

How to Build a Low-Cost, Extended-Range RFID Skimmer

Ilan Kirschenbaum* Avishai Wool†

Abstract

Radio-Frequency Identifier (RFID) technology, using the ISO-14443 standard, is becoming increasingly popular, with applications like credit-cards, national-ID cards, E-passports, and physical access control. The security of such applications is clearly critical. A key feature of RFID-based systems is their very short range: Typical systems are designed to operate at a range of 5-10cm. Despite this very short nominal range, Kfir and Wool predicted that a rogue device can communicate with an ISO-14443 RFID tag from a distance of 40-50cm, based on modeling and simulations. Moreover, they claimed that such a device can be made portable, with low power requirements, and can be built very cheaply. Such a device can be used as a stand-alone RFID skimmer, to surreptitiously read the contents of simple RFID tags. The same device can be as the “leech” part of a relay-attack system, by which an attacker can make purchases using a victim’s RFID-enhanced credit card—despite any cryptographic protocols that may be used.

In this study we show that the modeling predictions are quite accurate. We show how to build a portable, extended-range RFID skimmer, using only electronics hobbyist supplies and tools. Our skimmer is able to read ISO-14443 tags from a distance of ≈ 25 cm, uses a lightweight 40cm-diameter copper-tube antenna, is powered by a 12V battery—and requires a budget of $\approx \$100$. We believe that, with some more effort, we can reach ranges of ≈ 35 cm, using the same skills, tools, and budget.

We conclude that (a) ISO-14443 RFID tags can be skimmed from a distance that does not require the attacker to touch the victim; (b) Simple RFID tags, that re-

spond to any reader, are immediately vulnerable to skimming; and (c) We are about half-way toward a full-blown implementation of a relay-attack.

1 Introduction

1.1 Background

Radio Frequency Identification (RFID) technology, using the ISO-14443 standard [ISO00], is rapidly becoming widely adopted by many governmental, industrial and commercial bodies. Typical applications include contactless credit-cards, national-ID cards, E-passports, and physical access control (cf. [Fin03], [GSA04]). The security of such applications is clearly critical.

A key security feature of RFID-based systems is their very short range: ISO-14443 systems are designed to operate at a range of 5-10cm. Thus, the perception is that the RFID tag (or smartcard) must almost touch the RFID reader, which should imply that the tag’s owner is physically present and holding the tag. Unfortunately, this perception is incorrect. Recently, Kfir and Wool [KW05] described a relay-attack on RFID systems, that violates the implication that the tag being read is in fact near the RFID reader. Their system architecture involves two devices, a “leech” and a “ghost”, that communicate with each other (see Figure 1). Such a system would, for instance, allow an attacker to make purchases using a victim’s RFID-enhanced credit card—despite any cryptographic protocols that may be used.

As part of their work, [KW05] predicted that the rogue “leech” device can communicate with an ISO-14443 RFID tag from a distance of 40-50cm, based on modeling and simulations. Moreover, they claimed that such a device can be made portable, with low power requirements, and can be built very cheaply. However, beyond acting as a component in a relay-attack, a “leech” can also be used as a stand-alone RFID skimmer, to surreptitiously read the contents of simple RFID tags. Our goal

*Ilan Kirschenbaum is with the School of Electrical Engineering Systems, Tel Aviv University, Ramat Aviv 69978, ISRAEL E-mail: ilankir@gmail.com.

†Avishai Wool is with the School of Electrical Engineering Systems, Tel Aviv University, Ramat Aviv 69978, ISRAEL E-mail: yash@acm.org.

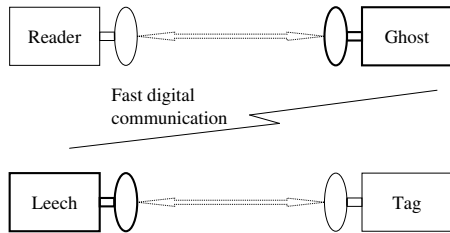


Figure 1: Relay attack system overview.

in this work was to actually build such a skimmer.

1.2 Related work

1.2.1 Attacks on RFID Systems Using the ISO-14443 Standard

The starting point of our work is [KW05]. Their analysis predicts that an RFID tag can be read by the “leech” from a range of tens of centimeters, much further than the nominal ISO-14443 range of 5-10 cm. They also claimed that the “ghost” device can communicate with the reader from distance of tens of meters. [KW05] presented several variants of possible relay-attack implementations, with different costs and required personnel skills. In this work we validate their claims about the practicality of the leech device.

Another part of the relay attack against ISO 14443A RFID systems was implemented by Hancke [Han05]: He implemented the fast digital communication between the leech and the ghost (see Figure 1), while using standard (nominal range) devices for the leech and ghost themselves. His system used cheap radios, and achieved a range of 50 meters between the reader+ghost and the leech+tag. His work demonstrates that the range between the victim tag and the reader is limited only by the technology used for leech-ghost communication. To counter the relay attack, [HK05] have designed a distance-bounding protocol, which requires ultra-wide-band communication.

In a widely reported work, Finke and Kelter [FK05]) managed to *eavesdrop* on the communication between an ISO-14443 RFID reader and a tag. They attached the tag directly to a reader (at zero distance), and showed that the combined communication between the reader and tag can be read from 1-2 meters by large loop antenna located on the same plane of the reader and the tag. Note that this is quite different from the challenges facing a skimmer: (a) The skimmer must be close enough to the tag, and produce a strong enough magnetic field, to power the tag (i.e., the tag must be within “activation range”); (b) A skimmer cannot rely on a legitimate reader’s strong signal being modulated by the tag. Nev-

ertheless, [FK05] shows that the eavesdropping range on RFID communication is a much greater than skimming range—and we show that skimming range is much greater than the nominal read range.

1.2.2 Attacks on RFID Systems Using Other Standards

There are many RFID systems that do not use the ISO-14443 standard. Typically, such systems are designed for larger read-ranges, but provide much more limited capabilities than ISO-14443: they are unable to power a programmable smartcard processor, and usually only contain fixed logic circuitry or even just a short piece of data, much like a magnetic-stripe card. Over the last 2 years, several attacks have been reported against some of these systems.

In a very widely reported event [Kre05, Sch05], a group from Flexilis claimed to set new world record of passively reading an RFID tag from 69 feet at Def-Con’05. However, the RFID technology used for this experiment was not ISO-14443, but a UHF-based technology in the frequency range of 800 MHz to 2.5 GHz which is designed for a much larger read range.

A German hacker ([Hes04]) used a simple PDA, equipped with an RFID read/write device, and changed product prices in a grocery shop using a software he wrote. He managed to reduce the Shampoo price from \$7 to \$3 and go through the cashier without incident. Supermarket checkout trials held by NCR corporation showed that some clients standing at the cashier paid for groceries held by clients standing behind them in the queue [Whi05].

A research team in Johns Hopkins University ([BGS⁺05]) managed to build a system that sniffs information from RFID-based car keys and immobilizers, and were able to purchase gasoline without the owners consent.

A research group in MIT ([Lin05]) designed and implemented an RFID field probe that can sense RFID magnetic fields from up to 4 meters. However, it is designed to sense magnetic fields of frequencies between 900 to 950 MHz, which are very different from the 13.56 MHz of the ISO 14443 standard.

