modulation scheme. a) A backscatter node, depicted as an RFID tag, reflects incident RF power differently based on whether a switch across the antenna load is closed or open. b) A backscatter receiver, depicted as a canonical diode-based envelope detection circuit, rectifies the incoming RF signal and filters out the high-frequency components, leaving a representation of the original input data to be recovered.

reflecting off the antenna is now modulated along with the changes in the antenna termination. A reader can then receive this modulated signal and decode the encapsulated information. In EPC Gen 2, the modulation frequency is known as the backscatter link frequency (BLF), and it ranges from 40 to $640\,\mathrm{kHz}$ on top of a carrier frequency ranging from 860 to $960\,\mathrm{MHz}$. For backscatter to work, there must be a transmitter somewhere sending out a (usually $0.5\,\mathrm{W}$–$2\,\mathrm{W}$) signal for the backscatter device to reflect. This transmitter may or may not be co-located with a receiving terminal. Typically, the tag powers itself from energy harvested during the switching intervals in which the switch is open and the antenna is loaded by an impedance-matched internal RF-to- direct current (DC) power conversion circuit. One can think of backscatter as similar to communicating with a mirror or shiny object to send Morse code by reflecting the sun or a searchlight while camping or hiking. You might have forgotten a radio or have run out of batteries on your excursion, but with a simple mirror, you can leverage power generated elsewhere to effect a meaningful long-distance communication scheme.

Backscatter communications have garnered increasing attention during the 21st century due to their extremely low power usage. In fact, one could conceivably attach a batteryless, passively-powered backscatter radio to everything and connect it to the internet. At that point, one would have what one could term an “Internet of Things”. In all seriousness, however, the ubiquity of the phrase “Internet of Things” underscores the myriad of applications lying latent and untapped in the public’s imagination that could be realized by backscatter radios. And UHF RFID is a remarkably lightweight implementation of a backscatter radio system. So why don’t we see it everywhere?

1.4 The Promise of UHF RFID - What Happened?

In fact, when UHF RFID hit the scene around the year 2000, people *did* expect to see UHF RFID everywhere. The internet had just succeeded in connecting pretty much every human being living in the developed world, and the next logical step in technology development was to connect every *object* to the internet. Major publications expected UHF RFID to be ubiquitous in the coming years [4–6]. Notably, Wal-Mart issued an edict that its top suppliers were to use RFID technology to track and inventory their shipments [7]. Tech pundits were so concerned about the impact that RFID would have on our everyday lives that some called for an RFID Bill of Rights [8] and saw in RFID a harbinger of the end times [9].

But that's not what happened.

Wal-Mart eventually bailed on their UHF RFID initiative due to supplier unhappiness with the added costs and technical problems with the then-new technology [7]. Competing technologies made inroads to markets thought suitable to RFID. In the past, major grocery store chains had studied UHF RFID but concluded that the overall cost of the required infrastructure was too expensive [10]. Today, Amazon is pioneering computer vision for retail grocery and it appears as of now to be the correct solution for that market [11]. Bluetooth, and especially Bluetooth Low Energy (BTLE), has become a consumer-market "good enough" IoT enabler because it comes installed on all smartphones. Due to its relatively high minimum peripheral cost on the order of $10, BTLE isn't the internet of everything, but it still covers a fair amount of stuff. Sure, UHF RFID has found niche applications in automotive tolling and high-end apparel retail [12], but it's not in general something that one commonly sees going about their daily life.

1.5 What's Next?

So it should be clear that UHF RFID, or some similar lightweight backscatter technology, is valuable for truly realizing the Internet of Things. But it hasn't found its killer app yet. That's OK. Even the bar code itself took 20 years from its original patent filing to be used and another 20 years after that to become ubiquitous [13]. Twenty to 40 years is a long time to wait, however. It seems archaic to sit back and wait for a someone in a large corporation to come up with a workable vision for RFID, convince management to spend lots of money on it, and then successfully bring it to market.

What if instead - we could all hunt for the killer app of UHF RFID together - on the cheap! This is not so easy; dreaming up such an app is only a small fraction of the battle. Building the custom prototype best suited to capitalizing on that app is the first major step to proving out the idea and attracting outside investment.

It turns out that the tools of the maker movement allow us to do this, namely, to build hardware prototypes for a nominal price [14], including those of UHF RFID readers and tags. Cheap design software such as Kicad, Eclipse, and lite versions of field-programmable gate array (FPGA) development software allow anyone with a computer and access to the internet to design feature-rich customer electronics for free! Printed-circuit board (PCB) fabrication can be accomplished for a few hundred dollars or less using any one of a number of push-button services. PCB assembly can take place with a $40 toaster oven and a $150 Reflowster, itself a product of the maker movement. Access to cheap metalworking tools at Maker Spaces permit the low-cost manufacture of complex metal geometries [15], including potentially those of novel UHF RFID antennas. Finally, digital sharing and modification of open-source design files allow us to all go on the hunt for the killer app *together*.

Open source projects already exist for UHF RFID. The Wireless Identification Sensing Platform (WISP) project is an implementation of a software-defined UHF RFID tag [16] made up of discrete components, but is only a bit larger than a typical UHF RFID tag. A somewhat larger, but easier to assemble, software-defined tag, was also recently described [17]. Note that the software-defined aspect of the project is important. When most of the complex design functionality is present in software, either in the microcontroller unit (MCU), FPGA, or both, it becomes much easier for someone holding the hardware to implement and test major changes to the design. It can be done instantaneously, without reinventing the entire project, for free! There are implementations of software-defined UHF RFID readers too, but to the knowledge of these authors, the ones that are open-sourced and publicly available are high cost, being implemented on thousand-dollar-and-up Ettus Universal Software Radio Peripheral (USRP) platforms such as [18] and [19]. An extensive list of UHF RFID readers based around software-defined radios (SDRs) that have appeared in the academic literature and have provided enough information to compute approximate cost is shown in Table 1.

Therefore, there exists a need for the final tools of the hunt for the killer app of UHF RFID: a low cost software-defined UHF RFID reader, and matching low cost, high performance antennas suitable for a variety of application scenarios. These tools will be the topic of the remainder of this article.

Table 1: Summary of prior art in SDR/FPGA - based UHF RFID readers. [20]

References	Key Components	SDR Bill of Materials (BOM) Cost	# FPGA Logic Elements	Range	Output Power	Comments
[21]	Assorted Linear Technologies components. Xilinx Virtex 4 FPGA.	$>$ \$235	$>$ 13824	Not reported	Not reported	No measured results reported.
[22]	Stratix II EP2S60 FPGA. Big MCU PCB. Big radio PCBs.	$>$\$874	60440	6m	Not reported	Only receive digital described. Antenna type unclear.
[23] [24] [25]	Various RF parts. Xilinx Virtex II FPGA. TI TMS320C6416 Digital signal processor.	$>$ \$500	Up to 93184	11m (in hall)	35dBm	Modular, Mono- and Bistatic. 5dBi antenna.
[26] [27] [28]	USRP1 Radio platform. EP1C12Q240C8 FPGA. RFX900 x1/x2 card.	$>$\$970	12060	Up to 6-7m [26] [27]	27dBm [26]	Bistatic. 8dBic antennas [26].
[29] [30]	Various RF parts. Virtex 4 LX100 FPGA. S3C2410 MCU.	$>$\$2500	$>$110592	8-9m	30dBm	Antenna gain or type not reported.
[31]	TH72035 Transmitter. MAX931 Comparator. MSP430F5510 MCU.	$>$\$9	N/A (MCU)	0.15m	9dBm	Monostatic. Dipole antenna (1-2dBi). Not fully tested.
[32]	AS3992 RF front end. XC3S500 FPGA.	\$73.55	10476	3.5m	N/A	Receiver only. "Loop antenna".
[33]	USRP N200 Radio platform. Spartan-3A 1800 FPGA. Wideband radio (SBX) card.	$>$\$2203	$>$37440	Not reported	17.8dBm	Bistatic. 7dBic antennas.
[34] [35]	USRP-2922 Radio platform. Spartan-3A 3400 FPGA. Wideband radio (SBX) card.	$>$\$3092	$>$53714	"Same as AS3992 Eval. Board"	Not reported	Monostatic.
[36]	USRP-2942 Radio platform. Kintex 7 410T FPGA.	$>$\$7373	$>$406000	$>$2.35m	Not reported	Bistatic.
[37]	F28377D MCU. ADF4360-3(?) Phase locked loop. LT5516 Demodulator(?).	$>$\$40	N/A (MCU)	Not reported	Not reported	Physically large. Manual leakage cancellation. Only implements Query=0 transaction.
Proposed in Section 4 of this article [20]	SX1257 SDR. MAX 10M02 FPGA. 2x PE64102, 2x PE64906. NRF51822QFAA MCU.	\$11.71	2304	2.6m (dipole) 15.2m (patch)	26dBm	Monostatic. Dipole (1.2dBi) and patch (12.5dBi) antennas measured. 64cm^2 PCB area.

2 RFID Reader Fundamentals and Hardware Challenges

Passive RFID poses several challenges on the reader architecture, since it is a highly asymmetrical communication scheme where the "intelligence" of the system is concentrated in the reader, to allow for simple and cheap tags. In particular, they are different from conventional radio systems in two ways:

- Backscatter communications is used
- Tag power supply is provided by reader

Both points greatly affect the front end hardware of a reader. Backscatter communication necessitates that the reader transmit (TX) and receive (RX) paths are active simultaneously, and the TX signal must be strong enough to power the tag. RFID readers therefore face similar challenges as full-duplex or simultaneous transmit and receive (STAR) systems [38]. To separate the TX and RX paths, one of the antenna access topologies shown in Fig. 3 can be used. Each of these three topologies suffers from some transmit to receive leakage. Even if one or more of the antenna access topologies could be made perfect, scattering from nearby objects additionally creates unavoidable leakage. A monostatic reader topology uses a single antenna for transmit and receive. A circulator or directional coupler is used to separate the transmit and receive paths. Here, the intrinsic transmit to receive isolation IS, i.e. how much power leaks from the transmitter into the receiver, is determined by the antenna return loss and the isolation or directivity of the circulator or directional coupler. A bistatic reader topology (Fig. 3b) uses two separate antennas to achieve isolation. The leakage is primarily determined by the antenna patterns and the antenna spacing. The third topology uses a single dual-port antenna, where the antenna itself provides isolation. It is true for all scenarios that the intrinsic isolation provided by the antennas and the circulator typically is too small. Some form of analog transmit leakage cancellation is required [39], to avoid blocking in the receiver low noise amplifier or analog to digital converter.

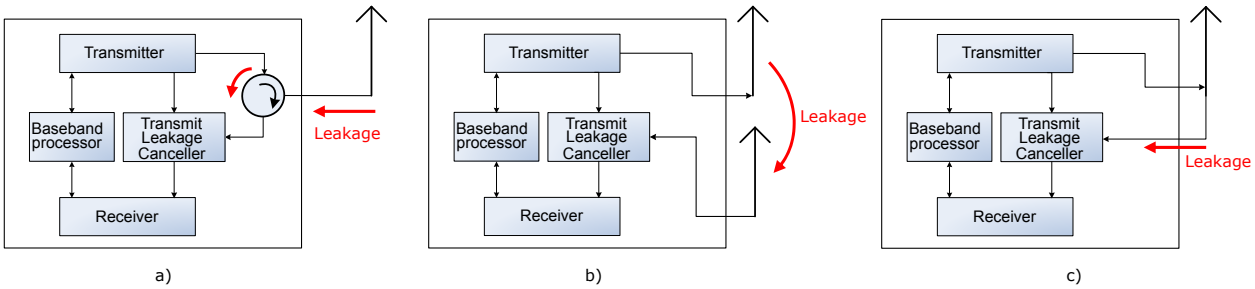


Figure 3: RFID reader access topologies and leakage: monostatic (a), bistatic (b), monostatic with dual-port antenna (c).

The fact that the tags do not have their own power supply but instead harvest the radiation produced by the readers sets a limit on the read range. This is typically called forward read limit and is determined by the ability to "wake up" tags with the readers transmit signal [40–43]. Therefore high transmit powers in the order of 0.5 - $2\,\mathrm{W}$ are common ($1\,\mathrm{W}$ is allowed in the USA, using an antenna with up to $6\,\mathrm{dBi}$ [44]).

