# Extending the range of NFC capable devices

Bart Hermans & Sandino Moeniralam

University of Amsterdam

February 6, 2017

## Abstract

Near Field Communication (NFC) is a short range radio frequency technology. Because of the short range, cloning attacks of NFC devices are impractical. To make this possible, you would need to be very close to the tag. Currently, a lot of research has been done on NFC range extension. However, almost all of this research is executed in a lab environment that is not comparable to a day-to-day working environment. During this research, we research NFC range extension in a day-to-day environment.

Specifically, we look at the size of the rectangular loop antenna using a mathematical formula. Also, we research the optimal orientation and angle of NFC tags compared to the antenna. Finally, we are also researching the impact on the range when multiple NFC tags are introduced within the range of the NFC reader.

At the end of this research we were able to extend the range of NFC to 13.4 cm by creating our own antennas. We also identified that the length of the wire, diameter of the wire and the angle of the smart card does influence the range of NFC. However, orientation does not. Introducing multiple smart cards into the range would influence the reliability of the identification of smart cards.

# 1 Introduction

## 1.1 NFC

Near Field Communication (NFC) is a wireless communication technology which enables two compatible devices to transmit small amounts of data at a time. NFC is based on the radio frequency identification (RFID) technology. Usually the range between two NFC devices cannot be larger than 10 centimeters. NFC devices can be placed into two categories: passive and active devices.

Passive devices don't have a power source of their own. For this reason they cannot communicate directly to each other. When a powered device wants to communicate with a passive device, the passive device is powered using the electrical inductance that exists because of the data transmission. An example of a passive device is a wall advertisement which includes an NFC tag. Passive devices can only send requested information, they are not able to read data from other devices.

Active devices are different from passive devices in that they have a power source of their own. Compared to passive devices, active devices are able to send and receive data to both passive and active devices. An example of an active device is a smart phone which is NFC enabled.

High frequency NFC devices communicate at the 13.56 MHz frequency. This frequency is the same across all device types. Communication can happen in three different modes: peer-to-peer, read/write and card emulation mode.

In peer-to-peer mode NFC tags communicate directly to one another (bidirectional). This mode only works between active-active and active-passive NFC devices. In read/write mode, an active device communicates directly with another device. The other device only writes the received data to its chip or reads the requested data back to the active device. It doesn't matter if the device which acted upon the request is an active or passive device. Card emulation mode is being used when the NFC device wants to emulate a smart card or contactless credit card. This mode is useful in cases where a person wants to check-in to public transport using his or her smart phone (which has the digital information of a public transport card stored on this device)[1].

### 1.1.1 Standards

The newest NFC technology is based on the ISO/IEC 18092 standard. Which itself is based on the ISO/IEC 14443 standard. The ISO/IEC 14443 international standard was originally developed for close proximity contactless smart cards. The standard itself is divided into four parts. The first part describes the physical characteristics of close proximity cards. The second part describes the radio frequency characteristics as well as certain device types which are not the same as the passive and active categories. The third part focuses on describing anticollision techniques. The last part describes the protocol requirements option. This allows cards to enable or disable contactless transmission on cards. The development of the ISO/IEC 18092 was driven by a working group called the NFC forum. The ISO/IEC 18092 uses a reduced version of the ISO/IEC 14443 standard. For example, it stripped the fourth part out of the specification. On top of this they added the earlier described active and passive modes as well as the three transmission modes.

[1] http://www.androidauthority.com/what-is-nfc-270730/

One notable aspect worth mentioning is that both standards are not fully interoperable with each other. If an ISO/IEC 18092 compliant device is in peer-to-peer mode, it will not be recognized by a ISO/IEC 14443 device. The reason for this is that the ISO/IEC 14443 standard does not have a section which is equivalent to the peer-to-peer mode[2]. Currently, only the read/write and card emulation mode are interoperable between the two standards[3].

## 1.2 NFC Device types

As described in the previous subsection, the ISO/IEC 14443 describes two device types. There is also a third propriety device type. All three of the device types differ in the aspect that they all use different configurations for sending (polling) and receiving (listening) data[4]. The next section describes the properties of type A & B devices. An explanation of the properties itself follows afterwards. Please note that there also exists an NFC type F device. This device type, however, is only used in Japan[5].

### 1.2.1 Type A & B

Both type A & B devices are described by the ISO/IEC 14443 standard. NFC type A & B devices can communicate at a data rate of 106 kbps[6]. Table 1 & 2 shows the differences[7,8] between the two device types in polling and listening mode

| **Type** | **Properties** |
|---|---|
| Listening | ASK load modulation with Manchester encoding |
| Polling | ASK 100% with modified Miller encoding |

Table 1: Device type A

| **Type** | **Properties** |
|---|---|
| Listening | BPSK load modulation with NRZ-L encoding |
| Polling | ASK 10% with NRZ-L encoding |

Table 2: Device type B

### 1.2.2 Modulation

Amplitude Shift Keying (ASK) is a method where a specific amount of amplitude of the waveform will present a one-bit. Whereas a zero-bit would be represented by an amplitude of zero. The percentages at which NFC devices can do ASK modulation is called the modulation index. An index of 10% means that the modulated signal amplitude is 10% of the signal amplitude before modulation. In the case of an index of 100%, the amplitude of the modulated and unmodulated signal are almost equal. Worth mentioning

[2] http://www.icma.com/ArticleArchives/StandardsOct12.pdf

[3] http://bitexperts.com/Question/Detail/3360/difference-between-iso-14443-and-iso-18092-i-e-rfid-vs-nfc

[4] http://www.rfwireless-world.com/Tutorials/NFC-Modulation-and-NFC-Coding.html

[5] http://www.nfc.cc/2009/01/03/iso-14443-iso-18092-type-a-type-b-type-f-felica-calypso-nfcip-nfc-help/

[6] http://www.rfwireless-world.com/Articles/NFC-basics.html

[7] http://www.rfwireless-world.com/Tutorials/NFC-Modulation-and-NFC-Coding.html

[8] http://www.rfwireless-world.com/Terminology/NFC-A-vs-NFC-B-vs-NFC-F.html

is that the real value always lies around the index, so it's never an exact value[9,10].