1.2.3 RFID Systems and Protocols in General

A broad overview of RFID technology can be found in T.A.Scharfeld’s thesis [Sch01]. This thesis analyzes RFID theory, standards, regulations, environment influence, and implementation issues.

Free attack/analysis tools that detect RFID cards and show their meta information are available from the RF-Dump web site [GW04]. These tools are able to display

and modify the card data, such as the card ID, card type, manufacturer etc.

Juels, Rivest and Szydlo [JRS03] propose a blocking tag approach that prevents the reader from connecting with the RFID tag. Their method can also be used as malicious tool: In order to disrupt the Reader-to-Tag communication, their blocker tag actually performs a denial-of-service attack against the RFID reader protocol by using the “Tree-Walking Singulation Algorithm” in the anti-collision mechanism. Juels and Brainard [JB04] propose a variant on the blocker concept which involves software modification to achieve a soft blocking tag.

[Wei03] and [SWE02] offer a “Hash-Lock” approach to low cost RFID devices which use a “lock/unlock” mechanism to protect against retrieving the RFID ID number. In the simplest scenario, when the tag is locked it is given a value (or meta-ID) y , and it is only unlocked by presentation of a key value x such that $y = h(x)$ for a standard one-way hash function h .

[RCT05] describe a portable device, called an RFID Guardian, that is supposed to cover a whole individual’s surrounding, to communicate with the various tags in the person’s possession, and protect the person from potentially hostile RFID fields. The RFID Guardian is supposed to be able to cover a range of 1-2 meters, however, the authors do not describe the RFID Guardian implementation, and it is unclear how it overcomes the physical limitations of the claimed range.

1.3 Contribution

In this study we show that the modeling predictions of [KW05] are quite accurate. We managed to build a portable, extended-range RFID skimmer, using only electronics hobbyist supplies and tools. Our skimmer is able to read ISO-14443 tags from a distance of ≈ 25 cm, uses a lightweight 40cm-diameter copper-tube antenna, is powered by a 12V battery—and requires a budget of $\approx \$100$.

Beyond validating the theoretical modeling, we believe that our design, implementation and tuning processes are of independent interest: Most circuit designs and application notes are written for well equipped RF labs, and we needed to modify them or design our own to meet our ridiculously low budget. In particular, our experience shows that the standard RFID tuning process, described in ISO 10373-6 ([ISO01], is inappropriate for hobbyist workshops, and may be missing some key details that are necessary to make it work. Instead, we describe several tuning processes that do work reliably, even in low-budget environments.

We conclude that (a) ISO-14443 RFID tags can be skimmed from a distance that does not require the attacker to touch the victim; (b) Simple RFID tags, that re-

spond to any reader, are immediately vulnerable to skimming; and (c) We are about half-way toward a full-blown implementation of the relay-attack predicted by [KW05].

Organization: Section 2 describes our skimmer system’s design. Section 3 describes our construction techniques. Section 4 details the tuning methods we experimented with. Section 5 describes the skimmer’s actual performance, and we conclude with Section 6. Additional details can be found in an appendix.

2 System Design

RFID systems that are based on the ISO-14443 standard operate with a 13.56 MHz center frequency, which mandates RF design methods. The system units should be matched for maximal power transfer and efficiency, and the whole system should have an excellent noise figure to improve the receiving and discrimination circuits sensitivity, which in turn allows a large read range.

2.1 Design Paradigms

Our assumption is that we are constructing an ad-hoc system for attack purposes, and mass production is not involved. Therefore modular design and perfect implementation are not the main design goals. Instead, we focused on quick, simple, and cheap methods.

There are two design paradigms that can be followed; the “normal” paradigm is to design all the system sub-units to have a uniform 50Ω input and output impedance. The other paradigm is to design and implement a proprietary RF system, with non-standard characteristics.

The advantages of using standard design include the variety of ready-to-use designs, applications notes, and test equipment. The resulting system is scalable, versatile, and modular. However, the need for accurate design, dealing with accurate filters and semiconductor’s min-max parameters and ratings, stretches the design and implementation time, and may cause long and tedious system testing and tuning.

In contrast, designing a proprietary, non-standard interface systems has some practical advantages. First, accuracy is no longer mandatory. Second, the system can work in its natural output and input characteristics without the need to adjust its interfaces to standard characteristics, that might need extra matching networks and components. In particular, some amplifier designs have an output impedance that differs from 50Ω , and their designated antennas’ impedance is closer to the amplifier’s impedance than to 50Ω . In this case, there is no sense to adjust both amplifier output and antenna input to 50Ω .

Since our goal was to emulate a hacker, we chose to follow the proprietary design paradigm. We used 50Ω

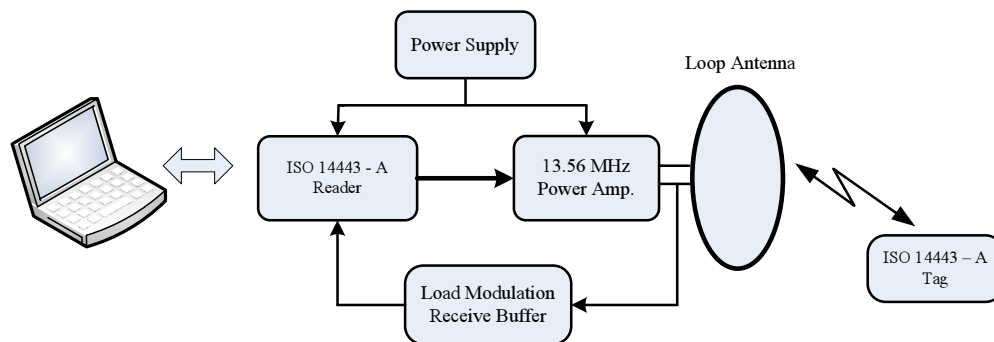


Figure 2: Extended Range RFID Skimmer.

designs where they suited our needs, but we did not attempt to tune all the sub-units precisely. As we shall see, the results were quite satisfactory, despite the very basic work environment and tools.

2.2 System Units

The skimmer is comprised of 5 basic units (see Figure 2): A reader, a power amplifier, a receive buffer, an antenna and a power supply. The RFID reader generates all the necessary RF signals according to the ISO 14443 type A protocol. These signals are amplified by the power amplifier to generate the RF power which is radiated through the loop antenna. The loop antenna performs the interaction with the ISO 14443 RFID tag, and senses the load modulation signals. These signals are buffered by the Load Modulation Receive Buffer and fed back to the reader detection input. The Reader communicates with a host system via an RS232 serial interface. Typically, the host is a computer, however, it can also be a small microcontroller based card, with some non-volatile memory that collects and stores skimmed data.

Our main objective was to increase the output power and antenna size as these two factors directly influence the reading range.

2.3 The RFID Reader

The RFID reader module we used was the Texas Instrument (TI) S4100 Multi-Function reader module, [TI03]. The module can be purchased alone for around \$60, and the TI web site ([TI05]) contains sufficient documentation for designing and programming this module. The S4100 module has a built in RF power amplifier that can drive approximately 200 mW into a small antenna. The TI module supports several RFID standards. We focused on the ISO 14443 Type A standard, that is used in contactless smartcards and E-passports.