2.1 Receiver Noise

Successful communications with a tag requires two things: The power at the tag needs to be large enough to wake it up, and the signal to noise ratio (SNR) of the backscattered signal must be sufficient for decoding the data stream by the reader. The second condition, often called back link limitation, is mainly determined by the noise present in the reader. While some of it is thermal noise, there is an additional component related to the carrier signal leaking from the transmitter [45–47]. Any noise or phase noise of the leaking transmit signal will directly end up in the receiver; additionally, the phase noise of the receiver's local oscillator (LO) due to reciprocal mixing with the leaking carrier also contributes to noise in the receive band [48, 49]. In both cases, the received spectrum at the receiver baseband looks similar to Fig. 4: In the center, we note the strong leakage signal, with noise sidebands and a flat noise floor, that adds to the backscattered signal from the tag which is centered around the BLF. The total noise introduced into the receiver $P_{\mathrm{N,TX}}$ due to thermal transmit noise, phase noise of the transmit signal, and reciprocally mixed LO noise with the transmit carrier can be modelled as a transmit SNR SNR_{TX} of the reader's transmitter. Since the effective transmit noise spectrum is not flat, SNR_{TX} will depend on the BLF. The noise power in the reader's receiver can then be expressed as:

$$P_{\mathrm{N}} = N_{\mathrm{th}}F + \frac{P_{\mathrm{N,TX}}(BLF)}{IS \cdot G_{\mathrm{I}}} = N_{\mathrm{th}}F + \frac{P_{\mathrm{TX}}}{SNR_{\mathrm{TX}}(BLF)IS \cdot G_{\mathrm{I}}} = N_{\mathrm{th}}F + \frac{P_{\mathrm{TX}}}{FOM_{\mathrm{R}}(BLF)IS}, \tag{1}$$

where N_{th} is the thermal noise power, F is the noise figure of the receiver, P_{TX} is the transmit power of the reader, IS is the intrinsic isolation between transmitter and receiver, and G_{I} is the isolation gain of the leakage cancellation circuit, i.e. the ratio of initial leakage power to the leakage power when using the leakage canceller. The product of transmit SNR and isolation gain is a reader quality parameter summarized as FOM_{R}. The achieved isolation gain will in practice depend on the leakage amplitude and phase, but here is considered constant for simplicity. We further omit the dependency on the backscatter link frequency in further equations for brevity. The first term in (1) is the thermal noise, the second term is the noise due to the leaking carrier. When this latter term dominates, the SNR at the receiver is given by: [47]

$$SNR_{\mathrm{RX_{SI}}} = \frac{FOM_{\mathrm{R}}FOM_{\mathrm{Ant}}G_{\mathrm{Tag}}^2\eta_{\mathrm{Mod}}}{FSPL^2}, \tag{2}$$

where G_{Tag} is the gain of the tag antenna, η_{Mod} is the modulation efficiency of the tag, and $FSPL$ is the free space loss. The two figure of merits FOM_{R} and FOM_{Ant} are explained in Fig. 5 and motivated from a bistatic or dual-port antenna reader scenario where the intrinsic isolation IS is determined by the antennas and their placement. For high performance monostatic readers with a good circulator, the intrinsic isolation remains antenna-dominated when the antenna return loss is lower than the circulator isolation (see Fig. 3).

To demonstrate that the self-interference noise often dominates and (2) sets the reader SNR, we investigate the monostatic low-cost reader discussed in Section 4, with the relevant parameters of this reader and the assumed Monza 5 based tag [50] – summarized in Table 2. Using the Friis transmission equation for forward and backward links, and the receiver noise from (1), we compute the maximum possible read range

$$d_{\mathrm{max,rv}} = \frac{\lambda}{4\pi}\sqrt[4]{\frac{EIRPG_{\mathrm{RX}}FOM_{\mathrm{R}}FOM_{\mathrm{Ant}}G_{\mathrm{Tag}}^2\eta_{\mathrm{Mod}}}{SNR_{\mathrm{RX_{min}}}\left(EIRPG_{\mathrm{RX}} + N_{\mathrm{th}}FFOM_{\mathrm{R}}FOM_{\mathrm{Ant}}\right)}}, \tag{3}$$

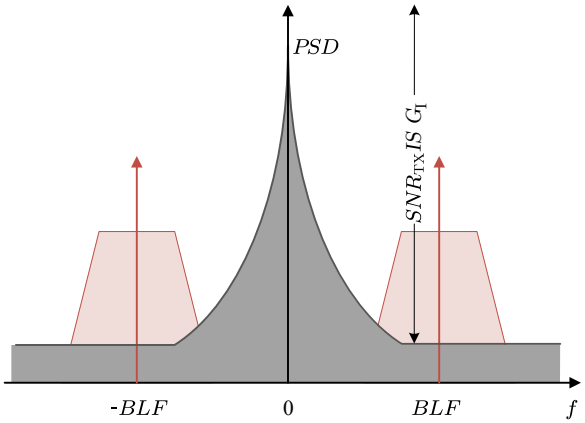


Figure 4: Power spectral density of RFID reader received baseband signals. The dominating leaking transmitter noise components are in grey, the backscatter signal is drawn in red. Source: Modified from [47, Fig. 3]

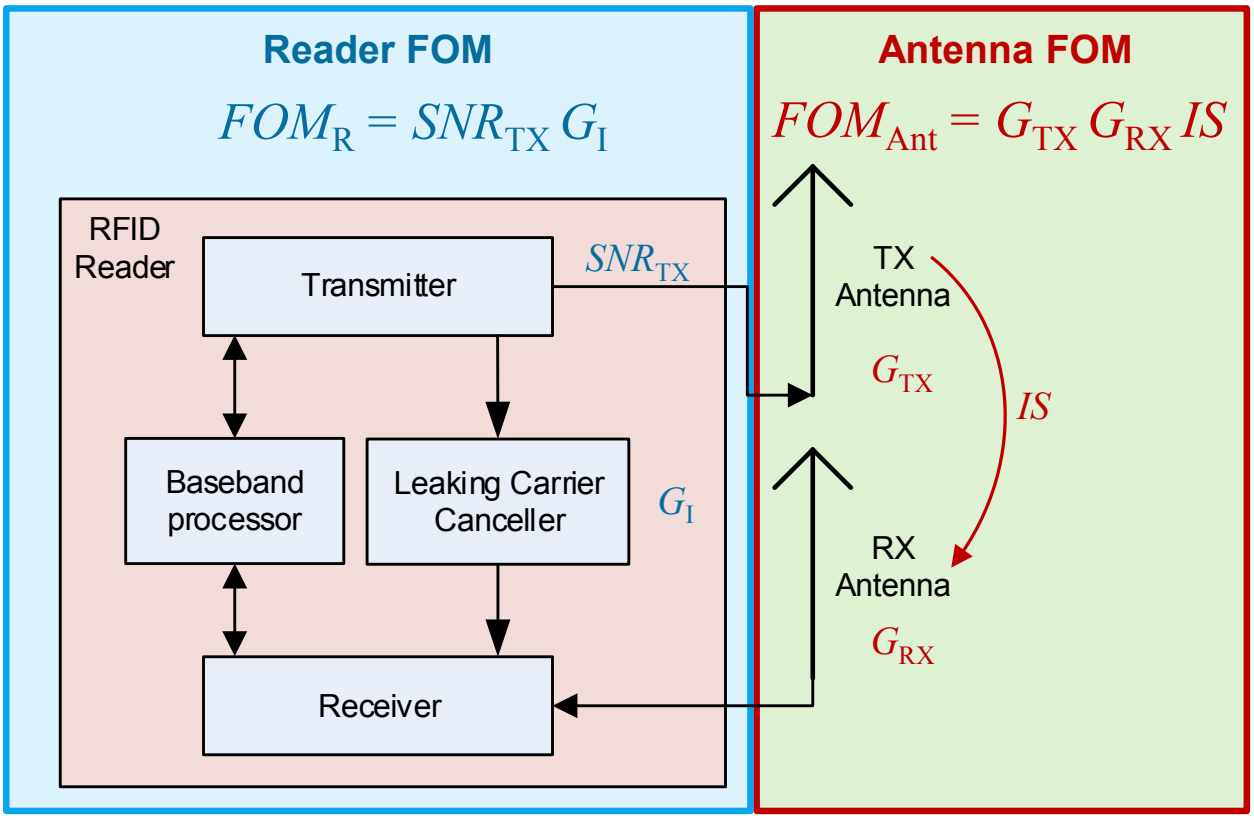


Figure 5: Definition of the figure of merits (FOMs) for the example of a bistatic reader.

Table 2: Tag and reader parameters

Sensitivity $P_{\mathrm{Tag}_{\mathrm{min}}}$	-17.8	dBm
Antenna Gain G_{Tag}	1	dB
Modulation Efficiency η_{Mod}	-10	dB
Frequency f	915	MHz
Bandwidth B	90	kHz
Noise Figure F	26	dB
Transmit Power P_{TX}	26	dBm
Reader FOM FOM_{R}	96	dB
Required SNR $SNR_{\mathrm{RX}_{\mathrm{min}}}$	7	dB

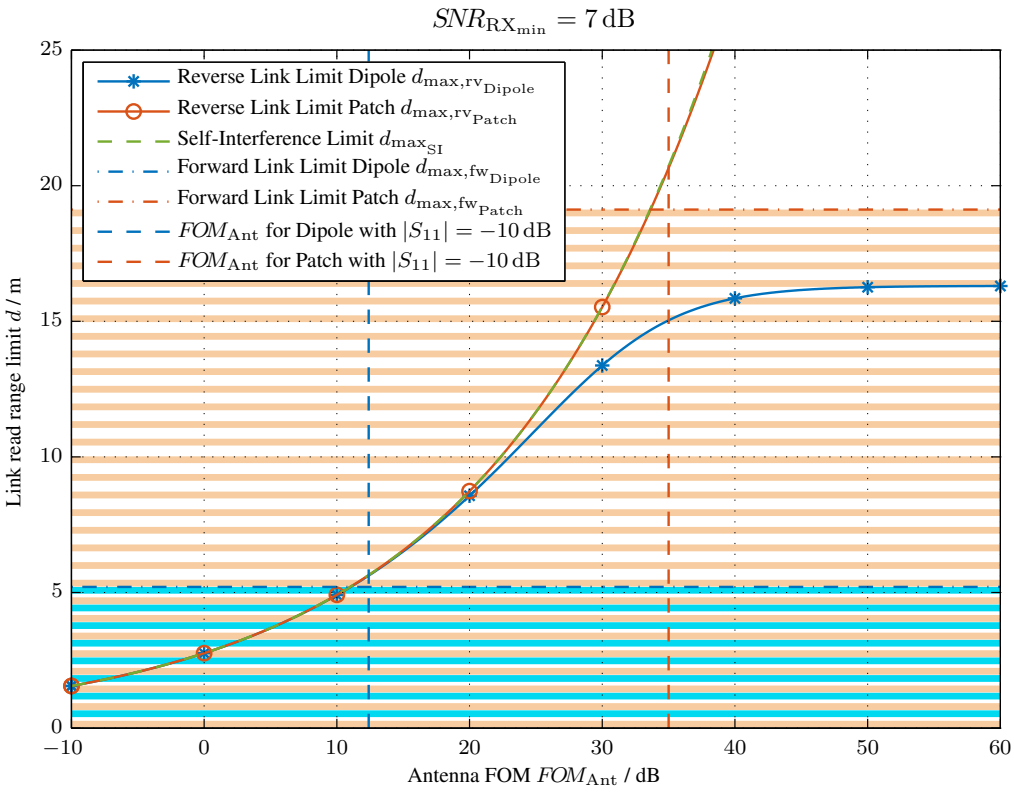


Figure 6: Read range limit d for the presented reader (Table 2) for a dipole and a patch reader antenna. The dipole has a gain of 1.2 dBi, the patch antenna has 12.5 dBi. The antenna FOMs $FOM_{\mathrm{Ant}} = G_{\mathrm{TRX}}^2 IS$ for a return loss of 10 dB are indicated by vertical lines for the dipole and the patch antennas. The hatched areas indicate feasible operation due to forward link limits $d_{\mathrm{max,fw}}$ based on a transmit power of $P_{\mathrm{TX}} = 26\,\mathrm{dBm}$.

where λ is the free space wavelength, $SNR_{\mathrm{RX_{min}}}$ is the minimum SNR required by the reader to decode the backscattered signal, and $EIRP$ is the equivalent isotropically radiated power from the reader's transmitter. From the power received at the tag [47, (1)] the forward link limitation, i.e. the maximum distance for which the tag responds is found

$$d_{\mathrm{max,fw}} = \frac{\lambda}{4\pi}\sqrt{\frac{EIRP G_{\mathrm{Tag}}}{P_{\mathrm{Tag_{min}}}}}. \tag{4}$$

These limits are plotted in Fig. 6 for two different reader antennas. Additionally, we plot the self-interference link limit [47, (10)] which can be computed from (2)

$$d_{\mathrm{max_{SI}}} = \frac{\lambda}{4\pi}\sqrt[4]{\frac{FOM_{\mathrm{R}} FOM_{\mathrm{Ant}} G_{\mathrm{Tag}}^2 \eta_{\mathrm{Mod}}}{SNR_{\mathrm{RX_{min}}}}}. \tag{5}$$

Assuming fixed gain antennas, the remaining free parameter for adjusting FOM_{ANT} is the isolation IS between the antennas. We see that up to a value of $FOM_{\mathrm{ANT}} = 20\,\mathrm{dB}$, both antennas behave the same and would result in a read range of $8.6\,\mathrm{m}$. For higher FOMs and the low gain dipole antenna, the relatively low $EIRP = 27.2\,\mathrm{dBm}$ causes the read range to flatten out at $16.3\,\mathrm{m}$ due to thermal noise. However, the forward link limitation (powering the tag) for this case is $5.2\,\mathrm{m}$, so that the thermal noise limited case cannot be reached. Similarly, for the high gain patch antenna, the theoretical forward read range limit is $19.1\,\mathrm{m}$ requiring an antenna FOM of $FOM_{\mathrm{Ant}} = 33.6\,\mathrm{dB}$. This point is still dominated by the self interference limit $d_{\mathrm{max_{SI}}}$. From the gain of the patch antenna of $12.5\,\mathrm{dBi}$, we can compute the required return loss for this FOM to be $8.6\,\mathrm{dB}$, which is easily achieved by a high quality antenna. To be forward link limited, the dipole antenna needs to have a return loss of $8.6\,\mathrm{dB}$, which is not always achieved in a realistic scenario where the dipole antenna is directly connected to the reader and influenced by nearby objects. In a practical environment, multipath propagation will also cause fading and range correlation effects of the noise [49, 51]. Assuming a return loss of $10\,\mathrm{dB}$ for both antennas, we see that this scenario is forward link limited. Using a tag with higher sensitivity (e.g. NXP's Ucode7 [52]) raises the forward link limit lines in Fig. 6 and results in a reverse-link limited scenario.