BPSK stands for Binary Phase Shift Keying. Whereas ASK uses amplitude to differentiate between a 0 or a 1, BPSK uses changes (shifts) in waveforms to identify the binary data[11].

Section 1.2.1 described that some communication modes use load modulation. Load modulation is used by the antenna to absorb energy generated by the reading device. This energy can be used to power the NFC tag so that the tag can communicate with the reader[12].

### 1.2.3 Encoding

The NFC device types can use three different encoding styles for data transmission. In NRZ-L encoding, a 1 is indicated by a static high state of power. A 0 is indicated by a low state. In Manchester encoding bits are identified using a transition in states. For example, a low state transitioning to a high state indicates a 0. A 1 is indicated using a high state that transitions to a low state. Modified Miller encoding has a different rule set. A 1 is indicated using a short drop after 50% of the bit duration. Zeros are usually expressed without a drop if they follow a 1. When a 0 does not follow a 1, the 0 is identified using a drop in the first half of the bit time. Figure 1 visualizes what just has been described[13].

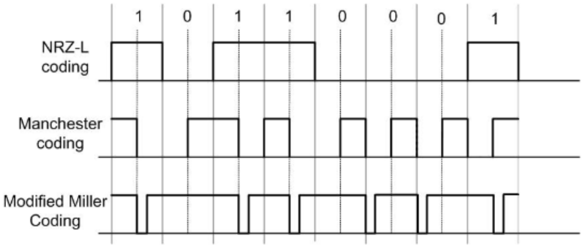

Figure 1: NFC encoding schemes

## 1.3 NFC use cases

NFC has a lot of use cases. Most of them are focused on proving that you're allowed entrance to somewhere (an art exhibition for example) or for transferring data. A very practical use case for NFC is access control in corporate offices. People can get a personal NFC tag which can then be activated so that the person can access the building. Once the person resigns, the only thing that the company needs to do is remove the NFC tag from the system. Other use cases include data transfer (peer-to-peer mode) and mobile payment using your smart phone (card emulation mode)[14].

## 1.4 Extended NFC use cases

If NFC could be extended to a range in which you can keep the NFC tag in your pocket, access control verification to enter a corporate office would speed up significantly. For instance, during rush hour, people would not need to wait in line to enter the building. This is quite common in large office buildings because taking the

[9] http://www.rfwireless-world.com/Terminology/ASK-vs-FSK-vs-PSK.html

[10] http://www.edaboard.com/thread195890.html

[11] http://www.rfwireless-world.com/Terminology/BPSK.htm

[12] http://www.st.com/content/ccc/resource/technical/document/technical_note/f9/a8/5a/0f/61/bf/42/29/DM00190233.pdf/files/DM00190233.pdf/jcr:content/translations/en.DM00190233.pdf

[13] http://www.rohde-schwarz.com.cn/data/skins/chinese/topic/1MA182_4e.pdf

[14] http://www.rohde-schwarz.com.cn/data/skins/chinese/topic/1MA182_4e.pdf

tag out of your pocket and holding it against the NFC reader can take time. Instead, people could just walk through the gates if they are allowed access. A commercial use case could be for stores to count the amount of people standing at specific places in the store based on the NFC tag in their smart phone.

A criminal use case of an extended NFC device could be tag cloning. At the moment this is impractical because the range of NFC only allows (weak) cards to be cloned within a theoretical range of 10 centimeters.

## 1.5 NFC antennas

Instead of 2 antennas communicating using radio waves, NFC uses tightly coupled inductors[Ok et al., 2012]. Inductive coupling works by 2 loop antennas or coils, influencing each others magnetic field. This magnetic field can be influenced by two factors: the amount of current flowing trough the wire and the number of coil turns. A second coil will induce the power of the magnetic field generated by the first coil when it's introduced into the magnetic field. For two NFC devices to be coupled, the distance between the coils must be less than the wavelength of the magnetic field divided by $\pi$ [Mareli et al., 2013].

With WiFi antennas, the range can sometimes be extended by increasing the power that the antenna transmits. With NFC this isn't the case. On one hand, the inductance has to be strong enough to be able to power an NFC tag. However on the other hand, the inductance also has to be weak enough for the NFC tag to load modulate the data from the power[15].

### 1.5.1 Tightly vs loosely coupled

The further the receiving coil is from the transmitting coil, the less flux it receives. Hence, the less power transfer takes place. The more flux the receiving coil receives, and therefore the more power transfer takes place, the stronger the two coils are coupled. The stronger two coils are coupled, the less loss and heating takes place, the more efficient the inductive power transfer is. Loosely coupled systems operate over longer distances than tightly coupled systems. Loosely coupled systems have higher interference and require more power input to function than a similar tightly coupled system would need. Loosely coupled coils have practical uses. As with tightly coupled systems, with loosely coupled systems the receiving coil does not need to be perfectly aligned[Paret, 2016].