In addition to the basic S4100 module, we purchased the RX-MFR-RLNK-00 Texas Instrument Multi-Function Reader evaluation kit. The evaluation kit costs \$650 and contains a complete ready-to-use reader, which is built around the S4100 module. The kit includes a small built-in 8.5 cm loop antenna and is assembled in a plastic box. It is supplied with basic demo software, various tags for its supported protocols, documentation and references. The kit has an RS232 serial port for interfacing a host computer. We measured a reading range of 6.5 cm using its built in antenna.

Although we could have used the (dismantled) evaluation kit's main board for our experimentation, we chose to build our own base board to demonstrate that buying the evaluation kit is not required. We followed the Interface Circuitry design suggested by TI ([TI03]), but omitted the Low Frequency LED driver. We could have omitted the RS232 level shifters and use TTL levels for the serial port communication, however, the skimmer is supposed to work near the antenna, and to be exposed to strong and noisy electro-magnetic fields, therefore we included common RS232 level shifters in our base board design. This design requires a 5 volts power supply. See Section 2.7 for power supply design and description.

2.4 Antennas

A necessary condition for an increased range is a larger antenna. Theoretical analysis ([Lee03]) shows that for a desired range, r , the optimal antenna diameter is $\approx r$. We wanted to demonstrate a reading range of 25-30 cm.

TI's RFID Web site [TI04] supplies an antenna cookbook for building various kinds of antennas for different reading ranges and purposes. As a first experiment, we used a printed PCB 10×15 cm rectangular antenna design found in the cookbook. We later used it as a tuning aid for tuning the system, as described in Section 4. Figure 4 shows the PCB antenna's matching circuit.

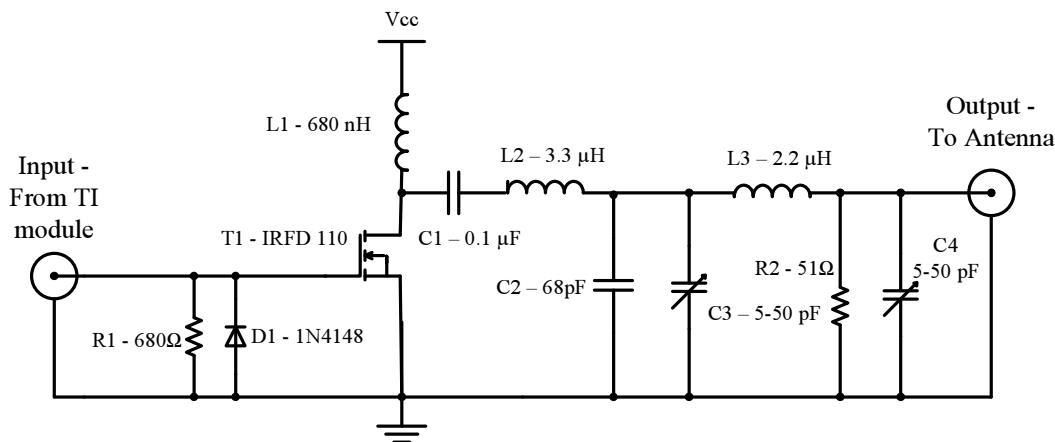


Figure 3: The 13.56 MHz Power Amplifier.

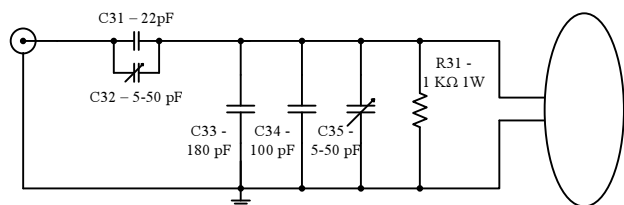


Figure 4: The PCB Antenna 50 Ω Matching Circuit.

For our larger, high power antenna, we constructed a 39 cm copper tube loop antenna. The basic design for the loop antenna's matching network was taken from the PCB antenna (Figure 4), subject to minor changes: Specifically, the resonance parallel capacitors C33 and C34 that were merged into one capacitor of 82 pF, since the calculated antenna's inductance was around 1 μH.

2.5 Power Amplifier

We based our power amplifier on [Me104], and modified it to suit our unit's interface. The scheme of the power amplifier we designed appears in Figure 3. We interfaced the power amplifier directly to the TI module's output stage embedded in the skimmer base board. However, we did not match impedances between the two since we did not have to transfer power to the power amplifier, but only drive its input for biasing the power FET by a sufficient voltage swing.

2.6 The Load Modulation Receive Buffer

The TI S4100 module is designed around the S6700 Multi-Protocol Transceiver IC, an integrated HF reader

system that contains all the high frequency circuitry comprising an Analog Front End (AFE) that decodes the ISO standards protocols. The S6700 has a Receiver input, which is directly connected to the reader's antenna.

This receiver input is unable to handle the voltage levels that are developed on our large loop antenna: During the system development process we measured 184 volts over the antenna with a supply voltage of 17.1 volts. In order to keep the reader from potential damage, and still deliver the load modulation signals to the reader's receiver input, we had to attenuate the antenna signals before feeding them back to the TI module. A simple resistor attenuation network is not suitable since it dramatically influences the antenna's resonance circuit quality factor, Q . Therefore, we chose to use an attenuating buffer (See Figure 5). The buffer was designed using a high impedance RF FET (T2 in Figure 5), in order to keep the antenna's quality factor as designed. The buffer was attached to the antenna and to the TI module via a direct coupling connection, in order to reduce the signal phase shifting to minimum. The C21 variable capacitor is used to compensate for the parasitic capacitance introduced by the T2 FET.

2.7 The Power Supply

In order to drive the large loop antenna, we needed to provide a power supply.

For lab work, we used a stabilized external power supply. Note that the base board that embeds the TI module contains a voltage regulator, therefore the external power supply unit does not have to be regulated. Nevertheless, we used a regulated power supply to reduce its noise figure. Figure 6 shows the regulation and filtering circuitry which we placed on the base board and on the power am-

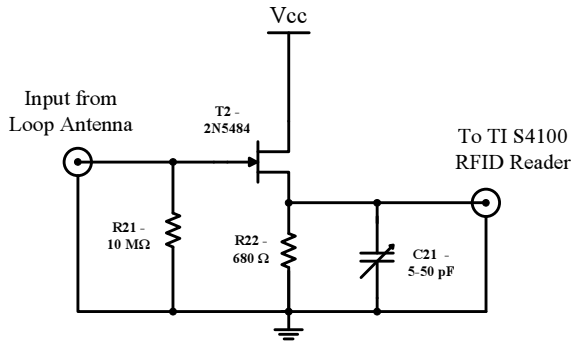


Figure 5: The Load Modulation Receive Path buffer.

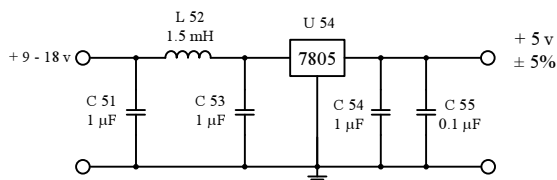


Figure 6: Power supply filter for the reader base board and the power amplifier.

plifier board.