We conclude that to achieve forward link limitation, a reader setup must have high reader and antenna FOMs. Those conditions boil down to

- The reader must have low transmit (phase) noise and a clean RX local oscillator
- A leakage canceller with an isolation gain of at least $50\,\mathrm{dB}$
- Well matched, high gain reader antennas
- The reader antenna vicinity needs to be free of scattering objects

2.2 Reader Antennas

Depending on the reader access topology (Fig. 3), different antenna solutions are feasible. The monostatic configuration in principle sets a single requirement on the used reader antenna: Providing a high return loss ensures a large transmit to receive isolation IS, and therefore a large FOM_{Ant} assuming a perfect circulator, even for moderate antenna gains. This in principle allows for simple dipole based antennas; however, circular polarization (CP) is preferred in a typical scenario where the tag orientation is unknown. Another way to mitigate this problem is to use two cross-polarized antennas and switch between them to be able to read randomly positioned, linear polarized tags. Circular polarization has another big benefit for RFID readers: The scattering from large metallic objects will be flipped in polarization. An object illuminated by a right-hand circularly polarized (RHCP) antenna will scatter left-hand CP fields, which are not received by the RHCP antenna. This reduces the total leakage signal and can mitigate range correlation effects and increased receiver noise. Most tags use linearly polarized antennas so their backscattered signals are linearly polarized as well, causing a $6\,\mathrm{dB}$ penalty for CP reader antennas on the reverse link that is independent of the tag orientation. Further, any reader antenna gain improves the antenna FOM (Fig. 5) and therefore the reverse-link read range.

For bistatic readers, the antenna return loss is less of an issue, because the isolation is now defined by the antenna patterns and orientation. This makes the performance of this configuration highly dependent on the exact geometry and the used antennas [51], which is a drawback in many applications where the end user is not skilled in radio propagation.

2.2.1 Dual-Port Antennas

The use of monostatic configurations with dual-port antennas in RFID is still very rare, but offers the substantial benefi to reliably reach very high antenna FOMs. Table 3 lists several dual-port reader antennas that exceed $FOM_{\mathrm{ANT}} > 30\,\mathrm{dB}$ in chronological order. Many solutions are based on polarization to isolate the transmit and receive paths (A-D,F,H) using either dual linear or dual circular polarizations. A dual linear antenna configuration in RFID has the significant

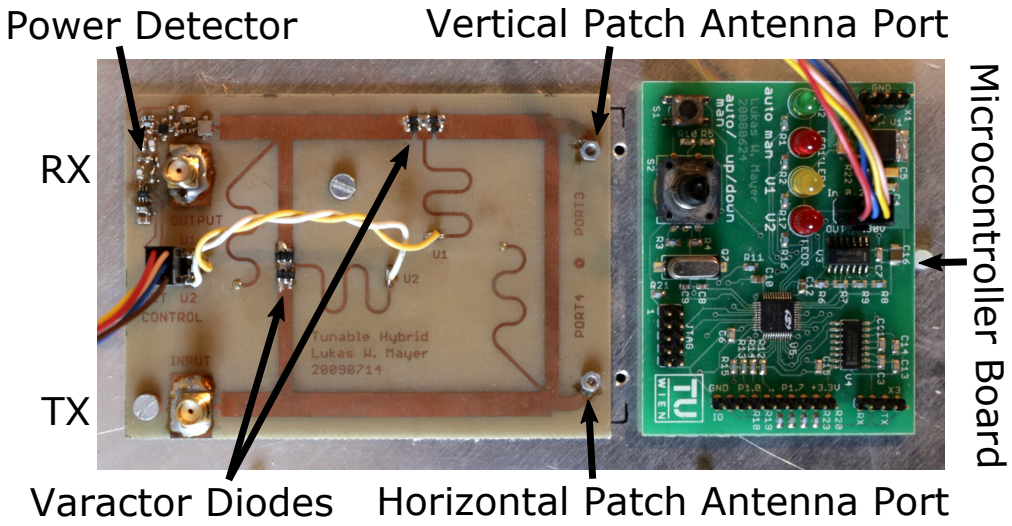


Figure 7: Tunable 3 dB-hybrid with integrated power detector to provide two decoupled ports and feed a dual linear patch antenna to create dual circular polarisation. Compare to [53, Fig. 1]

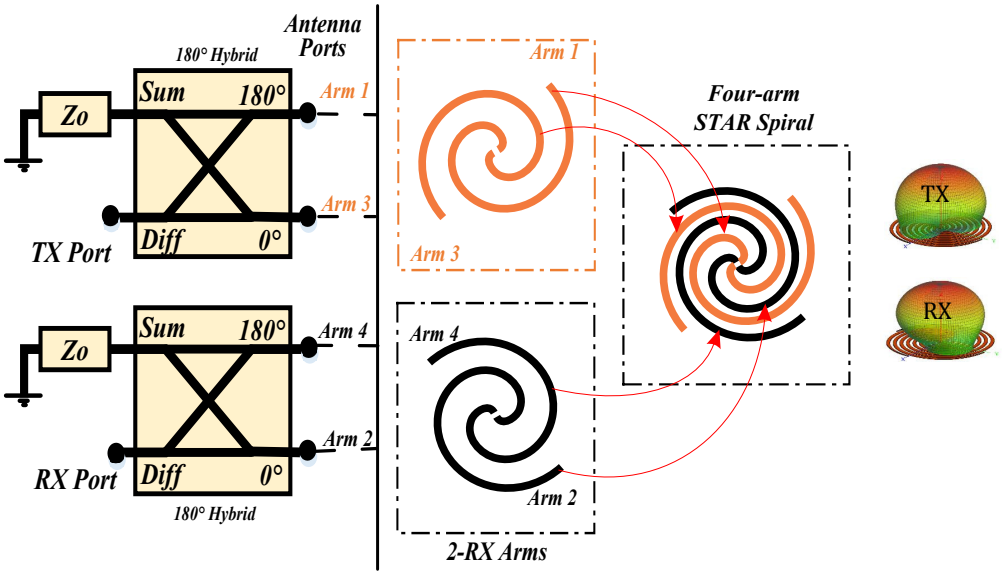
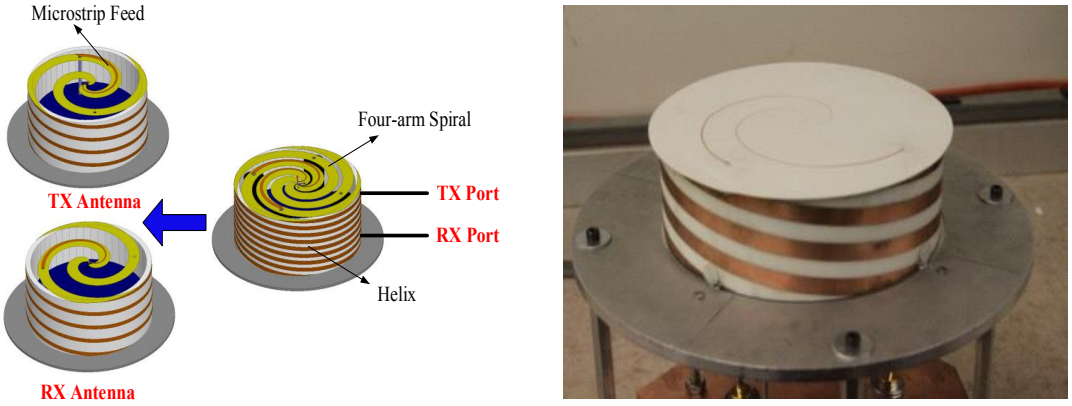


Figure 8: Principle of 4-arm STAR spiral: To 2-arm spirals are fed by 180°-hybrids. Source: Modified from [54, Fig. 1]



(a) (b)

Figure 9: Wideband 4-arm spiral antenna I, Table 3 [54]. a) shows the decomposition in a separate transmit and receive 2-arm spiral, b) shows a photograph of the manufactured antenna. Source: Modified from [54, Fig. 11]

Table 3: Comparison of Dual-Port Reader Antennas.

Description: Reference	Patch A [57]	Patch Array B [58]	inverted F antennas C [59]	Patch Array D [60]	Concentric inverted F array E [55]	Patch w. tuned 3dB Hybrid F [53]	Patch G [56]	Patch w. 3dB Hybrid H [61]	4-Arm Spiral I [54]
Frequency	5400-6000	2400-2500	429-437	860-960	860-960	852-876	900-930	846-929	800-3500
Bandwidth	10.5 %	5 %	2 %	11 %	11 %	2.8 %	3.3 %	7.3 %	126 %
Isolation	Pol.	Pol.	Pol.	Spacing& Pol.	Sym. Beamformer	Pol. & tuned Hybrid	Sym. Beamformer	Pol.	Sym. Phase
TX Pol.	Horiz.	Horiz.	Horiz.	LHCP	RHCP	RHCP	RHCP	RHCP	RHCP
RX Pol.	Vert.	Vert.	Vert.	RHCP	RHCP	LHCP	RHCP	LHCP	RHCP
TX Gain	7.8 dBi	14.5 dBi	3.7 dBi	7 dBi	1 dBi	9.5 dBi	8.1 dBi	6 dBi	4 dBi
RX Gain	7.6 dBi	14.5 dBi	3.4 dBi	7 dBi	0.7 dBi	9.5 dBi	8.1 dBi	6 dBi	4 dBi
Isolation	28 dB	35 dB	25 dB	36 dB	35 dB	52 dB	45 dB	25 dB	37 dB
FOM_{Ant}	43.4 dB	64 dB	32.1 dB	50 dB	37.7 dB	71 dB	61.2 dB	37 dB	45 dB
Size x	$15.2\lambda_0$	-	$4.6\lambda_0$	$6.1\lambda_0$	$3.9\lambda_0$	$8.6\lambda_0$	$4.0\lambda_0$	$7.5\lambda_0$	$11\lambda_0$
Size y	$15.2\lambda_0$	-	$4.6\lambda_0$	$13.7\lambda_0$	$3.9\lambda_0$	$8.6\lambda_0$	$4.0\lambda_0$	$7.5\lambda_0$	$11\lambda_0$

BF: Beam Former, all frequency data in MHz

drawback that tags need to be oriented in a slanted fashion with respect to the transmit and receive polarizations to receive enough signal from the reader to wake up but also scatter back effectively into the reader antenna. Having dual circular polarized antennas avoids this problem with a fixed 3 dB penalty in both the transmit and receive paths, but suffers from the aforementioned problem of increased leakage due to the polarization flip of scattering objects. The antenna with the highest FOM of 71 dB in this table (F) uses polarization decoupling based on a dual-port patch antenna fed with a 3 dB-hybrid coupler. This coupler is shown in Fig. 7, and is loaded with varactor diodes and a power detector. It is directly mounted to the groundplane of the patch antenna, and the ports on the right of Fig. 7 directly feed the vertical and horizontal ports of a dual linear polarized patch antenna, creating circular polarization. A microcontroller running a gradient algorithm (explained in the next section) uses the power detector to continuously adjust the varactor bias voltages and maintain high isolation [53].

The antennas E,G and I from Table 3 use RHCP both for transmit and receive in a truly monostatic configuration, all three achieving isolations exceeding 35 dB. This isolation is based on symmetry in the antennas and the used beamformers, making the transmit currents cancel in the receive path [54–56]. Fig. 8 explains this principle: A 4-arm spiral can be decomposed in two 2-arm spirals shifted by 90°. When the transmit arms are fed by a perfectly balanced 180°-hybrid, the coupling to the neighboring receive arms is completely cancelled due to the symmetry in the antenna [54]. The resulting transmit and receive radiation patterns are identical, except for the mentioned 90° rotation. Fig. 9b shows a practical implementation of this concept using an infinite microstrip balun on a two-layer PCB. The metallic traces are conceptually shown in Fig. 9a. This concept avoids the costly external beamformer, and provides 37 dB of isolation while maintaining a gain exceeding 4 dBi over a 126 % bandwidth. Since antennas G and I [54, 56] are PCB based, they should lend themselves well to cheap mass production combined with excellent performance.