### 1.5.2 Antenna size

The size of the antenna plays a considerable role in the range of the magnetic field. The bigger the antenna, the bigger the magnetic field. Thus, the greater the area in which tags can be powered. However, as stated before the tags also determine if there will be sufficient coupling to make NFC communication possible. For example, a small NFC tag will only allow a small range of effective NFC communication even when the antenna is quite large in comparison[16,17].

Additionally, when the size of the antenna increases, the diameter of the wires should also increase to cope with the resistance and inductance. In other words, thicker wires are used

[15] http://electronics.stackexchange.com/questions/132603/how-to-increase-the-read-range-of-an-active-nfc-tag

[16] http://www.sagedata.com/learning-centre/rfid-read-range.html

[17] http://blog.atlasrfidstore.com/improve-rfid-read-range

to decrease the inductance as well as the resistance[18].

### 1.5.3 Calculating inductance

The lower the self-inductance, the more sensitive the antenna and the smaller the range will be[19]. Also, the greater the self-inductance, the greater the range of the magnetic field will be and the worse the antenna will be able to receive data from the other device. However, there is a limit to altering the amount of inductance. As stated by [20] [Palit, 2015], the coupling will not happen when the self-inductance of an NFC antenna is outside the range of 0.3$\mu$H and 3$\mu$H. $\mu$H is a measurement unit for displaying self- or mutual-inductance[21].

The self-inductance of a rectangular loop NFC antenna in $\mu$H can be calculated using the formula[22] in equation 1.

$$L = N^2 \frac{\mu_0 \mu_r}{\pi} (-2(w+h) + 2\sqrt{h^2+w^2} - h \times \log(\frac{h+\sqrt{h^2+w^2}}{w}) - w \times \log(\frac{w+\sqrt{h^2+w^2}}{h}) + h \times \log(\frac{2h}{a}) + w \times \log \frac{2w}{a}) \div 1000 \tag{1}$$

Where $N$ equals the number of rounds of wire, $w$ equals the width of the antenna, $h$ equals the height of the antenna and $a$ the radius of the wire. All of these input values (except $N$) are in centimeters. The relative permeability of the medium $\mu_r$ is 1 (air)[23]. The physical constant $\mu_0$ to define the permeability of a vacuum is defined using the formula[24,25] in equation 2.

$$\mu_0 = 4 * \pi * 10^{-7} \tag{2}$$

# 2 Research questions

Our main research question is as follows:
*What properties of the rectangular loop antenna of an NFC reader and the NFC tag influence the effective range of communication with passive NFC devices?*

This main research question is supported by three sub-research questions:

- *Does the thickness and length of the wire of high-frequency loop antennas affect the range of NFC communication?*
- *How do the orientation and angle of the tag affect the range?*
- *Will the NFC reader be able to identify an NFC tag at the same distance, when there are multiple NFC devices within the range?*

## 2.1 Research scope

This research is only focused on high frequency rectangular loop antennas. The reason for this is that NFC antennas operate best when they have the same shape as their tags[26]. During this

[18] http://www.ti.com/lit/an/scba033/scba033.pdf

[19] http://www.antenna-theory.com/definitions/nfc-antenna.php

[20] http://www.ekswai.com/nfc.htm

[21] https://www.translatorscafe.com/unit-converter/en/inductance/1-13/

[22] https://emclab.mst.edu/inductance/rectgl/

[23] http://www.engineeringtoolbox.com/permeability-d_1923.html

[24] http://physics.info/constants/

[25] http://www.chemie.fu-berlin.de/chemistry/general/constants_en.html

[26] https://devzone.nordicsemi.com/blogs/957/nfc-tag-antenna-tuning/

research we create four different antennas. Two of these have a ratio of 1:2 and two have a ratio of 1:5. These ratios are based on the size of the antenna inside the NFC smart card. Each ratio has antennas of 1.5 and 2.7 mm in diameter. The antennas are connected to a Proxmark3, which is specifically designed for NFC research[27]. The NFC tags consist of a blank card and three access control smart cards of KPMG. The blank card is only used for the first two experiments. This blank card is shipped together with the Proxmark3 for NFC research. For the last experiment we want to use equivalent smart cards. We are using the KPMG entrance cards for this.

### 2.2 Report structure

This research paper begins with an introductory background section on NFC and NFC antenna design. Section 1 is the result of a literature research we conducted. Having kept in mind the most important aspects of relevant research papers, we formulated research questions in Section 2.

In section 3 we describe previous research which has been done on NFC range extension. In the same section we also describe how our research is new compared to previous work. Following on that, we define our research framework in Section 4 (Methods). Inside Section 4 the experimental setup as well as the defined experiments are described. Each of the experiments contain a paragraph on how we conduct the experiment and do measurements. The results of these experiments are described in Section 5. Section 6 is reserved for a discussion of these results along with the refutations of possible counter arguments. This leads to a conclusion which is described in Section 7. Whatever unresolved issues remain as well as follow up ideas are discussed in Section 8, future work. Quite some results are gained from the experiments of which the exact data points are placed in Section 9, Appendices.