The role of L52 in Figure 6 is to maintain clean and low ripple levels on the DC supply in order to keep a low noise figure of the DC supply voltage. Since the DC supply voltage reaches all the internal chips circuitry, having clean DC voltage to the internal load modulation signals detection circuitry can improve detection range.

To demonstrate the skimmer’s mobility, we also operated it using a Non-Spillable 7 AH Zinc-Lead rechargeable battery used in home security systems. It has a 12 volts nominal voltage level, is very common and can be purchased in any home security system store. An added bonus of using a non-switched DC power supply is that it eliminates any switching noise.

3 System Building

3.1 Printing a PCB Antenna

Our first choice was to build a home made 10×15 cm PCB RFID antenna which is fully specified in the TI antenna cookbook. To demonstrate the low-tech requirements, we manufactured this antenna in our hobby workshop. Appendix A describes the PCB printing process.

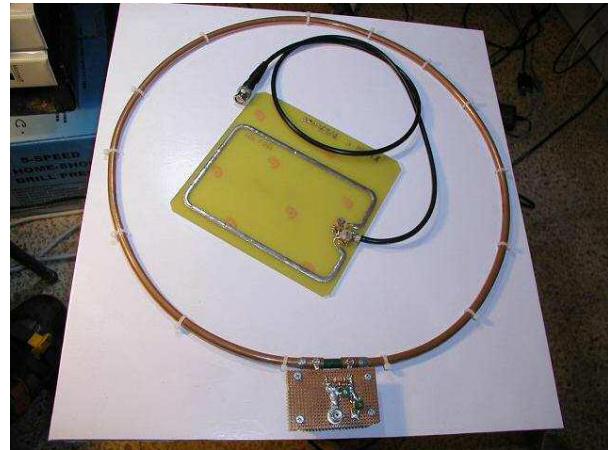


Figure 7: The copper-tube loop antenna and the PCB Antenna.

3.2 Building a Copper Tube Loop Antenna

The TI cookbook describes a design for a square 40×40 cm copper-tube antenna, which seemed appropriate. However, we chose not to construct it precisely, since cheap copper tube (for cooking gas) is sold packed in circular coils, and constructing an antenna with a square or rectangle shape requires straightening the tube, and requires additional 90 degrees matching adapters, which increase the antenna’s cost. Instead, we designed our own circular antenna, which has similar characteristics to the TI cookbook antenna.

We built the loop antenna from 5/16 inch cooking gas copper tube. The tube is tied to a solid non flexible wooden tablet, in order to maintain its shape and to avoid inductance changes under mechanical deformation forces.

The loop antenna construction process was basically mechanical handcraft work, requiring no special equipment beyond basic amateur’s electrical tools. Note that copper tube must be soldered using at least a 100-watts blow torch. Figure 7 shows the finished copper tube antenna and the PCB antenna.

3.3 Building the RFID Base Board

According to the interfacing information we found in the S4100 module datasheet, we designed a small PCB base board, having the S4100 module as a Piggy Back.

We manufactured the RFID base board PCB using a different method than we used to make the PCB antenna. For this board, we used a Decon DALO 33 Blue PC Etch protected ink pen to draw the leads on the Glass-Epoxy tablet. This technique allowed us to print the PCB during any time of day, without the need to wait for the sun. See

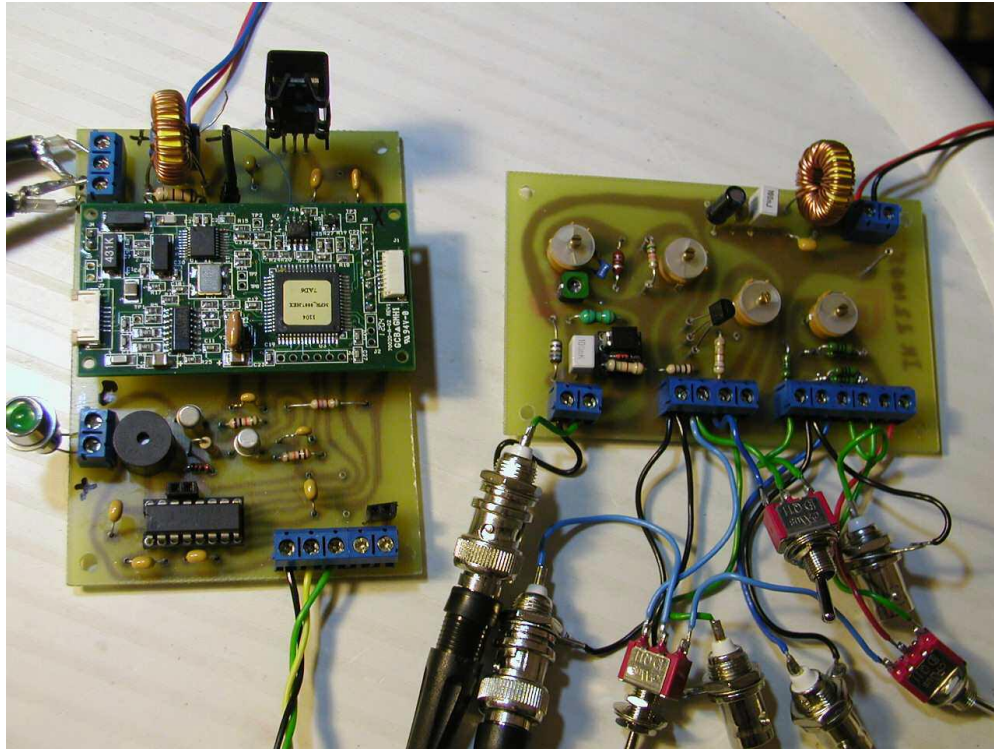


Figure 8: The TI S4100 module mounted on our base board on the left, and the power amplifier board on the right.

Figure 8 for a picture of the base board.

3.4 Building the Power Amplifier

As we noted in Section 2.5, the power amplifier design is based on a Melexis application note ([Mel04]), recall Figure 3. We used the output stage of the TI S4100 reader module in the base board to drive the power amplifier input. We did not invest any effort in impedance matching since the power amplifier input is voltage driven. We manufactured the PCB for the power amplifier using the same technique as used for the base board, and with the same low cost DC ripple filter (recall Figure 6) to maintain a low noise figure.

Beyond the Melexis design, empirical results led us to connect a filter comprised of R2 and C4 at the output (See Figure 3). This filter reduces the Q of the output impedance matching filter, enabling fine tuning of the output signal phase. We discovered that the filter increased the read range significantly.

The output voltage amplitude of the power amplifier varies depending on the power supply voltage. For instance, with a 17.1 volts power supply we measured over 180 volts on the resonance circuit and the antenna. Therefore, ideally, high voltage rating capacitors, and high current rating inductors should be used. We used

regular, but easy to obtain, passive components, and managed to burn quite a few during our experimentation.

3.5 Building the Load Modulation Receive Path Buffer

As we mentioned before, the high voltage swing on an antenna driven by the power amplifier must be attenuated in order to supply the correct samples of the RF received signal back to receive input of the S4100 module. Therefore, we needed to build the buffer described in Section 2.6. We placed the buffer's circuitry on the same PCB that housed the power amplifier - see Figure 8.