2.3 Leakage Cancellers

Leakage cancellers are employed in practically all RFID readers for two reasons: First, they prevent blocking or overloading of the receiver circuits, and secondly, they reduce the effect of transmit noise leaking into the receiver, as discussed in Section 2.1. To fulfill both goals, they have to provide a second path that takes a part of the transmit signal,

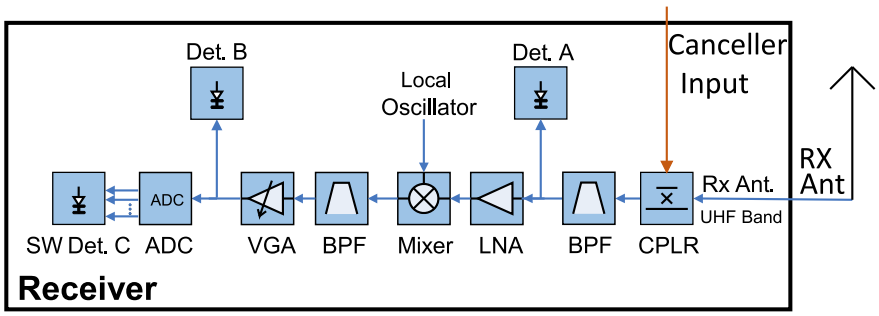


Figure 10: RFID reader receiver with detector (Det.) options. The reader is composed of a directional coupler (CPLR), a bandpass filter (BPF), a low noise amplifier (LNA), a variable gain amplifier (VGA), an analog to digital converter (ADC), and a software (SW) detector in the baseband.

and injects it with the appropriate amplitude and phase into the receiver so that the leaking signal and this injected signal cancel [38]. The bandwidth of this cancellation depends on the difference in path length between the leakage and cancellation path [62], which can be a challenge for readers that allow for arbitrary cable lengths to be connected between the antennas and the reader.

Another challenge is how to adjust a cancelling circuit effectively, especially since a misadjusted cancelling circuit degrades the system performance. A block diagram of a generic superheterodyne reader receiver is shown in Fig. 10. The received signal passes a directional coupler, where the cancellation signal is injected, and a bandpass filter (BPF). The signal is then amplified in a low noise amplifier (LNA), mixed down to an intermediate frequency, again filtered and amplified by a variable gain amplifier (VGA) and finally digitized in an analog to digital converter (ADC). Additionally, this block diagram shows provisions for extra power detectors, labeled A to C. Detectors A and B require extra hardware (a detector diode), while detector C is implemented in software. The benefit in the dedicated hardware detectors lies in the fact that they provide meaningful data even if the receiver is overloaded by a strong leakage signal and a misadjusted, or deactivated leakage canceller. This is especially true for detector A, since it is situated before the first amplifier and can therefore be designed to be linear up to high power levels. Detector B has the benefit of added gain of the previous receiver chain, but is more susceptible to overloading. The biggest benefit of detector C is the fact that for many reader architectures it can provide amplitude and phase information of the leaking signal, and therefore can be used to directly adjust a leakage canceller, if it is calibrated in amplitude and phase.

Table 4: Comparison of Canceller adjustment techniques

Algorithm	References	Detector type	Det. linearity constraint	Speed	Canceller calibration
Full search	[63]	Power	None	Slow	No
Gradient search	[38, 64, 65]	Power	Low	Medium	Minimal
Fast algorithm	[66, 67]	Power	High	Fast	Yes
Direct I/Q	[68, 69]	Amp. & phase	High	Fast	Yes

A summary of popular adjustment algorithms for leakage cancellers is given in Table 4, sorted from slowest to fastest. We see that the slowest full search algorithm that just steps through all possible settings of the canceller circuit has no calibration requirements or detector linearity constraints. The very commonly used gradient algorithm just requires a detector that is not fully saturated and a monotonously reacting canceller control. The fast algorithm requires a calibrated canceller and derives the required canceller setting from three successive amplitude measurements [66]. Finally the direct I/Q algorithm requires an amplitude and phase detector and a calibrated canceller. Both referenced implementations [68, 69] achieve this in a pure analog way with a separate analog I/Q detector at location A in Fig. 10, but a digital implementation using the software detector C is possible. Many readers also employ two or more algorithms to find the best cancellation setting. For example, it is beneficial to first find a coarse canceller setting that reduces the power levels in the receiver using a "full search" algorithm, and then apply a smarter algorithm to fine tune that result utilizing the detectors that were previously overloaded by the strong leakage signal.

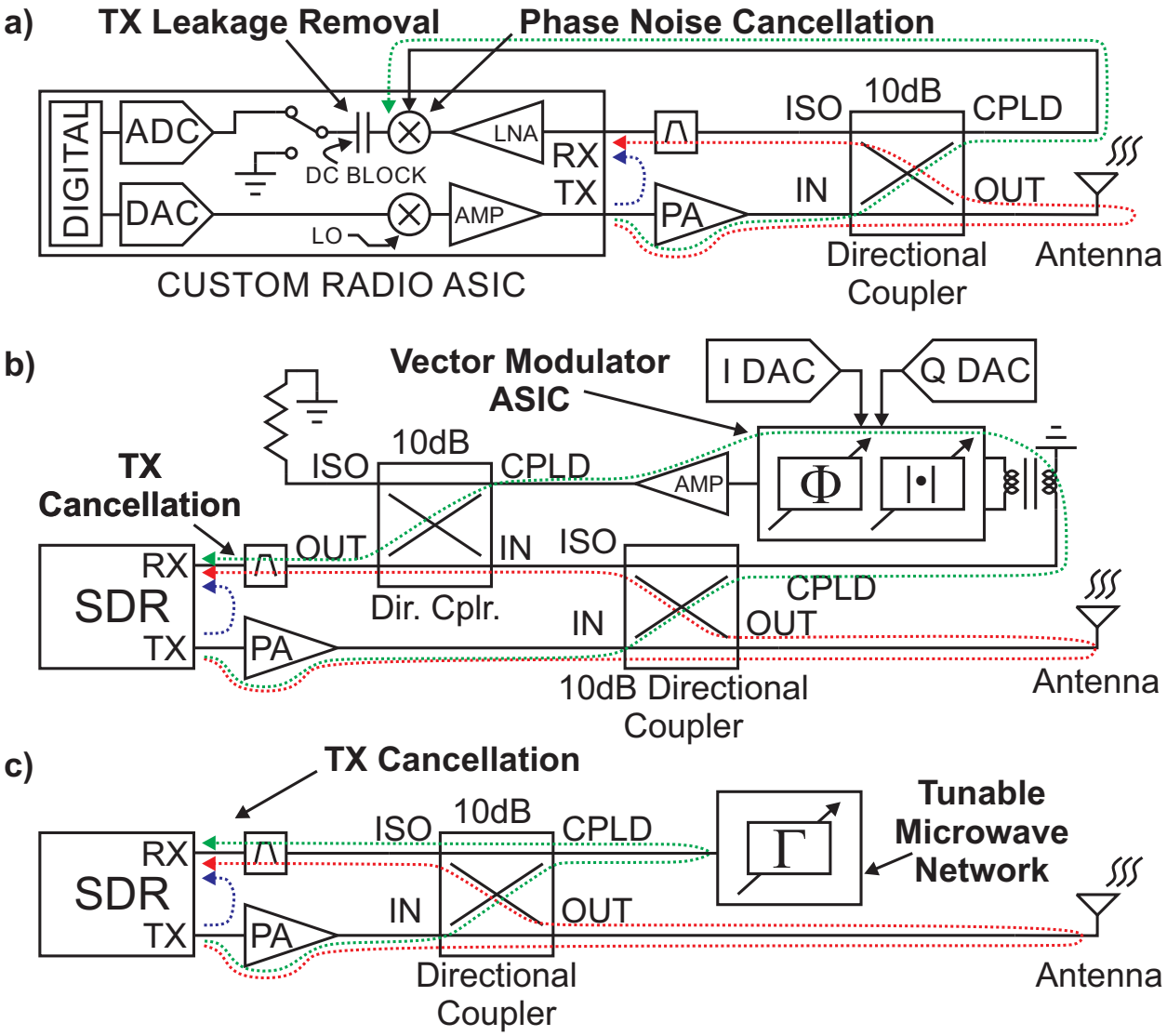


Figure 11: Transmit leakage cancellation circuit concepts in UHF RFID literature applied to monostatic reader with directional coupler-based antenna duplexing: a) On-chip; b) Vector modulator; c) Reflected power canceller. New abbreviations in this figure include: Amplifier (AMP), Coupled Port (CPLD), Directional Coupler (Dir. Cplr.), Isolated Port (ISO), and Power Amplifier (PA).

3 Low-Cost Leakage Cancellation Circuits

As described above, maintaining a large transmit-to-receive isolation in the UHF RFID reader is critical to achieving a meaningful tag read range. This proves to be doubly true when using low-cost radio hardware, which will have higher transmit and receive phase noise than otherwise. Thousand-dollar reader systems can afford bulky circulators and elaborate cancellation mechanisms to ensure that a pristine tag backscatter signal appears at the radio receiver input. But what if the leakage cancellation circuit needs to cost on the order of $3 in bulk? How does one go about choosing an architecture and improving it, if necessary, to meet the isolation requirements of the system?

3.1 Classes of Leakage Cancellation Circuits

In the UHF RFID literature, these authors consider three main classes of leakage cancellation circuit, shown in Fig. 11. Each of these circuits can be used in a monostatic or bistatic reader antenna arrangement with some modification. For the purposes of this article, the monostatic arrangement, with transmit and receive paths accessing the antenna with a directional coupler, will be discussed and depicted in keeping with the theme of low cost.

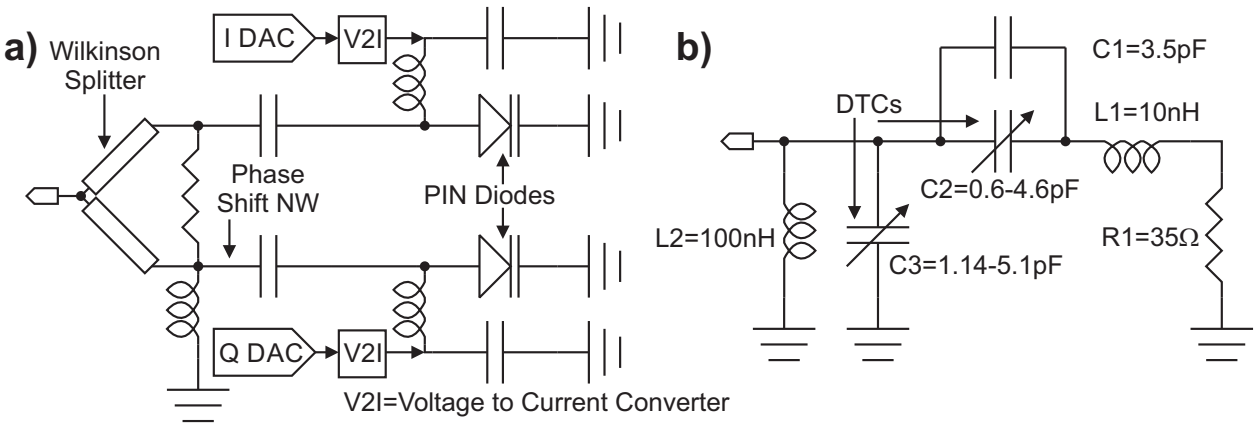


Figure 12: Prior art in UHF RFID reader reflected power canceller tunable microwave networks: a) PIN diode-based [37, 76] ; b) Digitally tunable capacitor (DTC)-based [77].

3.1.1 On-Chip

As described in [70] and shown in Fig. 11a, to significantly reduce the phase noise resulting from the transmit leakage, the mixers in the radio receiver can be driven by a coupled and attenuated version of the transmitter output in place of an RX local oscillator (LO). This works for UHF RFID because the transmit signal is strictly sinusoidal while the reader is receiving the tag's response. Since the phase noise of the transmitter output and, by design, the RX LO is naturally highly correlated with that of the transmit leakage, when these two signals multiply in the receiver mixer, very little of the phase noise appears at baseband. While the downconverted transmit leakage still exists as a low-noise DC signal, this signal can be removed by resettable alternating-current (AC) coupling capacitors or DC-cancelling servo circuits [70]. The advantages of such circuits are that they can be had for very low incremental cost and occupy a very small amount of PCB space. The downside is that the application-specific integrated circuit (ASIC) described in [70] does not appear to be publicly available on major distributor websites and the fixed cost of developing and sourcing a new ASIC for this purpose can easily run over a million U.S. dollars.

3.1.2 Vector Modulator

Perhaps the most obvious approach to improving transmit leakage cancellation is to couple off a portion of the transmit signal, explicitly adjust the amplitude and phase of this signal, then couple the resulting signal back into the receive path. This approach is known as "vector modulation", is depicted in Fig. 11b, and has been utilized in numerous UHF RFID reader studies [62, 64, 71–73]. While vector modulation can be effectively deployed with publicly available ASICs, such alternatives are few (AD8340 & HMC630LP3E) and expensive ($10.19 & $16.29, respectively, in bulk). In addition, the leakage cancellation path typically requires a balun, two external digital-to-analog converters (DACs), an amplifier to recover from the path losses, and an extra directional coupler. While all of these supporting devices may be had for $1-$2 each in bulk, the cost adds up quickly.