## 3 Related work

It is important that we focus on a very specific part of range extension in NFC. In 2016, students of the SNE master did a research project that had a relation with NFC range extension[van Dijk and Sangers, 2016]. We use this research to determine important antenna properties. Another research paper called: *Range Extension Attacks on Contactless Smartcards*[Oren et al., 2013]. This paper did research on successfully executing relay attacks. One choice that they made during their research was using separate antennas for transmitting and receiving. Moreover, the positioning and type of the antennas were found to be very important[Oren et al., 2013]. We use this research as a starting point to develop our own antennas. Research that was done in 2011 titled: *RFID Jamming and Attacks on Israeli e-Voting.* This paper researched a way to exploit the voting mechanism that Israel introduced. The authors managed to use high frequency antennas to increase the range of NFC devices. Another interesting fact that the research concluded was that placing a metal plate under the antenna increases the range[Oren et al., 2012]. If time allows us, we could use this view to also look at the positioning of NFC devices. Another paper we looked at was: Range Extension of an ISO/IEC 14443 type A RFID System with Actively Emulat-

[27] https://store.ryscc.com/products/new-proxmark3-kit

ing Load Modulation[Finkenzeller et al., 2011]. An important element that the paper mentions is that the data could be sent over two different side bands around the 13.56 MHz frequency. To effectively extend the range, it's important to use the upper side band instead of both the upper and lower side band. The reason for this is that by choosing one side band, the transmit power can be enhanced by a factor of four. The reason to choose the upper side band in particular is that there exist NFC tags which only evaluate the upper side band[Finkenzeller et al., 2011]. Another important point to make is to use thick wires when creating big antennas[Finkenzeller et al., 2011]. This research is used as input to determine the size of our antennas. This conforms to the design of NFC to only work with HF antennas[28]. As stated at the beginning of this section, quite a lot of research has already been done on extending the range of NFC capable devices. However, this is mostly theoretical [Mourad et al., 2014]. One of the goals of this research is to look at the practical side of NFC range extension.

# 4 Methods

This section describes the experimental setup as well as the tools we use to conduct our measurements. We also describe the accuracy of each of these tools. In Subsection 4.2 we describe all of the experiments in terms of how we are going to conduct the experiment and what we want to measure.

## 4.1 Experimental setup

All of our experiments are conducted on a set of wooden planks. Additionally, we make sure that no metal objects are within a range of 50 centimeter of our experimental setup. By doing this, we prevent our results being influenced by any objects that are out of the scope of our experimental setup. 50 cm is the maximum expected range at the start of the experiments. Should we manage to increase the range of an NFC tag nearing 50 cm, the distance to other metal objects is increased by another 50 cm.

As NFC tag we use a blank card with a size of 5.4 cm in height and 8.5 cm in length. The reason that we are using a blank card is because it enables us to write data to the smart card should we want to do this later on in our research. The rectangular loop antenna in the smart card has a height of 4.1 cm and a length of 6.9 cm. For the third experiment we use three access control cards (for access to the building of KPMG). These smart cards also have a height of 5.4 cm and a length of 8.5 cm and have 2 coils inside. The outer, thin coil has a dimension of 7.2 cm times 4.8 cm. The inner, thicker coil has a dimension of 6.8 cm times 3.8 cm.

The NFC reader consists of a Proxmark3 naked edition and 4 self-made rectangular loop antennas. These antennas are constructed based on the inductance formula and size of the smart card of Section 1.5.3 and 1.5.2. In short, the following types of antennas are constructed: 2 antennas from a wire of a diameter of 1.5 millimeters and 2 antennas of a diameter of 2.7 millimeters. The first type of antennas has a ratio of 1:2 compared to the size of the antenna inside the smart card. The second type has a ratio of 1:5. The reason that we create antennas of different size and thickness is because we want

[28] http://blog.atlasrfidstore.com/rfid-vs-nfc

to determine whether size and/or wire thickness has an impact on the range of NFC communication. The resistance is calculated using the formula[29] in equation 3.

$$R = \frac{l \times \rho}{A} \tag{3}$$

Where $l$ stands for the length of the wire in meters. $\rho$ equals the electrical resistivity (which is $1.68 \times 10^{-8}$ $\Omega$·m for copper). $A$ stands for the cross sectional area of the wire in meters squared[30,31]. The output of the formula is the resistance in $\Omega$ of the antenna. Figure 2 shows a picture of the experimental setup during experiment 1.

## 4.2 Experiments

During this research we conduct three different experiments.

Table 3 shows the properties of each antenna we create. Each of the antenna has one round of wire. The relative permeability of the medium which we use to calculate the self inductance is 1, as defined in Section 1.5.3. The radius column equals the radius of the copper wire. Whereas, the length column equals the length of the wire which we use to construct the antenna.

One round is used with each antenna because any increase in the number of rounds will increase the self-inductance. As stated in Section 1.5.3, this has a negative impact on the coupling of two NFC antennas.

As shown in Table 3, the length of wire we use for each antenna includes an additional 8 cm. The reason from a practical point of view is that otherwise we are not able to connect the antenna to the Proxmark3. Knowing that one meter of copper wire has no significant resistance, we conclude that these additional 8 cm has a negligible impact on the inductance of the antennas.

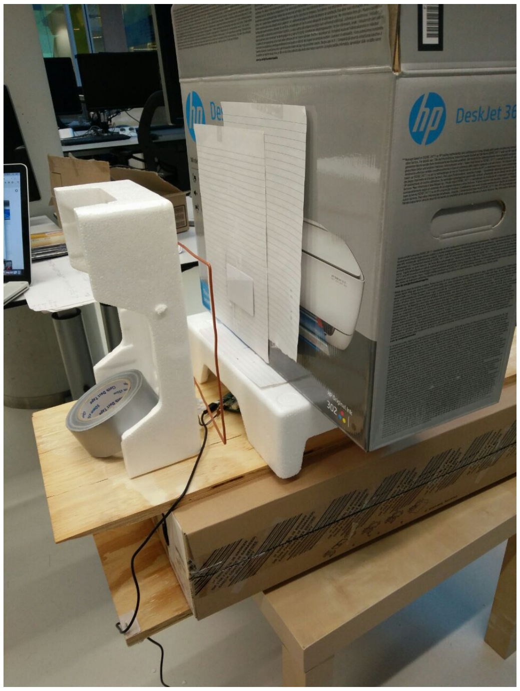

Figure 2: Experimental setup during experiment 1

The return value in volts on the Proxmark3 is determined using the **hw tune** command. This command automatically measures the optimal antenna values. Based on the command sheet [32], this is the only command to define power settings of the antenna.