One challenge we had to deal with is that the TI S4100 module is designed to work with a low power antenna, and includes an attenuation resistor that is suitable for such an antenna. In order to provide our (attenuated) signals to the S4100, we had to solder the buffer's output directly into the S4100 module, bypassing the original attenuation resistor. Figure 9 shows the bypass.

4 System Tuning

A crucial implementation phase is system tuning and adjustment. Specifically, we have to tune the various reso-

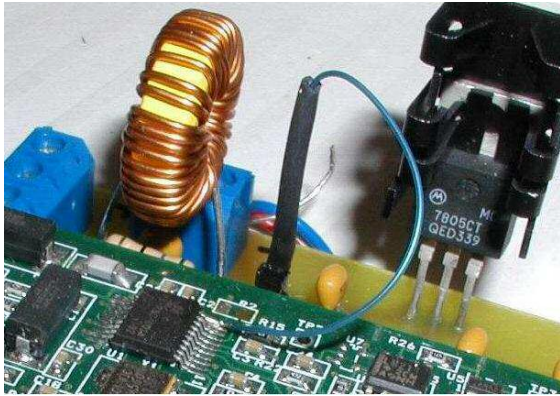


Figure 9: The direct connection to the TI module, by-passing the existing attenuation resistor.

nance circuits and matching networks for maximal power transfer. The only test equipment we used throughout the entire project was cheap 60 MHz oscilloscope, that any electronic hobbyist has in his workshop. Note that while resonance frequency can be tuned using an oscilloscope, matching the antenna to the amplifier requires a different procedure since both a magnitude and a phase must be matched.

4.1 Standard Tuning Methods

We say that a tuning method is “standard” if it requires a $50\ \Omega$ design.

The first and most straightforward tuning method is to use an RF network analyzer. Among its various features, a network analyzer can measure the magnitude and phase of a system input, allowing us to know exactly what matching network to connect to this system in order to match it to the desired impedance. In our case, a network analyzer can measure the antenna input impedance, e.g., its phase and magnitude, which would enable us to calculate the matching circuitry for $50\ \Omega$ input impedance. In case we already have a matching network, the RF network analyzer can measure the return loss and let us tune the system to minimum returned power. Unfortunately, an RF network analyzer costs over \$10,000, well beyond the budget of an amateur.

Another tuning method is to measure the Voltage Standing Wave Ratio (VSWR), and to adjust the antenna’s impedance to be best matched to the driving amplifier output stage by tuning the returned power to the desired value ([Poz05]). This method requires a VSWR meter, which costs several hundred US\$: still beyond a typical hobbyist budget. A cheap way to measure the VSWR (without a VSWR meter) is to use directional couplers, that cost between \$20–\$70, but their input and

output impedance is $50\ \Omega$, requiring $50\ \Omega$ interface sub-systems design. We have not attempted this method.

Finally, one can tune the system using an RF watt-meter, or an RF power meter. These instruments sense the RF power and translate the sensor’s measurement to a standard scale. The sensor can be based on a diode, or on a bolometer: an RF power sensor whose operation is based on sensing purely resistive element radiation. This method is a second-order-effect tuning since it measures the antenna power reception rather than the actual direct amplifier to antenna matching. This kind of equipment costs between \$300 (used) to \$600 for a simple watt-meter, including the sensor, to about \$3000 for an RF power meter that also features a VSWR meter and various other RF measurement capabilities.

4.1.1 The ISO 10373 Tuning Method

Since tuning the RFID receiver is a critical part of building such a device, Annex B of the ISO 10373-6 standard ([ISO01]) suggests a tuning process. This process seemed attractive since it only calls for low-cost components and uses basic oscilloscope capabilities. Therefore, despite the fact that ISO 10373 is a standard ($50\ \Omega$) tuning process, we invested a significant effort into trying to use it. Our experience leads us to conclude that the process is not very effective, at least for hobbyist setups.

The ISO 10373-6 testing configuration is based on monitoring a phase difference between the signal source and the load. The monitoring device utilizes a standard oscilloscope for displaying Lissajous figures in XY display mode, see Figure 10. If the time constant of the reference network equals the time constant of the network formed by the calibration resistor along with the oscilloscope Y probe’s parasitic capacitance, no phase difference should be monitored. If there is a difference in the two time constants, there will be a phase shift between the two probes of the oscilloscope, and the Lissajous figure should form an ellipse, whose main axis is at a 45-degree angle. The “fatness” of ellipse is related to the phase difference: when the system is perfectly tuned, there is no phase difference, and the Lissajous figure collapses to a straight line.

[ISO01] has two steps. The first step calibrates the test set to eliminate the oscilloscope input impedance from influencing the tuning step. In this step, the impedance matching network and the antenna of Figure 10 are replaced with a $50\ \Omega$ resistor to simulate $50\ \Omega$ load. The second step is the actual antenna tuning step. In this step, we replace the calibration resistor with the antenna containing the matching circuit, and trim the capacitors until we monitor that the Lissajous figure is closed, indicating a zero phase shift.

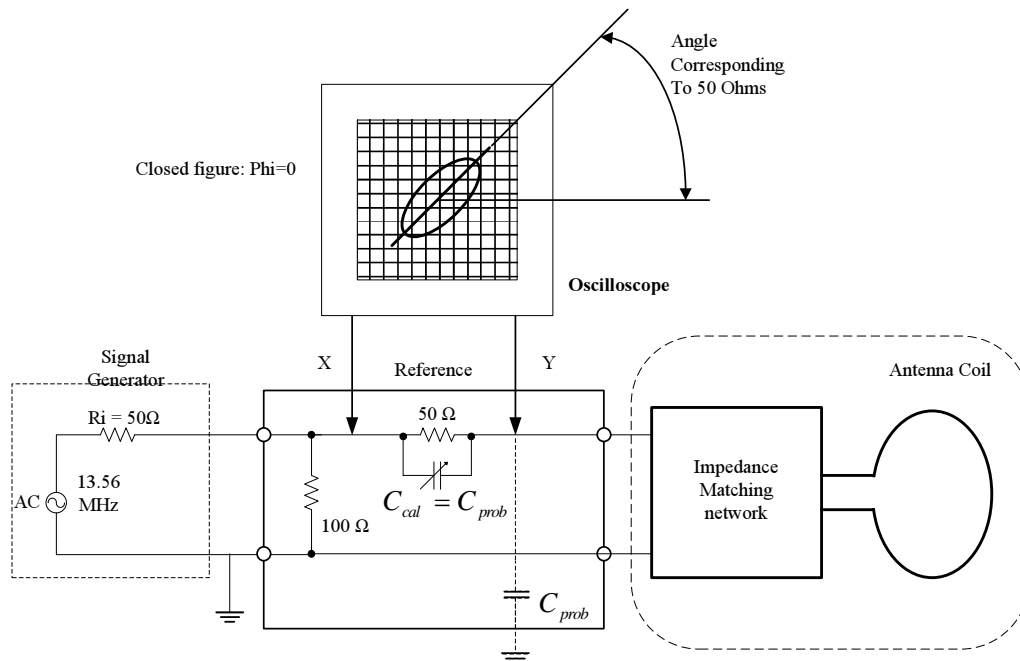


Figure 10: The ISO-10373 setting—Matching the antenna input impedance to 50 Ω . In the first step, the impedance matching network and the antenna are replaced with 50 Ω resistor to simulate 50 Ω load.