3.1.3 Reflected Power Canceller

Instead of explicitly processing the coupled TX leakage signal through a vector modulator, imagine just bouncing it back into the receiver using a termination with a reflection coefficient (Γ) equal to the negative of the antenna's (Γ_{ANT}), plus any phase adjustments related to routing mismatches on the PCB. Then, the two reflected signals cancel at the isolated (ISO) port of the directional coupler. This is the concept behind the "reflected power canceller" (RPC), depicted in Fig. 11c. This concept originated in the radar technical literature [74] and subsequently was applied to UHF RFID in [75]. To account for a changing antenna reflection coefficient, RPC architectures with tunable microwave networks (TMNs) used to adaptively generate these arbitrary reflection coefficients (Γ_{TMN}) were subsequently reported in the UHF RFID literature [37, 76, 77].

Tunable microwave networks described for UHF RFID RPCs fall roughly into two categories: those comprised of tunable P-insulator-N (PIN) diodes [37, 76] and those defined by the use of digitally tunable capacitors (DTCs) [77]. PIN diodes can be modeled as current-controlled resistors at radio frequencies, and two of them accessed with a quadrature splitting network, shown in Fig. 12a, can realize a wide range of complex reflection coefficients. In addition to the cost of the two DACs required to set the currents, this architecture has the issue of noise current generated by the PIN

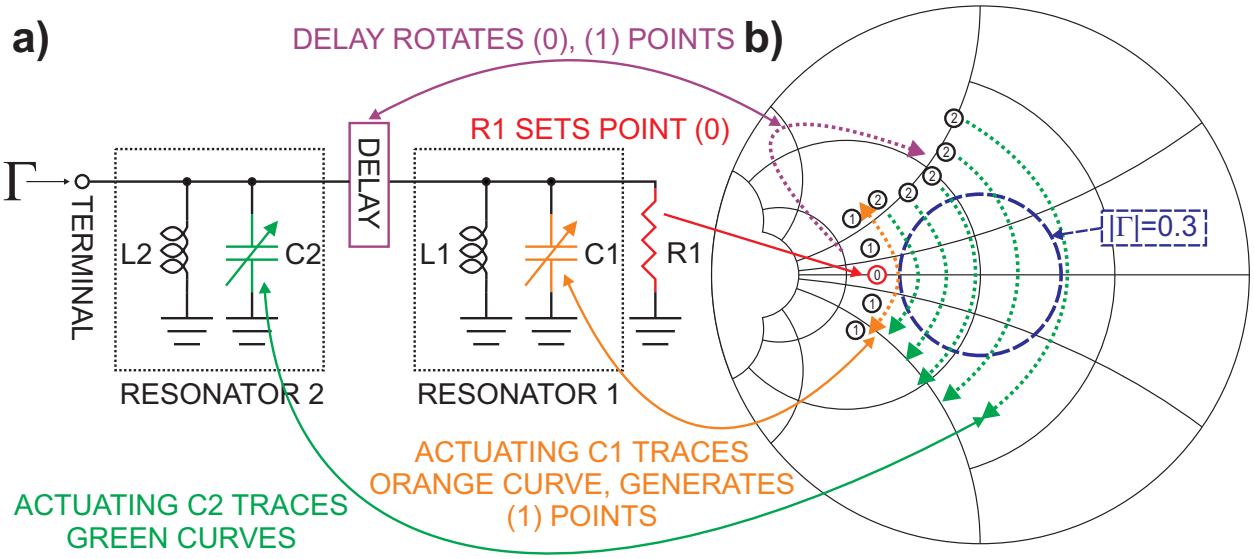


Figure 13: (a) Shunt-shunt coupled resonator network and (b) coverage of the tunable microwave network specification area. Source: Modified from [65, Figs. 2,3].

diode resistance modulating the resistance itself, thereby modulating the incident coupled transmit signal [76] such that significant noise can occur at the tag BLF. To avoid this problem, a relatively new class of component, the (DTC), was used to implement the TMN in the circuit shown in Fig. 12b [77]. DTCs are largely noiseless, handle watt-level power, but most importantly for our purposes, they are publicly available on the cheap, currently running for less than $0.60 in quantities of 6,000 or greater. The downside of currently available DTCs is the limited resolution. At about 5 bits apiece, a two-DTC network such as the one in [77] is only enough to practically achieve about 20dB of added transmit-receive leakage isolation.

3.2 Designing a Tunable Microwave Network (TMN)

For any RPC-based transmit leakage cancellation circuit, the rough objective is to design a TMN that can minimize the distance of any possible Γ_{ANT} to a realizable reflection coefficient Γ_{TMN}. For the standard case in which a low-cost antenna's reflection coefficient is constrained to be "less than -10dB" over the range of frequency operation, the specification area to be covered is a circle with radius equal to 0.3 centered at the middle of the Smith Chart, as depicted in Fig. 13b.

A coupled resonator network, depicted in Fig. 13a [78], was originally proposed for matching a mobile phone's power amplifier to its antenna. With component values chosen correctly, such a network with a $25\,\Omega$ seed impedance R1 covers the target area of the Smith Chart, as depicted in Fig. 13b. Though a successful blanketing of the target area was achieved, the problem of limited TMN resolution still remains.

Clearly, more 5-bit DTCs must be added to the network to realize more Γ_{TMN} in the target circle, since doing so permits greater TX-RX isolation. One conceptually simple way to do this would be to just couple more resonators onto the network. This can be made to work from a coverage standpoint, as depicted in Fig. 14; however, manipulating the four resulting state variables will be in general be computationally expensive for the tuning algorithm. Also, the point coverage of the target area is uneven, leading to wide open areas that result in larger-than-necessary maximum cancellation errors. A preferable approach is introduced in [65] and shown in Fig. 15 in which the inductors of the shunt resonators in the original two-resonator network are modified to act as tapped impedance dividers to yet another set of DTCs. If the inductive division is appropriately chosen, a Zobel transformation [79] can be applied to the network to show that the newly added DTCs serve as subranging programmable capacitors. Now, not only are the number of states increased to 1048576, but this is done without increasing the number of state variables. The worst-case cancellation ratio was indeed confirmed to increase from $20\,\mathrm{dB}$ to $50\,\mathrm{dB}$ via computational analysis, while the coverage characteristics can be seen to be quite uniform locally in Fig. 16.

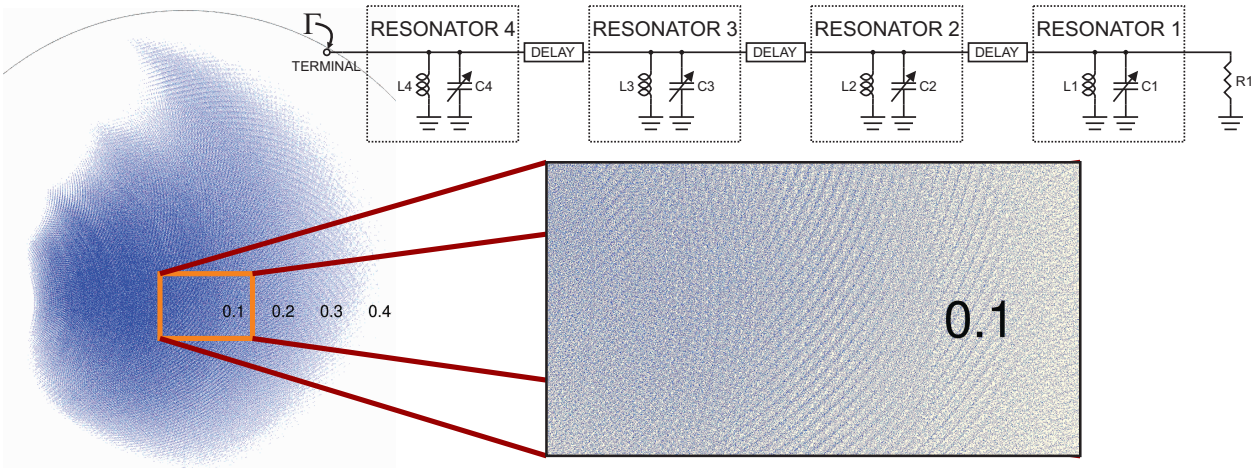


Figure 14: Initial attempt at increasing tunable microwave network resolution: four cascaded resonator stages and simulated coverage results. Source: Modified from [65, Fig. 4].

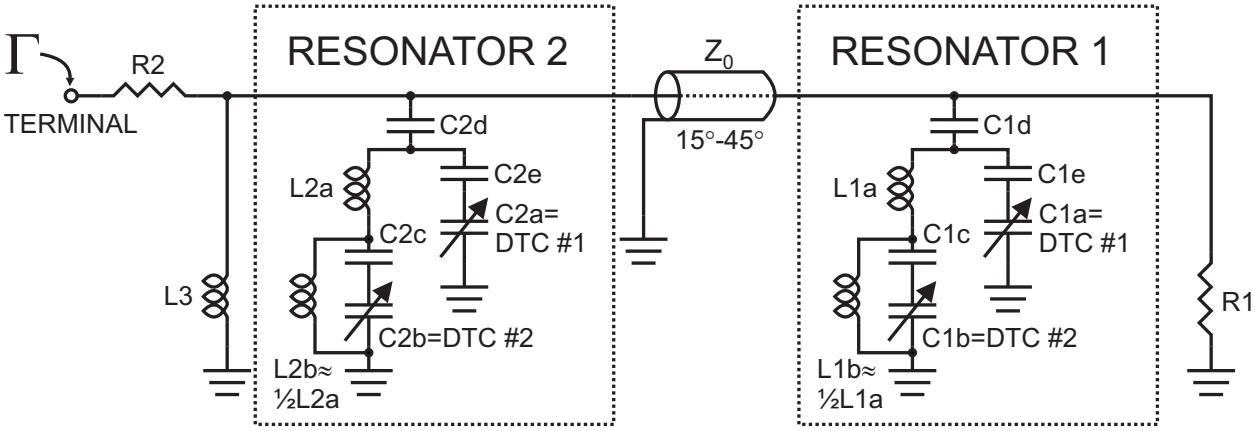


Figure 15: Proposed subranging digitally tunable capacitor-based tunable microwave network. Source: Modified from [65, Fig. 5].

3.3 Tuning Algorithm and Measured Results

The final reflected power canceller circuit implemented for the reader described in [20, 65] is shown in Fig. 17. The cost of the 4 DTCs is $2.30 in quantities of 15,000. The directional coupler cost $0.46 but would have been needed anyway. High quality inductors (the blue components in Fig. 17) were used for first-pass success at a bulk cost of $0.67 for all four in total. Since it is clear that the network can be quite lossy, much cheaper low-quality inductors can be used in future iterations. The TMN is driven by a blind gradient-descent algorithm in the reader FPGA which uses as its cost-minimization function an estimate of the transmit leakage RF magnitude derived from complex baseband data. This algorithm addresses a number of practical considerations in the SDR ASIC and TMN design and is described in more detail in [65]. The canceller circuit and algorithm were tested together using a set of dummy loads at the antenna port with $|S11| \approx -11\,\mathrm{dB}$ and 12 random $\angle(S11)$ with a transmit output power of $26\,\mathrm{dBm}$. While the suppression of the TX leakage, shown in Fig. 18a, is roughly as expected; greater than $49\,\mathrm{dB}$ for all angles, what really matters is the suppression of input-referred phase noise, since this is the signal which actually corrupts the backscattered tag response. As shown in Fig. 18b, this is improved by over $48\,\mathrm{dB}$ for all but two points and by over $44\,\mathrm{dB}$ for these. From this latter plot, after adding $19\,\mathrm{dB}$ to refer SDR ASIC-input-referred noise quantities back to the antenna, we can compute for the more typical angle results:

$$FOM_{\mathrm{R}} = P_{\mathrm{TX,ANT}}(\mathrm{dB}) - P_{\mathrm{N,ANT}}(\mathrm{dB}) - IS_{\mathrm{ANT}}(\mathrm{dB}) = 26\,\mathrm{dBm} - (-81\,\mathrm{dBm}) - 11\,\mathrm{dB} = 96\,\mathrm{dB} \quad (6)$$

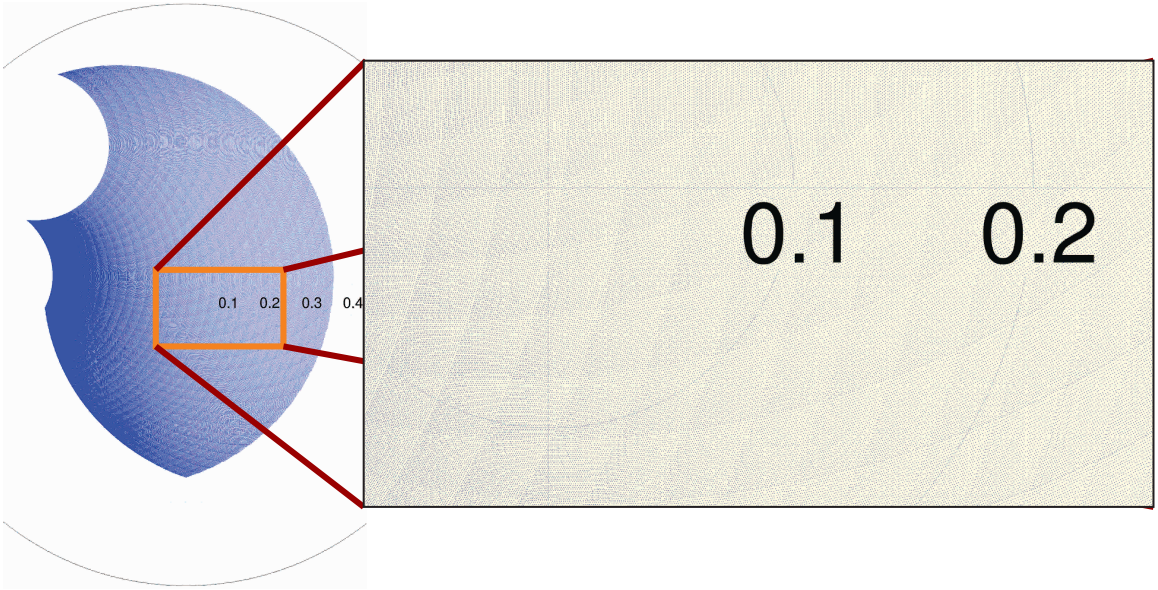


Figure 16: Simulation results of proposed subranging tunable microwave network reflection coefficient coverage. Source: Modified from [65, Fig. 7].