To measure the distance we use a tape measure which is aligned parallel to the NFC reader

[29] http://chemandy.com/calculators/round-wire-resistance-calculator.htm

[30] http://www.endmemo.com/physics/resistance.php

[31] http://chemandy.com/calculators/round-wire-resistance-calculator.htm

[32] https://github.com/Proxmark/proxmark3/wiki/commands

| Antenna | Dimensions | Ratio | Radius | Length | Resistance | Inductance |
|---|---|---|---|---|---|---|
| 1 | 13.8 × 8.2 cm | 1:2 | 0.075 cm | 52 cm | 0.0049 ± 0.0001 Ω | 0.36 ± 0.02 $\mu$H |
| 2 | 34.5 × 20.5 cm | 1:5 | 0.075 cm | 118 cm | 0.0112 ± 0.0001 Ω | 1.11 ± 0.03 $\mu$H |
| 3 | 13.8 × 8.2 cm | 1:2 | 0.135 cm | 52 cm | 0.0015 ± 0.00002 Ω | 0.31 ± 0.02 $\mu$H |
| 4 | 34.5 × 20.5 cm | 1:5 | 0.135 cm | 118 cm | 0.0034 ± 0.00002 Ω | 0.98 ± 0.02 $\mu$H |

Table 3: Properties of the antennas we create. The length and dimensions column have a measurement error of 5 mm for each measurement.

and tag. This tape measure has an accuracy of 1 mm. To measure the orientation and angle we use a digital protractor. This digital protractor has an accuracy of 0.1 degrees. In the experiments where we use the digital protractor, a measurement error of 5 degrees is taken into account. For constructing and measuring antennas we use a measurement error of 5 mm. The reason for this is that the experimental setup doesn't allow us to apply a higher accuracy.

#### 4.2.1 Experiment 1

In this experiment we build four different antennas based on the inductance formula from the introduction section and the size of the antenna in the smart card. This experiment takes place on a set of wooden planks as mentioned in the experimental setup. As starting position, we position the Mifare Classic 1K smart card one centimeter away from the antenna. This smart card is taped to a polystyrene board and aligned parallel to the antenna. We then bring the polystyrene board further away from the antenna (1 cm at a time) until the smart card cannot be read anymore. We then move the card closer to the antenna by 1 mm at a time, until we find the card can be read again. Another important aspect that needs to be addressed is that the card is aligned parallel to the center of the antenna.

At each position we try to identify the card using the **hf search** command[33]. This command is executed twice, to cope with unreliable identification distances. Once the card can be identified two consecutive times, we consider the specific range effective.

#### 4.2.2 Experiment 2

Using the antenna with the biggest range we conduct experiment 2 at the greatest distance that we measured. In this experiment we measure the effect of changing the orientation and angle of the card. Before we start we tape the digital protractor to the polystyrene board. We then rotate the smart card in steps of 10 degrees at a time. If we see that rotating the smart card has an impact on the identification, we narrow down the transition from identification to non-identification in steps of 5 degrees between the working rotation degrees and the non-working rotation degrees. When measuring the orientation, the card is parallel relative to the antenna.

[33] https://github.com/Proxmark/proxmark3/wiki/commands

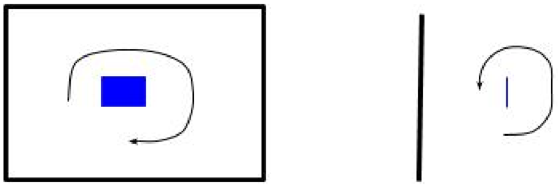

Figure 3: A schematic sketch of the setup. The card (blue) relative to the antenna (black). On the left measuring the orientation, on the right the angle.

Both the orientation as well as the angle is measured at a distance of 10 cm. The reason for this is to keep the smart card within the range of the antenna even when the angle of the smart card is 0 or 180 degrees. We measure the full 360 degrees. The angle is measured by placing the protractor on the same side of the card. When using the antenna, the protractor is removed as to not interfere with the measurements. A wooden skewer is taped horizontally to the smart card to act as an axle. When we conclude that the current angle identifies the card and the next 10 degrees doesn't, we go back 5 degrees to narrow down the value.

Every time we change the orientation and angle we try to identify the card using the **hf search** command of the Proxmark3. This command is executed twice, to cope with unreliable identification distances. Once the card can be identified two consecutive times, we consider the specific range effective.

### 4.2.3 Experiment 3

During experiment 3 we also choose the most optimal antenna of experiment 1. In experiment 3 we determine the effect of having multiple NFC smart cards within the range of the NFC reader. We tape all three smart cards, in different settings to the same polystyrene board. This polystyrene board is then aligned parallel towards the antenna of the Proxmark3. All cards are horizontally orientated (0°) towards the antenna. In all experiments the center of the card is aligned to the center of the antenna. For this experiment specifically we use the KPMG access cards that three of the researchers at KPMG have. The maximum range that we achieved with these cards is 8 cm. Hence, the starting distance for every measurement is 8 cm. We decrease this distance by 1 cm at a time until the cards are positioned 1 cm from the antenna. The first setting is to place the three cards horizontally next to each other, with zero spacing. The second setting is to place the three cards vertically with no spacing. Additionally, we tape all three cards on top of each other (stacked parallel to the antenna). This is done without any spacing. The goal of these activities is to determine if this would impact the range. The identification happens using the **hf search** command on the Proxmark3. This command is executed twice, to cope with unreliable identification distances. Once the same card can be identified two consecutive times, we consider the specific range effective.