4.1.2 Problems with ISO 10373

Despite its apparent simplicity, in practice we discovered that the ISO 10373-6 tuning process has a few problems.

The first thing to note is that this tuning method requires a 13.56 MHz signal source, with a 50 Ω output impedance, that can deliver enough power to drive an antenna such as our copper tube antenna. We invested a significant effort trying to build a clean and accurate signal source, but this turned out to be difficult to do in reasonable time. Even obtaining an accurate 13.56 MHz crystal proved to be problematic—none of the electronics suppliers we contacted carried such a component. To bypass this obstacle, we decided to use the TI S4100 module itself as a signal source—since it is matched to 50 Ω and can drive sufficient power to the antenna. Once we did this, we were able to construct the rest of the circuitry, and we tried to tune the antenna.

Unfortunately, in all possible settings of the antenna’s matching circuitry, we did not manage to get the expected Lissajous figures. In some settings we got wavy figures implying a non linear circuit working point. In other settings we did not get the figures centered around the desired 45 degrees slope. Worst of all, we found no correlation between more closed Lissajous figures and longer read ranges (which we obtained using the methods of sections 4.2 and 4.3.

To our frustration, we found that ISO 10373-6 does not

specify the exact oscilloscope Volt per Division setting. This level of detail matters since we are dealing with very fine tuning, and human eye, oscilloscope line thickness and human judgment in conjunction with parallax error, can lead to errors. We speculate that if major RF labs indeed use this standard for tuning, they probably have some additional “secret sauce” that fills in the missing details.

One possible reason for our difficulties may be that we used the TI module as a signal source. This improvisation may have inserted some undesired harmonics due to the sidebands in the downlink signal spectrum, interfering with the tuning process. Since the methods described in Section 4.3 were effective, we did not pursue this further.

4.2 Non-Standard Tuning Methods

Instead of the standard 50 Ω tuning methods, we used the following two non-standard methods. We found that they both work reliably, and give satisfactory results.

One tuning method includes sensing the reception power using a small loop antenna as a sensor, leading its receptive power to a home-made RF power meter. The RF power meter can be an AM demodulator, whose DC level is proportional to the received RF power, or a home-made bolometer—we chose to use the latter.

The other non-standard method is a trial-and-error iterative process of reading an RFID tag at increasing distances, while tuning the matching circuitry, until a maximal range is reached.

4.3 Tuning Methods that Worked

The antenna has two tuning steps. The first is tuning the resonance frequency by trimming capacitor C35 in Figure 4. The second step is tuning the series capacitor C32 in Figure 4 to achieve maximal power transfer to the antenna. For tuning the resonance circuit we used the power amplifier's output signal, driven by the reader base board to tune center resonance frequency.

Then, for tuning the entire system, we used the iterations method described earlier. For this we used a Philips Mifare Standard IC tag. Initially, we located the tag at the basic range according to the RFID standard, and tuned the series antenna network capacitor C32 to some initial tag read. When an initial reading is observed, we know that the final position of C32 is near the position of the initial readout. We gradually increase the power supply, and each time adjust the various capacitors to get a stable reading range, while increasing the distance between the tag and the antenna. To hold the tag at a fixed distance we used non-ferromagnetic objects: most of the time we used a stack of disposable plastic cups, and for fine range measurements we used a small supply of 1-2mm thick beer coasters, see Figure 12. We stopped at a 19 volts power supply since the maximum semiconductor ratings were reached. Surprisingly, the variable capacitors survived the high swing voltage, which was more than 180 Volts.

During the iterations, a secondary source of tuning information was the sound level from the computer speakers. We turned the speakers to their maximum volume while we tuned the antenna matching capacitor: The tuning process caused the speakers to hum, and their loudness gave an idea how close we are to the final matching.

One disadvantage of this iterative method is its sensitivity to different tags: Some tags gave larger read ranges than others. On the other hand, the process is simple and quick: It took us approximately 10 minutes to tune the system to maximal performance.

A second tuning method that worked was based on a bolometer. We placed our smaller PCB antenna in the magnetic field produced by the large loop antenna, and measured changes in the RF power it was exposed to. Instead of purchasing an expensive industrial RF wattmeter or bolometer, we built our own: We attached a 100 K Ω thermistor to a 50 Ω resistor using super glue. To improve the bolometer performance, we increased its thermal conductivity by using a silicon thermal grease around the attaching surface between the resistor and the

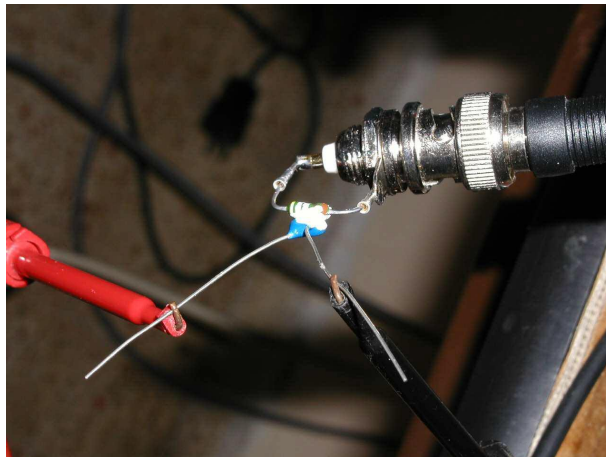


Figure 11: Home made bolometer using a resistor and a glued thermistor.

thermistor, see Figure 11. To keep it isolated from ambient temperature, we then covered it with a small piece of isolating PVC sleeve, used for thermal isolation of copper hot water pipes. Note that our bolometer is not calibrated to any standard units — but this is unimportant since all we care about is to reach a maximum value; we do not need to quantify the level of received RF power.

Using a binary search, while examining the amplitude over the antenna and reading the bolometer's resistance-temperature, we tuned the matching capacitor until we observed the maximum temperature. The results were accurate, and we reached the same final position of C32 that we marked at the end of iterations tuning process. This tuning method is independent of a particular tag—but it is slower, since it takes ≈ 15 seconds per setting for the thermistor to adjust to a new temperature and for the bolometer's reading to stabilize.

4.4 Miscellaneous Tuning Tips

4.4.1 Strong Magnetic Fields

Note that the antenna's magnetic field is so strong that it crashed one of the lab's computers even though it was approximately 1 meter away. We had to format the disk and re-install the OS and all applications.

4.4.2 Power Amplifier Tuning

The power amplifier has a simple tuning procedure. First, position the the C3 capacitor at its mid-point, and get a first readout from the tag. Then tune the antenna as described before. Finally, after tuning the antenna to maximal power matching, fine-tune C3 and attempt to increase the read range further.



Figure 12: The antenna tuning process. Note the tag placed over a stack of plastic cups and beer coasters in the center of the antenna. The power amplifier is marked as item 1, the reader base board is marked as item 2 and the battery is marked as item 3.

4.4.3 The Effect of a Battery Power Supply

During our lab work we used a linear stabilized power supply. We assumed that once we attach our system to a battery the reading range will grow because the battery delivers clean and ripple free voltage. However, in practice, we got only few millimeters improvement, if any. We believe that our linear power supply has quite a low noise figure so it gave us similar ranges to those achieved using a battery.