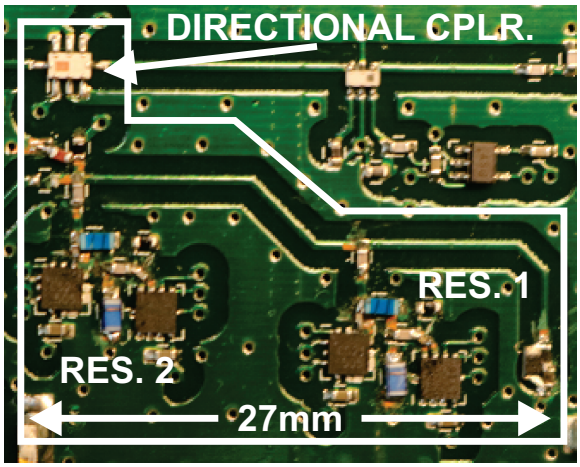
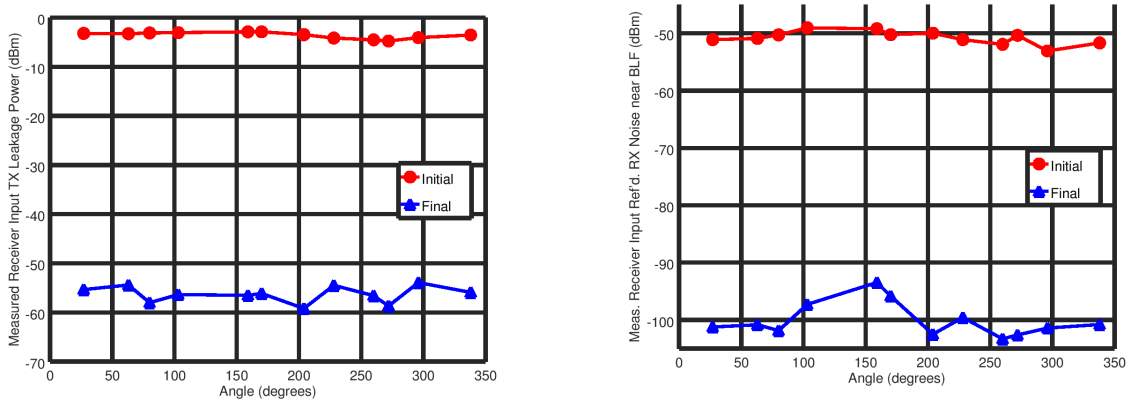


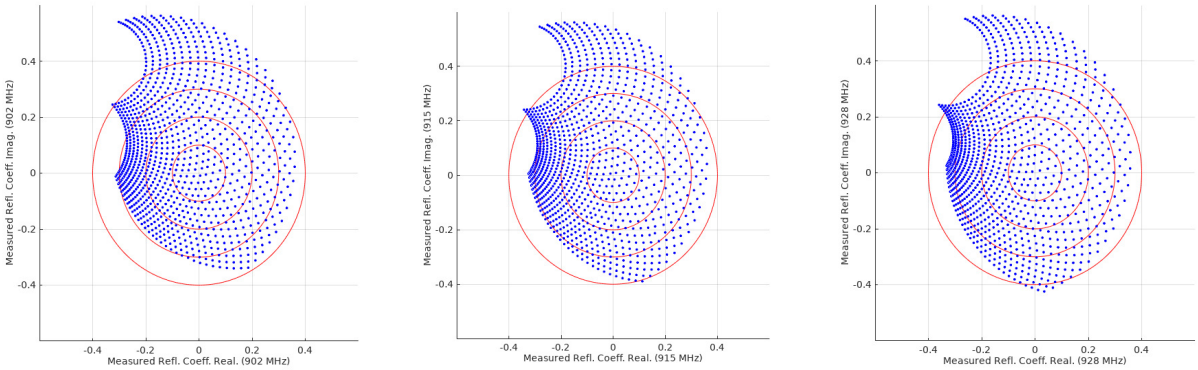
Figure 17: Photograph of implemented and tested reflected power canceller. “Res." denotes a resonator. “Cplr." denotes a coupler. Source: Modified from [65, Fig. 11].



(a) Measured transmit leakage referred to SDR ASIC RX input.

(b) Measured noise at data recovery circuit referred to SDR ASIC RX input.

Figure 18: Measurement results for transmit leakage cancellation network described in [65]. Source: Modified from [65, Figs. 9,13].



(a) 902MHz

(b) 915MHz

(c) 928MHz

Figure 19: Measured Smith chart coverage results across the U.S. 900MHz license free band. Source: Modified from [65, Fig. 12].

Coarse TMN coverage measurement results are shown in Fig. 19. The Smith chart coverage pattern is consistent with simulation and varies little over the U.S. 900 MHz license free band. More measurement results and test details for this circuit are provided in [65].

4 Low-Cost Software-Defined UHF RFID Readers

4.1 Top Level Architecture

In keeping with our goal of developing a tool for many people to explore UHF RFID, we endeavor to design a UHF RFID reader by selecting components that are as cheap as possible, integrating as much programmable functionality as possible, and that come with data sheets and other application information that are comprehensive as possible. Flowing from all of these considerations combined is the reader architecture shown in Fig. 20 [20], which also shows the pricing of key components. The SDR chip chosen is the Semtech SX1257. At the time this project was initiated, this was the lowest cost publicly accessible SDR ASIC which allowed access to its raw baseband (in-phase (I) and quadrature (Q)) data and permitted full duplex radio operation. Ideally, the SDR ASIC would include features such as those described in [70] to promote transmit leakage cancellation, but sadly does not. The FPGA chosen is the Altera (now Intel) 10M02 with 2,304 logic elements. One of the primary challenges of this project was fitting an entire UHF RFID digital back end and TMN controller into such a small resource count. The transmit leakage cancellation is accomplished by the reflective power canceller featuring a subranging DTC-based TMN described just previously. Together, these three

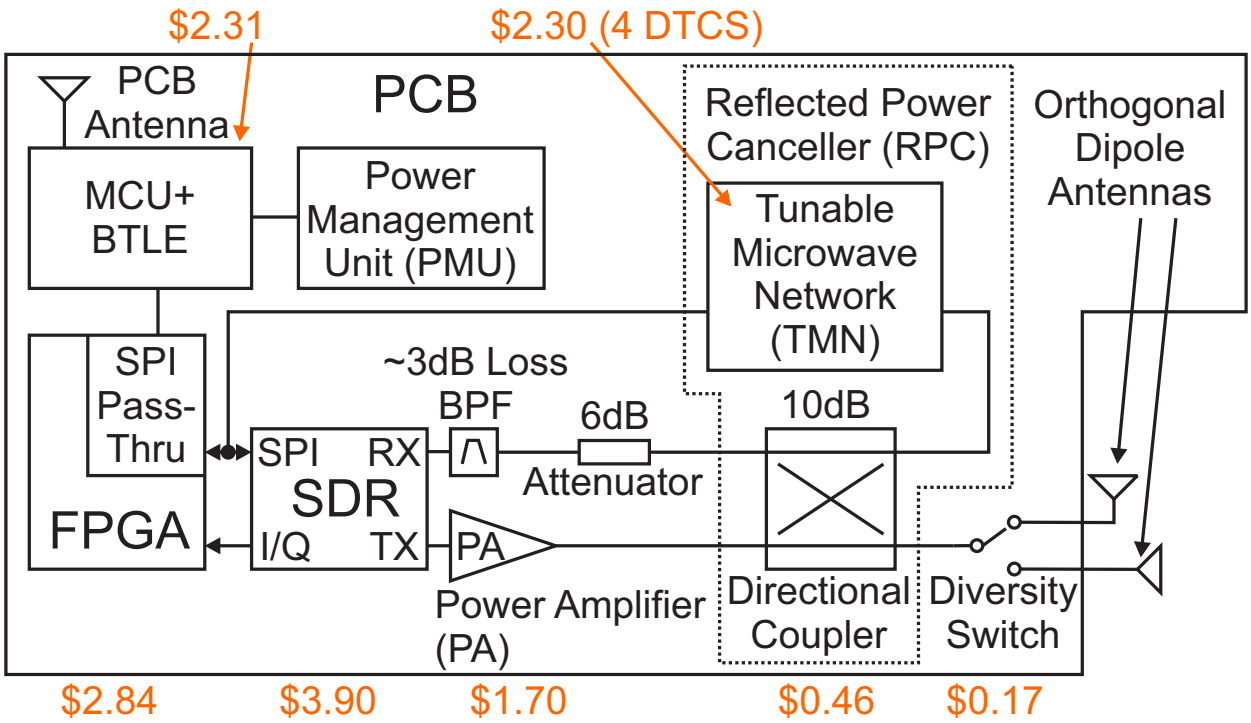


Figure 20: Proposed UHF RFID reader top-level block diagram with current publicly available bulk pricing. Source: Modified from [20, Fig. 1].

subsystems at $9.04 replace one of the publicly accessible reader ASICs available on major distributor websites. The cheapest of these, the ST25RU3980, currently sells for $21.60 in bulk, does not have a publicly accessible full data sheet (only a "datashort"), can only execute a single tag read every $500\,\mathrm{ms}$ [80], is currently scheduled for obsolescence, and still requires an external structure to provide transmit leakage cancellation for a reader output power of $26\,\mathrm{dBm}$ and an antenna $|S_{11}| \approx -10\,\mathrm{dB}$, given a $1\,\mathrm{dB}$-compression point (ICP1) of $7\,\mathrm{dBm}$ [81].

Intelligence is implemented on the proposed reader in a Nordic Semiconductor NRF51822 combined MCU + BTLE ASIC. In addition to extensive publicly accessible documentation and software development kits (SDKs) for their ASIC, Nordic will even tell you how to use the free Eclipse firmware integrated development environment (IDE) with their chips and toolkit [82]. The MCU controls the FPGA and sets control registers on the SDR ASIC through a serial peripheral interface (SPI) bridge on the FPGA. The FPGA accepts and provides 1-bit baseband I and Q data to and from the SDR ASIC, which converts said bitstreams to and from the over-the-air radio waveforms within the $900\,\mathrm{MHz}$ U.S. license free band. The power amplifier (PA) amplifies the SDR output up to about $1\,\mathrm{W}$, the receive BPF removes any interferers from outside the $900\,\mathrm{MHz}$ band, while the $6\,\mathrm{dB}$ attenuator ensures that the maximum TX leakage does not damage the SDR ASIC receiver input. Diversity antenna ports and a switch to commutate between them provide access to RFID tags of different polarizations in the local environment. The implemented reader, shown in Fig. 21, is assembled on a 4-layer PCB that measures 7.4" x 1.3".

4.2 FPGA

The Software-Defined Radio aspect of the reader consists of two devices: the FPGA and the MCU. While the FPGA is often thought of as "hardware", it is programmed with code and can in principle be re-flashed over the air through the MCU and hence can accurately be claimed as "software-defined". Given the current state of low-cost ASIC technology, the software-defined UHF RFID reader cannot be implemented using an MCU alone. Most affordable MCUs running at moderate power dissipation feature a maximum clock rate of few hundred MHz. While a few operations may be parallelized on some MCUs, the UHF RFID digital back end requires dozens of arithmetic operations running at the frequency of the SDR ASIC (in this case, $36\,\mathrm{MHz}$), not to mention the hundreds running at somewhat lower rates. A power-and-cost-competitive MCU capable of handling this task on its own does not currently exist, but this sort of signal processing burden is easily handled by an FPGA.

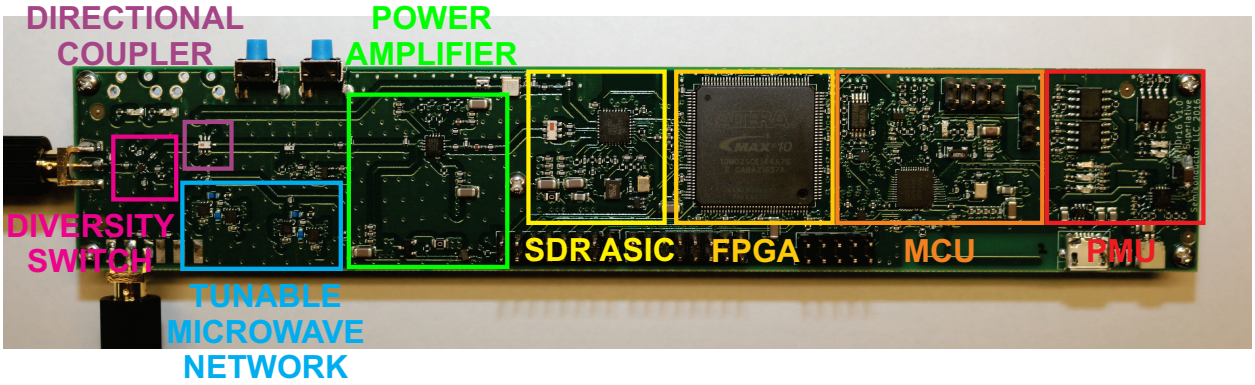


Figure 21: Implemented reader with key subsections highlighted. Source: Modified from [20, Fig. 8].