Figure 4 shows how the cards are aligned next to each other. Figure 5 shows how the cards are placed above each other. In Figure 6, the placement of the cards is shown during the last activity of experiment 3. Please note that during all activities, the spacing between the cards is zero.

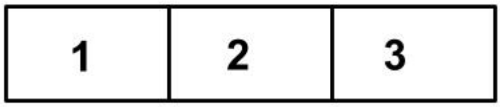

Figure 4: The cards aligned horizontally

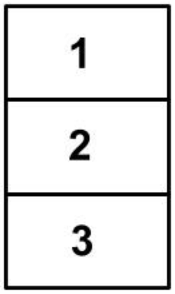

Figure 5: The cards aligned vertically

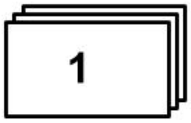

Figure 6: The cards stacked on top of each other

# 5 Results

This section is divided into three subsections. Each subsection describes the results of a specific experiment.

## 5.1 Ideal antenna

During experiment 1 we created four different antennas. A picture of each antenna is shown before the measurements are presented. We included the tables corresponding to the line diagrams in the appendices (Section 9.1). These tables contain the exact values from each measurement. With each of the antennas, the measured return voltage (using the **hw tune** command) is also shown. The reason that we list these return voltages is for the means of reproduction of this research. Please note that a return voltage of greater then or equal to 10 volts is considered optimal. A lower return voltage is also acceptable. However, this may give suboptimal results[34].

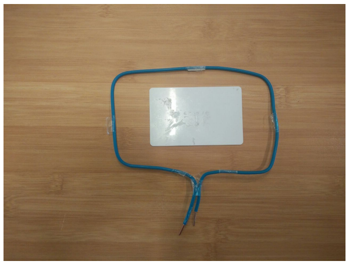

Figure 7: Antenna 1

The line diagram in Figure 8 shows the measurements we conducted with antenna 1. Based on the results, this antenna has a maximum range of 4.7 cm. Please note that we always measure 1 cm extra when we conclude that the smart card can't be identified anymore. The reason for this is that we want to make sure that a specific distance isn't just a bad working distance and that the next centimeter works without a problem. With the first antenna we measure a return voltage of 5.92V.

[34] https://github.com/Proxmark/proxmark3/wiki/antennas

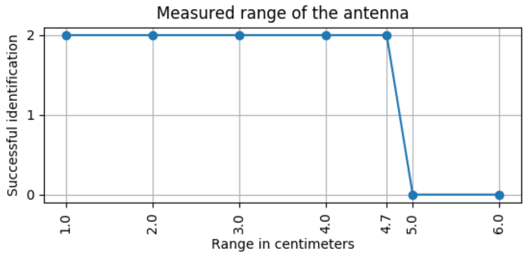

Figure 8: The range of antenna 1. The measured distances have a measurement error of 5 mm.

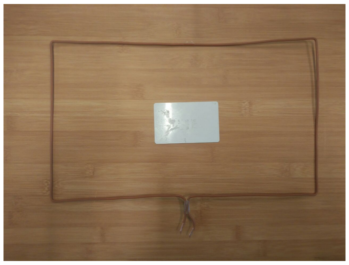

Figure 9: Antenna 2

The measurements of antenna 2 are shown in Figure 10. With this antenna we managed to achieve a range of 12.8 cm. Compared to the antenna from Figure 8, this antenna is only able to identify the smart card one time during two measurements. The tuning of this antenna results in a return voltage of 16.06V.

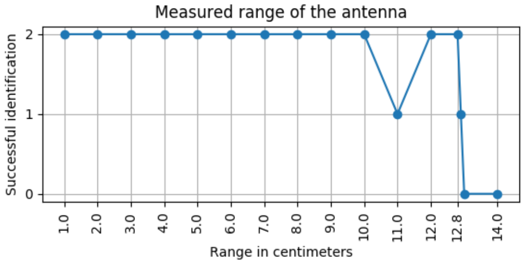

Figure 10: The range of antenna 2. The measured distances have a measurement error of 5 mm.

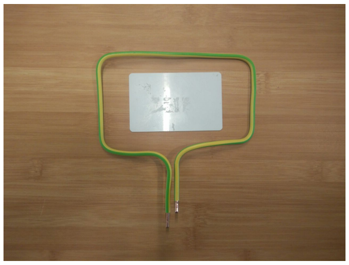

Figure 11: Antenna 3

The measured results of antenna 3 are shown below in Figure 12. Compared to the previous two antennas, this antenna is the first of two antennas created with a copper wire diameter of 2.7 mm. The range of this antenna is measured at 4.9 cm. The Proxmark3 measures this antenna with a return voltage of 5.46V.

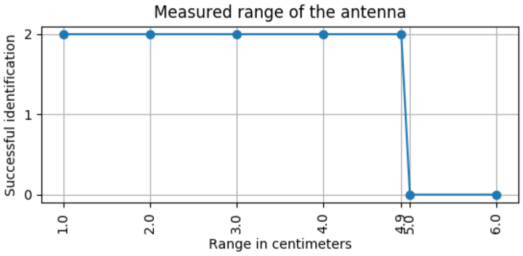

Figure 12: The range of antenna 3. The measured distances have a measurement error of 5 mm.