4.4.4 Surrounding Metal Objects

While tuning the antenna, care should be taken to remove any metal objects near the antenna. Reflections, grounded metal surfaces, and metal object permeability can influence the antenna's magnetic fields, leading to erroneous results. Even the human hands can influence the tuning results. To overcome these kinds of problems, we used only non ferromagnetic accessories, like a plastic table for laying the antenna, a wooden stick with the RFID tag attached to its edge for coarse range measurement, and plastic cups and coasters for fine range measurement.

5 Results

5.1 Achieved Read Ranges

Our reference system was the RX-MFR-RLNK-00 Texas Instrument Multi-Function Reader evaluation kit. The evaluation kit embeds the TI module we used, and comes with small 8.5 cm diameter round antenna directly connected to the module's output [TI05]. The basic read-range of the evaluation kit was 6.5 cm.

We first connected our 10×15 cm PCB antenna to the evaluation kit, without the power amplifier. This alone gave a range increase of 30%, to around 8.5 cm. Attaching the big loop antenna to the evaluation kit gave no results since the kit generates only 200 mW output power that is insufficient to drive the antenna.

Using the power amplifier we reached much larger ranges (see Figure 13). With the linear power supply providing 14.58 volts, we were able to read the tag at a range of 17.3 cm using the PCB antenna, and at a range of 25.2 cm using the copper tube antenna. With a 12-volt battery we reached a reading range of 23.2 cm using the copper tube antenna and 16.9 cm using the PCB antenna. Note that this type of battery, upon recharging, can sup-

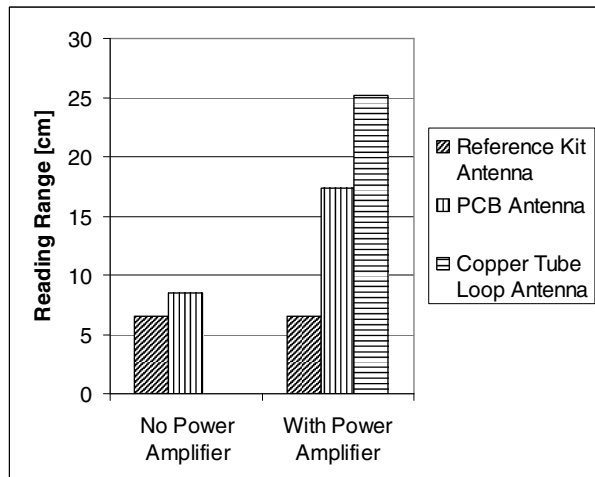


Figure 13: Skimmer read-range results with the reference kit antenna, PCB antenna, and the copper tube loop antenna, with and without the power amplifier.

ply more than its nominal voltage: we measured that it supplied 13.8 volts during the above experiments.

We observed that increasing the power supply voltage did not always cause a range increase: Higher power levels sometimes caused lower reception. This is in line with the predictions of [KW05]. The reason is that the distortion inserts harmonics that interfere with the detection of the side bands that are about 60 to 80 dB under the 13.56 MHz carrier power. We found that the optimal power supply voltage for our antennas was around 14.6 volts.

5.2 Comparison with the Theoretical Predictions

We measured a 170mA DC supply current to the power amplifier when using the the copper tube antenna. The combination of this current value and a read range of 25 cm match the predictions of [KW05] very well: The graph shown in Figure 14 is from [KW05], and the star indicates our empirical results on the predicted curve.

We believe that using high rating components and more powerful RF test equipment, we can reach the road map along the theoretical curve. This will be done in later work.

5.3 System Cost

Ignoring the time and cost of labor, the system cost is ridiculously low. The most expensive item in the system is the TI module, which costs around \$60. All the other components, the materials for the PCBs, and the

items needed for building the loop antenna, together cost at most \$40-\$50, giving a total cost of \$100-\$110.

6 Conclusions

In this work we have shown how to build a portable, extended-range RFID skimmer. Our skimmer is able to read ISO-14443 tags from a distance of ≈ 25 cm, uses a lightweight 40cm-diameter copper-tube antenna, is powered by a 12V battery—and requires a budget of $\approx \$100$. We were able to build and tune the skimmer using only electronics hobbyist supplies and tools. By doing this we have proved three things: First, we have validated the basic concept of an RFID “Leech” and the modeling and simulation work of [KW05]. Second, we have demonstrated that ISO-14443 RFID tags can be skimmed from a range that is 3-5 time larger than the nominal range, and more importantly, is a distance that does not require the attacker to touch the victim. This last observation can make a noticeable difference in the attacker’s mode of operation. Finally, we are about half-way toward a full-blown implementation of a relay-attack of [KW05].

Our work implies that simple RFID tags, that respond to any reader, are immediately vulnerable to skimming. Therefore, at the very least, RFID tags, and in particular E-passports, should incorporate additional controls that prevent the tag from being read surreptitiously: e.g., physical shielding inside a Faraday cage, and cryptographic application-level access controls that require the reader to authenticate itself to the tag.

However, in isolation, cryptographic controls can only protect against skimming—they cannot protect against a relay attack. To protect against a relay attack, the RFID tag must be equipped with additional physical controls such as an actuator, or an optical barcode physically printed on the passport jacket: these help ensure that the reader is in fact reading the tag that is presented to it and not some remote victim tag.

Acknowledgments

We would like to thank Sergey Belous, Sammy Datika, Klaus Finkenzeller, Yeheal Greenblat, Ziv Kfir, Motti Kirshenboim, Markus Kuhn, and Moshe Panijel, for many stimulating discussions and practical tips, that greatly helped us during this project.

References

- [BGS⁺05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. <http://rfid-analysis.org/DSTbreak.pdf>, 2005.

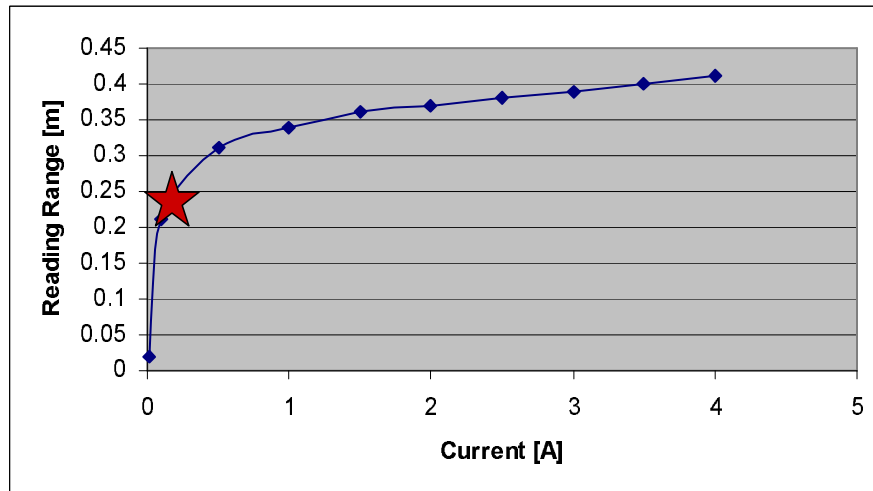


Figure 14: The predicted read-range versus the antenna current from [KW05]. The star indicates our empirical results.