The top level of the FPGA internal logic design is shown in Fig. 22. Connections to the SDR signal path are on the left, while input and output control connections are on the right of Fig. 22. The FPGA unburdens the MCU by allowing the MCU to load the FPGA's static random access memories (SRAMs) with various commands and transmit waveform data prior to an RFID radio operation and to extract receive waveform data when the operation is done. During radio operations, which require low latency, the MCU hands off control of the system to the FPGA's finite state machines (FSMs). Clock domain partitioning was critical to meet the data rate requirements of the SDR ASIC ($36\,\mathrm{MHz}$), the requirement to interface over SPI buses as quickly as possible ($27\,\mathrm{MHz}$), and the requirement to keep the bulk of the signal processing circuitry operating at a data rate as low as possible ($4.5\,\mathrm{MHz}$) in order to ease timing closure and maximize utilization of the FPGA resources. Why not set the minimum clock rate even lower? In general, most of the blocks in this clock domain have some implicit requirement to be running at about $4.5\,\mathrm{MHz}$. For example, the minimum clock rate dictates the time resolution of the waveforms that the transmit baseband waveform generator (TX GEN) can create. Too slow, and the waveforms generated don't meet the EPC Gen 2 transmit timing requirements. Another example is the clock recovery circuit. In order for it to provide a meaningful approximation to its continuous-time inspiration, it needs to be running at an oversampling ratio of at least 10 or so. With the tag BLF at $187.5\,\mathrm{kHz}$, the "data" rate handled by the clock recovery circuit is $375\,\mathrm{kHz}$, requiring a clock rate of greater than about $3.75\,\mathrm{MHz}$. More details on the various sub-blocks used in the FPGA can be found in [20].

4.3 Measured Results

Line-of-sight outdoor range of the reader was measured in an outdoor street setting, shown in Fig. 23a, and was found to be 2.6m for a half-wave dipole antenna and $15.2\,\mathrm{m}$ for a $12.5\,\mathrm{dBi}$ patch antenna before the tag read rate dropped to below 50%. The read range was less than the ideal number predicted in Fig. 6 due to an increase in the receiver noise floor during operation when an antenna was attached to the reader. Tones in the measured phase noise spectrum suggest that this increase is due to coupling from the antenna into the SDR ASIC, but the noise may also be due to delayed transmit reflections from objects in the environment. More results and testing details regarding the reader are covered in [20].

5 Conclusion

In this article, we've shown how to analyze and tackle many of the challenges associated with building a low-cost software-defined UHF RFID reader. We've discussed the essential requirements in terms of leakage cancellation and its impact on receiver noise and shown the benefit of high gain, well-isolated reader antennas along with a survey of the same in the context of an antenna figure of merit. Following this, we presented a survey of low-cost leakage canceller circuits and delved into some of the details of building the reader hardware, supporting the discussion with measured results of an implemented low-cost reader and its integrated reflected power canceller circuit. With such a reader, we expect the barrier to entry for experimenting with UHF RFID at long range to fall considerably, making it easier for the community at large to hunt for RFID's killer app. Of course, we don't expect the readers of this article to develop all of the hardware described herein from scratch. That is why in conjunction with the publication of this article, we are open-sourcing the reader project described above, with the source and licensing materials located at www.openrfidreader.net. It is our hope that the community of electrical engineers, hobbyists, tinkerers, and students find this to be an exciting, educational, and perhaps even profitable project through which they can computationally interact with the objects in the world around them.

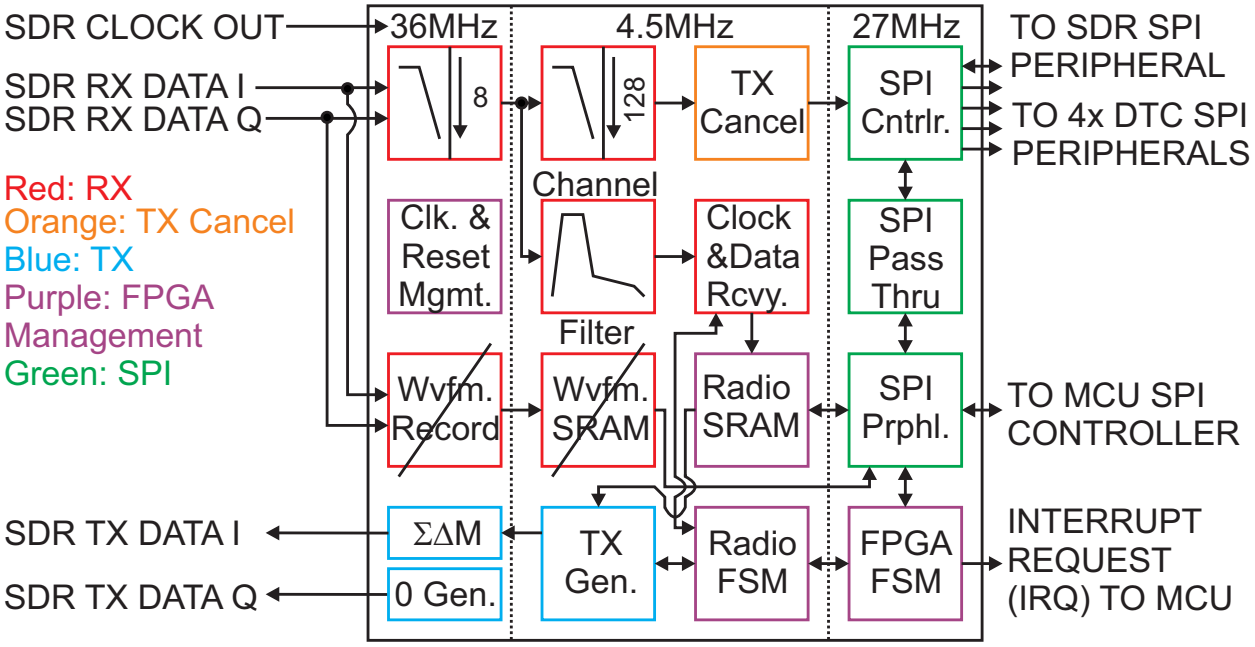
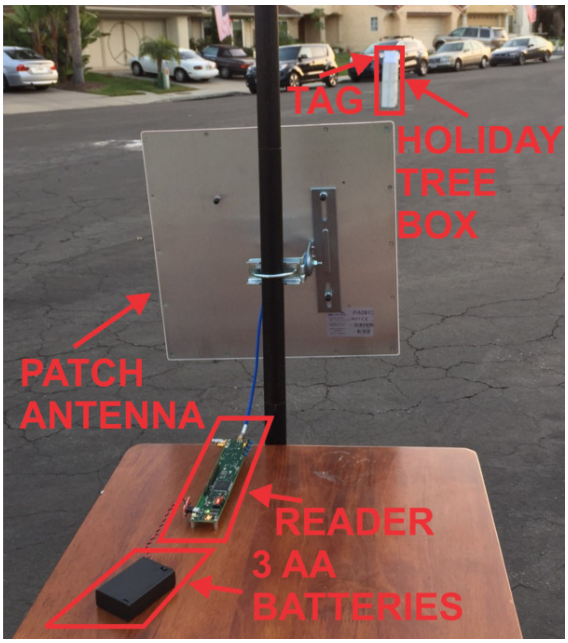
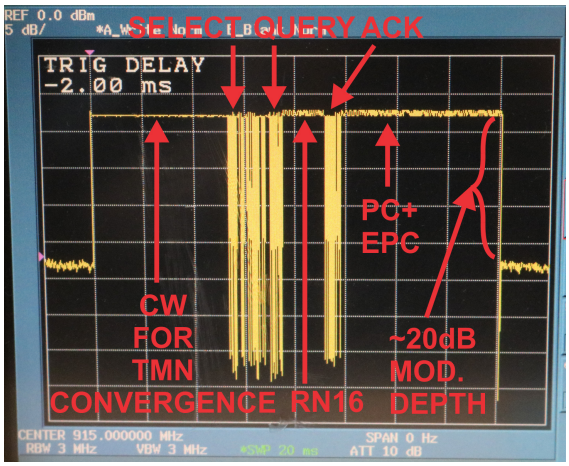


Figure 22: Depiction of reader FPGA digital design top level architecture. Crossed out blocks are those currently disabled to permit fitting of the design in the FPGA. New abbreviations in this figure include: Clock (Clk.), Controller (Cntrlr.), Finite State Machine (FSM), Management (Mgmt.), Peripheral (Prphl.), Transmit Waveform Generator (TX Gen.), Waveform (Wvfm.), Zero Waveform Generator (0 Gen.), and Sigma-Delta Modulator (ΣΔM). Source: Modified from [20, Fig. 3].



(a) Reader range measurement setup.



(b) Measured reader transmit waveform showing ≈20 dB modulation (mod.) depth and backscatter response. From left to right, a continuous wave (CW) signal is transmitted for TMN convergence, Select and Query EPC Gen 2 commands are transmitted by the reader, the tag backscatters an RN16 EPC Gen 2 response, the reader transmits an ACK command, and finally the tag backscatters its protocol-control (PC) and electronic product code (EPC) bits. Source: Modified from [20, Fig. 9].

Figure 23: Reader range test setup and over-the-air RFID traffic capture.

References

[1] "EPC radio-frequency identity protocols generation-2 UHF RFID specification for air interface protocol for communications at 860MHz - 960MHz version 2.0.1 ratified," 2015.

[2] R. Bhattacharyya, C. Floerkemeier, and S. Sarma, "Low-cost, ubiquitous RFID-tag-antenna-based sensing," *Proc. IEEE*, vol. 98, pp. 1593–1600, Sep. 2010.

[3] J. Melià-Seguí and X. Vilajosana, "Ubiquitious moisture sensing in automaker industry based on standard UHF RFID tags." in *Proc. IEEE Int. Conf. RFID*, Apr. 2019, pp. 1–4.

[4] C. R. Schoenberger, "The internet of things," *Forbes*, Mar. 2002.

[5] A. Bednarz, "RFID everywhere: from amusement parks to blood supplies," *Network World*, May 2004.

[6] R. Want, "RFID: A key to automate everything," *Scientific American*, Jan. 2004.

[7] M. Malone, "Did Wal-Mart love RFID to death?" *ZDNet*, Feb. 2012.

[8] S. Garfinkel, "An RFID bill of rights," *MIT Tech. Review*, vol. 105, p. 35, Oct. 2002.

[9] Wired Staff, "RFID: sign of the (end) times?" *Wired*, vol. 105, pp. 1593–1600, Mar. 2006.

[10] D. Friedlos, "Australia's Woolworths Supermarket Chain Studies RFID," *RFID Journal*, Oct. 2008, https://www.rfidjournal.com/australias-woolworths-supermarket-chain-studies-rfid, Accessed: 2020-09-17.

[11] X. He, "Will Amazon Go win the war between computer vision and RFID in retail?" *IDTechEx Research*, Jan. 2017.

[12] D. A. Kaplan, "The rise, fall, and return of RFID," *Supply Chain Dive*, Aug. 2018.

[13] The Build Network Staff, "6 lessons on innovation from the history of the barcode," *Inc. Magazine*, Jan. 2014.

[14] C. Anderson, *Makers: The New Industrial Revolution*, 1st ed. New York: Crown Business, 2012.

[15] M. Hatch, *The Maker Movement Manifesto*, 1st ed. New York: McGraw Hill, 2014.

[16] A. Sample, D. Yeager, P. Powledge, A. Mamishev, and J. Smith, "Design of an RFID-based battery-free programmable sensing platform," *IEEE Trans. Instrum. Meas.*, vol. 57, pp. 2608–2615, Nov. 2008.

[17] S. Thomas, "RFID for everyone: design of an easily-accessible, experimental, UHF RFID platform," in *Proc. IEEE Int. Conf. RFID*, Apr. 2019, pp. 1–4.

[18] J. Kimionis *et al.*, "Design and implementation of RFID systems with software defined radio," in *6th EUCAP*, Mar. 2012, pp. 3464–3468.

[19] A. Briand *et al.*, "Complete software defined RFID system using GNU radio," in *Proc. IEEE Int. Conf. RFID-TA*, Nov. 2012, pp. 287–291.

[20] E. A. Keehr, "A low-cost software-defined UHF RFID reader with active transmit leakage cancellation," in *Proc. IEEE Int. Conf. RFID*, Apr. 2018, pp. 1–8.

[21] N. Roy *et al.*, "Designing an FPGA-based RFID reader," *Xcell Journal*, vol. 2, pp. 26–29, 2006.