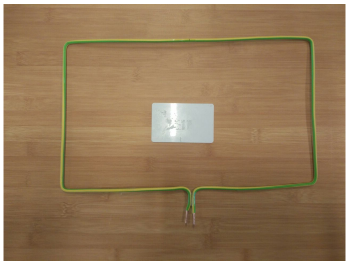

Figure 13: Antenna 4

The measurements of the fourth antenna (Figure 13) are shown in Figure 14. During the measurement of this antenna, we are not able to identify the smart card at a distance of 2 cm. However, we achieved a range of 13.4 cm with this antenna. During the tuning of the antenna using the Proxmark3, we measure a return voltage of 19.18V.

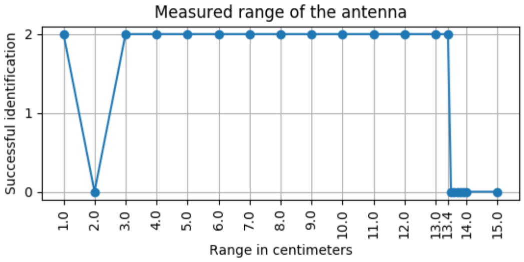

Figure 14: The range of antenna 4. The measured distances have a measurement error of 5 mm.

## 5.2 Orientation and angle

During experiment 2 only antenna 4 is used. The reason for that is that this antenna has the greatest range. The set of wooden planks and a polystyrene construction is used in this experiment. The exact data points that are being presented in this section can be found in appendix II (Section 9.2).

As shown in the first table in appendix II, the orientation of the card does not have an effect on the ability of the NFC reader to identify it. There is not a single orientation of the card that makes it unidentifiable by the NFC reader.

The diagram in Figure 15 shows the measurements of changing the angle of the card. As shown in the diagram (and Figure 16), we are only able to successfully identify the card when it has an angle between 55° and 135° or 235° and 315°. It does not matter whether the card is read from the front or from the back side, as long as it remains parallel to the antenna within a certain degree.

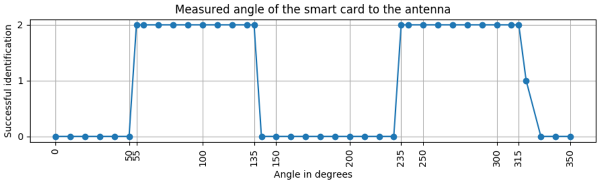

Figure 15: Measurements of the angle of the smart card. The measured angles have a measurement error of 5°.

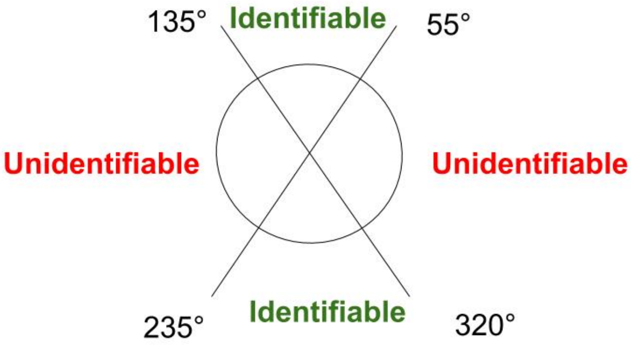

Figure 16: A side view showing the identifiability depending on the angle of the card. 90° and 270° is perfectly parallel relative to the reader.

## 5.3 Multiple smart cards

In this section we present the results of experiment 3. This experiment is also conducted with antenna 4. During this experiment we determined that the effect of having multiple smart cards within range has impact on the range. The data points in table notation can be found in appendix III (Section 9.3).

The line diagram in Figure 17 shows the result of having multiple smart cards above each other within the range of the NFC antenna. At 8 cm distance, smart card 1 is identified. At 1 & 2 cm, smart card 2 is identified.

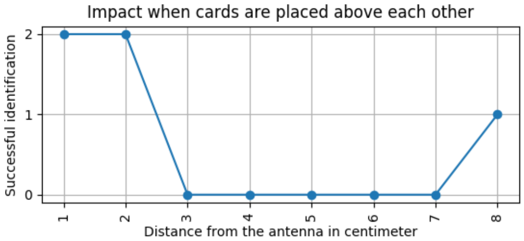

Figure 17: Measurements of having multiple cards above each other. The measured distances have a measurement error of 5 mm.

In Figure 18 a line diagram is listed for the measurements of having multiple smart cards next to each other within the range of the NFC antenna. Each time the NFC reader identifies a card, smart card 2 is identified.

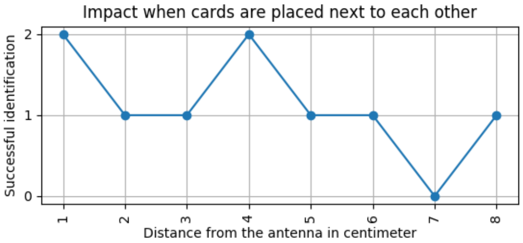

Figure 18: Measurements of having multiple cards next to each other. The measured distances have a measurement error of 5 mm.

The last measurement we conduct is measuring the effect of having three smart cards stacked on top of each other. During this measurement, all the cards are unidentifiable at all ranges.