- [Fin03] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, 2003.
- [FK05] Thomas Finke and Harald Kelter. Radio frequency identification—Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. BSI - German Ministry of Security, 2005. http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf, in German.
- [GSA04] U.S. government smart card handbook. Office of Governmentwide Policy, General Services Administration, February 2004.
- [GW04] Lukas Grunwald and Boris Wolf. RFDump, 2004. <http://www.rf-dump.org/>.
- [Han05] Gerhard Hancke. A practical relay attack on ISO 14443 proximity cards, 2005. <http://www.cl.cam.ac.uk/~gh275/relay.pdf>.
- [Hes04] Arik Hesseldahl. A hacker's guide to RFID. *Forbes Electronic Magazine*, July 29 2004. http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html.
- [HK05] Gerhard Hancke and Markus Kuhn. An RFID distance bounding protocol. In *Proc. 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Athens, Greece, September 2005. IEEE.
- [ISO00] Identification cards – contactless integrated circuit(s) cards – proximity cards - part 1 to 4. ISO/IEC 14443, 2000.
- [ISO01] Identification cards – test methods – proximity cards - part 6, annex B. ISO/IEC 10373-6, 2001.
- [JB04] A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap, April 2004. <http://theory.lcs.mit.edu/~rivest/>.
- [JRS03] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *Proc. 8th ACM Conf. Computer and Communications Security (CCS)*, pages 103–111, May 2003. <http://theory.lcs.mit.edu/~rivest/>.
- [Kre05] Brian Krebs. Leaving Las Vegas: So long Def-Con and Blackhat. *The Washington Post*, 2005. http://blogs.washingtonpost.com/securityfix/2005/08/both_black_hat_.html.
- [KW05] Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *Proc. 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, pages 47–58, Athens, Greece, September 2005. IEEE.
- [Lee03] Youbok Lee. Antenna circuit design for RFID application. Microchip Technology, Application Note AN710, DS00710C, 2003. <http://ww1.microchip.com/downloads/en/AppNotes/00710c.pdf>.
- [Lin05] Rick Lingle. MIT's economical RFID field probe, 2005. <http://www.packworld.com/articles/Departments/18784.html>.
- [Mel04] A power booster for the MLX90121. Melexis Application Note 390119012102, Rev.001, April 2004. http://www.melexis.com/relinfocfiles/AN90121_1.pdf.
- [Poz05] David M. Pozar. *Microwave Engineering*. John Wiley & Sons, Inc., third edition, 2005.
- [RCT05] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. RFID guardian: A battery-powered mobile device for RFID privacy management. In *Australasian Conference on Information Security*

and Privacy – ACISP’05, LNCS 3574, pages 184–194, Brisbane, Australia, July 2005. Springer-Verlag.

- [Sch01] Tom A. Scharfeld. An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design. Master’s thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, August 2001.
- [Sch05] Bruce Schneier. RFID passport security revisited. Schneier on Security: A weblog covering security and security technology, 2005. http://www.schneier.com/blog/archives/2005/08/rfid_passport_s_1.html.
- [SWE02] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS 2523*, pages 454–470. Springer-Verlag, 2002.
- [TI03] S4100 multi-function reader module data sheet. Texas Instruments, Module 11-06-22-715, 2003. http://www.ti.com/rfid/docs/manuals/refmanuals/rf-mgr-mnmn_ds.pdf.
- [TI04] HF antenna cookbook. Technical Application Report 11-08-26-001, Texas Instruments, January 2004. <http://www.ti-rfid.com>.
- [TI05] Rfid homepage. Texas Instruments, 2005. <http://www.ti-rfid.com>.
- [Wei03] Stephen A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master’s thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.
- [Whi05] Dan White. NCR: RFID in retail. In S. Garfinkel and B. Rosenberg, editors, *RFID: Applications, Security, and Privacy*, pages 381–395. Addison-Wesley, 2005.

A Printing the PCB antenna

The PCB antenna was made using PCB printing materials and hobbyist equipment as listed below:

- Raw PCB Glass-Epoxy tablet size 20x25 cm - price \$5
- Photo resist, Positive process - \$27
- Ferric Chloride - \$9
- Soda Caustic - \$9
- Piece of glass, size 18x23 cm for standard photo frame - \$1
- 1 A4 Pergament paper - 20 cents

- Black alcohol based non erasable water proof pen - \$1.25
- Acetone - \$4
- Rubber gloves, can be bought in a Dollar Store - \$1

The cookbook contains a complete description, including a print layout and electronic circuitry (See [TI04] pages 21-22).

The process of making the PCB antenna is identical to the process of making any PCB. Note that positive photo-resist PCB printing requires a positive layout film. Since making a celluloid film requires photographic equipment, we used the more common materials.

We first printed the antenna PCB layout on the pergament paper using an ink injection printer set up as follows:

- Print quality - best paper setting
- Transparency film - other transparency film
- Color - Print in gray scale - black only
- Check the GUI check box for “Actual size”
- Ink Volume - Heavy

The following instructions guide you through the antenna manufacturing process. Wear rubber gloves and protect eye glasses since Ferric Chloride acid is a very strong and harmful material, and contact with human eyes causes severe injury.

1. Cover the large areas of the ink with the water proof pen to avoid any penetrating light through the pergament paper.
2. Prepare the raw PCB Glass-Epoxy tablet for exposure by thoroughly cleaning it from dust and dirt. A clean surface is crucial to avoid PCB printing flaws.
3. Dry the tablet in an oven at a temperature around 70 Celsius degrees.
4. Thoroughly clean the glass against spots and dust.
5. In a dark room, spray a thin layer of Positive Photo Resist on the PCB tablet, and dry it in the oven at 70 Celsius degrees for about 20 minutes.
6. Make a 7% Soda Caustic solution with water.
7. Put the pergament printed layout over the PCB tablet in the correct direction (be aware of the Print Side (PS) and Component Side (CS)).
8. Put the glass on the pergament paper and hold them together tightly.

9. Expose the “sandwich” to bright sunlight for 4 to 6 minutes.
10. Remove the glass and pergament paper, and insert the exposed PCB into the Soda Caustic solution for about 20 minutes until all the photo-resist that was exposed to the sun is removed.
11. Thoroughly wash the PCB with water. Be extra careful not to scratch the photo-resist printed leads.
12. Make a 25 Celsius degrees Ferric Chloride solution, and insert the PCB until the exposed copper is fully etched. The PCB should be rapidly shaken within the acid, otherwise the etching process will take a long time. Shaking it will shorten the etching process to around 45 minutes. An aquarium pump is an effective and cheap way to stir the acid.
13. Wash the PCB thoroughly with water, dry it, and use the Acetone to remove the photo-resist from the antenna’s copper leads. We still had few small flaws left due to strong etching, therefore we covered the whole antennas copper leads with tin.

The 50Ω impedance matching network were soldered according to TI Antenna cookbook, see Figure 4, and we used a BNC connectors instead of SMA to reduce cost. At this point, the antenna is ready for tuning and use.

In countries lacking sunny days for long months, one can consider screen printing technology for printing the PCB antenna. This technique requires some background knowledge and some practical experience. The basic materials costs around \$150 dollars, and after few attempts, an average handyman can handle the task quite easily. We have not tried the screen printing as the process we described worked successfully for us.