[22] C. Huang *et al.*, "A new architecture of UHF RFID digital receiver for SoC implementation," in *IEEE WCNC*, Mar. 2007, pp. 1659–1663.

[23] C. Angerer *et al.*, "A flexible dual frequency testbed for RFID," in *Proc. 4th Int. Conf. Testbeds and Research Infrastructures for the Development of Networks and Communities*, Mar. 2008, pp. 3:1–3:6.

[24] ——, "Advanced synchronization and decoding in RFID reader receivers," in *Proc. IEEE RWS*, Jan. 2009, pp. 59–62.

[25] R. Langwieser *et al.*, "A modular UHF reader frontend for a flexible RFID testbed," in *Proc. 2nd Int. EURASIP Workshop on RFID Tech.*, July 2008, pp. 1–12.

[26] M. Buettner and D. Wetherall, "UW-CSE-09-10-02: A flexible software radio transceiver for UHF RFID experimentation," Univ. of Washington, Tech. Rep., Oct. 2009.

[27] G. Smietanka *et al.*, "Implementation and extension of a GNU-Radio RFID reader," *Adv. in Radio Sci.*, vol. 11, pp. 107–111, July 2013.

[28] L. Catarinucci *et al.*, "A cost-effective SDR platform for performance characterization of RFID tags," *IEEE Trans. Inst. and Meas.*, vol. 61, pp. 903–910, Apr. 2012.

[29] C. S. Yoon *et al.*, "A design of UHF-band RFID reader using FPGA," *ResearchGate*, pp. 1–4, Nov. 2014.

[30] C. Jin *et al.*, "A robust baseband demodulator for ISO 18000-6C RFID reader systems," *Int. J. Dist. Sensor Networks*, vol. 2012, pp. 1–12, Jul. 2012.

[31] P. Nikitin *et al.*, "Simple low cost UHF RFID reader," in *Proc. IEEE Int. Conf. RFID*, Apr. 2013, pp. 126–127.

[32] A. Borisenko, M. Bolic, and M. Rostamian, "Intercepting UHF RFID signals through synchronous detection," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013:214, pp. 1–10, Aug. 2013.

[33] N. Kargas *et al.*, "Fully-coherent reader with commodity SDR for Gen2 FM0 and computational RFID," *IEEE Wireless Comp. Letters*, vol. 4, pp. 617–620, Dec. 2015.

[34] F. Galler, T. Faseth, and H. Arthaber, "SDR based EPC UHF RFID reader DS-SS localization testbed," in *IEEE Wireless and Microwave Technology Conf. (WAMICON)*, Apr. 2015, pp. 1–4.

[35] ——, "Implementation aspects of an SDR based EPC RFID reader testbed," in *Intl. EURASIP Workshop on RFID Tech.*, Oct. 2015, pp. 94–97.

[36] L. Gortschacher *et al.*, "SDR based RFID reader for passive tag localization using phase difference of arrival techniques," in *2016 IEEE MTT-S Int. Mic. Symp.*, May 2016, pp. 1–4.

[37] A. J. S. Boaventura *et al.*, "The design of a high-performance multisine RFID reader," *IEEE Trans. Microwave Theory and Tech*, vol. 65, pp. 3389–3400, Sep. 2017.

[38] A. Boaventura, J. Santos, A. Oliveira, and N. B. Carvalho, "Perfect isolation: Dealing with self-jamming in passive RFID systems," *IEEE Microw. Mag.*, vol. 17, no. 11, pp. 20–39, 2016.

[39] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in *Proceedings of the 17th annual international conference on Mobile computing and networking*. ACM, 2011, pp. 301–312.

[40] P. V. Nikitin and K. Rao, "Performance limitations of passive UHF RFID systems," in *IEEE Antennas and Propagation Society International Symposium*, vol. 1011, 2006.

[41] J. D. Griffin and G. D. Durgin, "Complete link budgets for backscatter-radio and RFID systems," *IEEE Antennas Propag. Mag.*, vol. 51, no. 2, pp. 11–25, 2009.

[42] J. Rozman, M. Atanasijevic-Kunc, and V. Kunc, "Noise analysis of the UHF RFID system," *Analog Integrated Circuits and Signal Processing*, vol. 74, no. 3, pp. 591–598, 2013.

[43] Z. M. Bakir and H. M. AlSabbagh, "Limitations of forward and return links in UHF RFID with passive tags," *Int. Journal of Enineering Trends and Tech. (IJETT)*, vol. 5, no. 5, pp. 238–242, Nov. 2013.

[44] "Electronic code of federal regulations, title 47, part 15 §15.247," online, Sep. 2019.

[45] H. Yoon and B.-J. Jang, "Link budget calculation for UHF RFID systems," *Microwave Journal*, vol. 51, no. 12, pp. 64–74, Dec. 2008.

[46] G. D. Durgin, C. R. Valenta, M. B. Akbar, M. M. Morys, B. R. Marshall, and Y. Lu, "Modulation and sensitivity limits for backscatter receivers," in *IEEE Int. Conf. on RFID*. IEEE, 2013, pp. 124–130.

[47] G. Lasser and C. F. Mecklenbräuker, "Self-interference noise limitations of rfid readers," in *2015 IEEE International Conference on RFID (RFID)*. IEEE, 2015, pp. 145–150.

[48] G. De Vita and G. Iannaccone, "Design criteria for the rf section of uhf and microwave passive RFID transponders," *IEEE Trans. Microw. Theory Tech.*, vol. 53, no. 9, pp. 2978–2990, 2005.

[49] J.-H. Bae, J.-C. Kim, B.-W. Jeon, J.-W. Jung, J.-S. Park, B.-J. Jang, H.-R. Oh, Y.-J. Moon, and Y.-R. Seong, "Analysis of phase noise requirements on local oscillator for RFID system considering range correlation," in *2007 European Radar Conference*. IEEE, 2007, pp. 385–388.

[50] *Monza 5 Tag Chip Datasheet*, Impinj, Inc., Aug. 2016, version 3.0.

[51] R. Langwieser, C. Angerer, A. L. Scholtz, and M. Rupp, "Crosstalk and SNR measurements using a multi-antenna RFID reader with active carrier compensation," in *Proc. of the Third International EURASIP Workshop on RFID Technology*, 2010.

[52] NXP Semiconductors, *SL3S1204 UCODE7*, rev. 3.3 ed., Dec. 2013.

[53] L. W. Mayer and A. L. Scholtz, "Circularly polarized patch antenna with high Tx / Rx-separation," in *IEEE International Conference on RFID*, Orlando, USA, Apr. 2009, pp. 213–216.

[54] E. A. Etellisi, M. A. Elmansouri, and D. S. Filipovic, "Wideband monostatic simultaneous transmit and receive (STAR) antenna," *IEEE Trans. Antennas Propag.*, vol. 64, no. 1, pp. 6–15, 2015.

[55] W.-G. Lim, W.-I. Son, K. S. Oh, W.-K. Kim, and J.-W. Yu, "Compact integrated antenna with circulator for UHF RFID system," *IEEE Antennas Wireless Propag. Lett.*, vol. 7, pp. 673–675, 2008.

[56] W.-G. Lim, S.-Y. Park, W.-I. Son, M.-Q. Lee, and J.-W. Yu, "RFID reader front-end having robust Tx leakage canceller for load variation," *IEEE Trans. Microw. Theory Tech.*, vol. 57, no. 5, pp. 1348–1355, 2009.

[57] S. Padhi, N. Karmakar, C. Law, and S. Aditya, "A dual polarized aperture coupled microstrip patch antenna with high isolation for RFID applications," in *IEEE Antennas and Propagation Society International Symposium. 2001 Digest. Held in conjunction with: USNC/URSI National Radio Science Meeting (Cat. No. 01CH37229)*, vol. 2. IEEE, 2001, pp. 2–5.

[58] S. Padhi, N. Karmakar, and C. Law, "Dual polarized reader antenna array for RFID application," in *IEEE Antennas and Propagation Society International Symposium. Digest. Held in conjunction with: USNC/CNC/URSI North American Radio Sci. Meeting (Cat. No. 03CH37450)*, vol. 4. IEEE, 2003, pp. 265–268.

[59] J.-S. Kim, K.-H. Shin, S.-M. Park, W.-K. Choi, and N.-S. Seong, "Polarization and space diversity antenna using inverted-f antennas for RFID reader applications," *IEEE Antennas Wireless Propag. Lett.*, vol. 5, pp. 265–268, 2006.

[60] H.-W. Son, J.-N. Lee, and G.-Y. Choi, "Design of compact RFID reader antenna with high transmit/receive isolation," *Microwave and Optical Technology Letters*, vol. 48, no. 12, pp. 2478–2481, 2006.

[61] X.-Z. Lai, Z.-M. Xie, Q.-Q. Xie, and X.-L. Cen, "A dual circularly polarized RFID reader antenna with wideband isolation," *IEEE Antennas Wireless Propag. Lett.*, vol. 12, pp. 1630–1633, 2013.

[62] G. Lasser, R. Langwieser, and A. L. Scholtz, "Broadband suppression properties of active leaking carrier cancellers," in *IEEE Int. Conf. on RFID*, Orlando, USA, April 2009.

[63] Impinj, Inc., *Indy® R2000 Reader Chip (IPJ-R2000)*, rev. 1.3 ed., Jul. 2012.

[64] I. Mayordomo *et al.*, "Implementation of an adaptive leakage cancellation control for passive UHF RFID readers," in *Proc. IEEE Int. Conf. RFID*, Apr. 2011, pp. 121–127.

[65] E. A. Keehr, "A low-cost, high-speed, high resolution, adaptively tunable microwave network for an SDR UHF RFID reader reflected power canceller," in *Proc. IEEE Int. Conf. RFID*, Apr. 2018, pp. 1–8.

[66] G. Lasser, R. Langwieser, and C. F. Mecklenbräuker, "Automatic leaking carrier canceller adjustment techniques," *EURASIP Journal on Embedded Systems*, vol. 2013, no. 1, 2013. [Online]. Available: http://dx.doi.org/10.1186/1687-3963-2013-8

[67] S. Maddio, A. Cidronali, and G. Manes, "Real-time adaptive transmitter leakage cancelling in 5.8-ghz full-duplex transceivers," *IEEE Trans. Microw. Theory Tech.*, vol. 63, no. 2, pp. 509–519, 2015.

[68] P. Pursula, M. Kiviranta, and H. Seppä, "UHF RFID reader with reflected power canceller," *IEEE Microw. Wireless Compon. Lett.*, vol. 19, no. 1, pp. 48–50, Jan. 2009.

[69] S. Kim, Y. Jeon, G. Noh, Y.-O. Park, I. Kim, and H. Shin, "A 2.59-GHz RF self-interference cancellation circuit with wide dynamic range for in-band full-duplex radio," in *2016 IEEE MTT-S International Microwave Symposium (IMS)*. IEEE, 2016, pp. 1–4.

[70] S. Chiu *et al.*, "A 900 MHz UHF RFID reader transceiver IC," *IEEE J. Solid-State Circuits*, vol. 42, pp. 2822–2833, Dec. 2007.

[71] J.-W. Jung *et al.*, "TX leakage cancellation via a micro controller and high TX-to-RX isolations covering a UHF RFID frequency band of 908-914MHz," *IEEE Microwave and Wireless Comp. Letters*, vol. 18, pp. 710–712, Oct. 2008.

[72] D. P. Villame *et al.*, "Carrier suppression locked loop mechanism for UHF RFID readers," in *Proc. IEEE Int. Conf. RFID*, Apr. 2010, pp. 141–145.

[73] K. Kapucu *et al.*, "A fast active leakage cancellation method for UHF RFID readers," in *Proc. IEEE Int. Conf. RFID*, May 2017, pp. 182–186.

[74] P. Beasley, A. Stove, B. J. Reits, and B. As, "Solving the problems of a single antenna frequency modulated CW radar," in *Proc. IEEE Radar Conf.*, 1990, pp. 391–395.

[75] W.-K. Kim *et al.*, "A passive circulator for RFID application with high isolation using a directional coupler," in *Proc. 2006 European Microwave Conference*, Sep. 2006, pp. 196–199.

[76] T. Brauner and X. Zhao, "A novel carrier suppression method for RFID," *IEEE Mic. and Wireless Comp. Letters*, vol. 19, pp. 128–130, Mar. 2009.

[77] M. Koller and R. Kung, "Adaptive carrier suppression for UHF RFID using digitally tunable capacitors," in *2013 European Microwave Conference*, Oct. 2013, pp. 943–946.

[78] R. Whatley *et al.*, "CMOS based tunable matching networks for cellular handset application," in *Proc. IEEE Intl. Micr. Symp.*, Jun. 2011, pp. 1–4.

[79] O. J. Zobel, "Theory and design of uniform and composite electric wave-filters," *Bell Sys. Tech. J.*, vol. 2, pp. 1–46, Jan. 1923.

[80] *Gen2 - Save Power and Cost: AS3980 - Low Cost UHF Reader IC*, ams AG, Dec. 2013.

[81] *UHF RFID Single Chip Reader EPC Class1 Gen2*, ams AG, Jul. 2015, version 1-00 Short Datasheet.

[82] "Development with GCC and Eclipse," https://devzone.nordicsemi.com/nordic/nordic-blog/b/blog/posts/development-with-gcc-and-eclipse, accessed: 2019-08-19.