## 6 Discussion

During this research we found out that the achieved range extension did not apply to all NFC smart cards. We also had some smart cards of our own which we tested along the way. With these smart cards we were only able to achieve a range of a few centimeters. There could be argued that our results are therefore unusable for extending the range of NFC devices in a day-to-day environment. However, the blank card that we used is also available for people to use in a production environment[35].

Although, the digital protractor allowed for an accuracy of 0.1°, we applied an accuracy of 5° to our data points when conducting experiment 2. The reason for this is that with the materials available, we were not able to construct an experimental setup which allowed us to alter the angle and orientation in steps of 0.1°. To make this possible, a specialized construction should be created (a sort of wooden lathe for example). Because of the limited amount of time we had available for this research, we were not able to construct this. The same goes for experiment 1 and 2, where we applied a measurement error of 5 mm to measurements using the tape measure.

We used wires of two different diameters and two different ratios for the size of the antenna. These values were chosen as starting point for our research and not as a choice we made during our research. It could be argued that this approach would make the results not specific enough. However, with this approach we wanted to determine whether wire diameter and the size of the antenna would have effect on the range of NFC. This could then be further researched in

[35] http://www.nfc-nederland-shop.nl/nxp-mifare-classic-ev1-1k.html

future work.

During experiment 2 we used distances that are different than the maximum range we achieved with the most optimal antenna. The reason for this is that we wanted to keep the smart card within the range of the antenna, even when we altered the angle of the smart card to 0 or 180°. If we would conduct the measurement at the maximum distance, at these angles the smart card wouldn't fully be within range.

The reason that we did not add spacing between the cards during experiment 3 was to mimic a more realistic environment. Smart cards are commonly placed inside a wallet with little to no spacing between them. It might be the case that just having several smart cards on top of each other, is enough protection from skimming in itself. This together with an angle that makes identifying the card hard to do, can help establishing NFC smart cards as a relative safe option.

Finally, during the range measurements, with the fourth antenna we were unable to identify the smart card at a distance of 2 cm. However, at a distance of 3 cm, the smart card was readable again. We currently reason that this has to do with the strength of the electromagnetic field at that distance (a sort of dead spot as is sometimes the case in 2.4/5 GHz wireless). This could be identified by using an oscilloscope. The oscilloscope could be connected to a separate coil which is brought into a range of 2 cm from the antenna. We did not have an oscilloscope available, therefore this should be further researched in future work. Another reason we want to bring forward is that using the oscilloscope was outside the scope of our research. The reason for this is that we otherwise had to research the exact design of the smart card we used so that we could recreate this antenna using copper wire. Because the antenna inside the smart card is coated in plastic, an oscilloscope cannot be connected to the smart card.

### 6.1 Pitfalls

The first antenna designs during our research were made out of thin copper wire (approximately 0.1 mm thick). We discovered that this thin wire did not work very well for constructing HF antennas with a range larger than a few centimeters. Although, all of these antennas had a self-inductance value of approximately 3 $\mu$H, the return voltage we measured using the Proxmark3 was only 0.07V. This makes such antennas unusable as NFC high frequency antennas. During our research we discovered that the diameter of the wire should increase when the size of the antenna increases.

Moreover, during the research we saw that charging a laptop within 1 meter impacts the range of the NFC antenna. Therefore, all our experiments were conducted using a laptop on battery power.

## 7 Conclusion

During this research we researched different properties of rectangular loop antennas, and the effective range of communication with smart cards. The objective of this research was to identify properties that define the identification range of these cards.

From this research we can conclude that the thickness as well as the length of high-frequency rectangular loop antennas affect the range of NFC communication. Thicker does not necessarily mean better, nor do longer wires necessarily lead to better antenna design. Self-inductance is an important factor, that all working NFC antennas must adhere to. For this reason there is an upper and lower limit to the practical length and thickness of the wire, used for NFC antennas. However, we could not determine the exact relation between self-inductance of the antenna and the effective range. A higher or lower self-inductance does not intrinsically lead to a higher range. Of the 4 antennas that we constructed, the thickest and longest did lead to the best results. However, this antenna did not have the highest or lowest self-inductance.

Having researched the influence of the reader together with the card, we conclude that the orientation of the card relative to the reader does not effect the range. The angle however, does. NFC communication only allows a variation of about 35 to 45°, in either way, relative to being perfectly parallel to the reader.

The biggest distance achieved in this research, with the card being perfectly parallel to the antenna was 13.4cm. Our last experiment proved that placing multiple smart cards within the range of the NFC reader has impact on the range. When the cards were placed above each other, the identification was only reliable within a range of 2 cm. When the cards were placed next to each other, only the second card could be identified. However, identification was unreliable. When the smart cards would be stacked on top of each other, the cards would become unidentifiable.

# 8 Future Work

The starting point of our research was to focus on HF rectangular loop antennas. In previous work and also in our current research we were not able to determine whether the geometric shape of the antenna has an effect on the range. Our research could be repeated with HF circular loop antennas. The results of such research could be compared to determine which geometric shape produces the best range.

In the discussion section we mentioned that using different types of smart cards (outside of the scope of our research) produced different ranges. Based on our research, further research could be done to identify the reason for this behaviour. We reason that this is caused by using different coils inside smart cards.

During the literature research we encountered a source which used a formula to theoretically calculate the coupling of NFC devices[36]. However, this formula only applies to circular shaped loop antennas. With our results as input, research could be done on devising a formula to calculate the coupling of rectangular shaped loop antennas.

On top of this research, another topic of interest would be to determine the most effective level of amplification. Research specifically into inductive coupling, and the optimal level of self-inductance could potentially increase the range even further.

We would also like to propose further research into determining the most effective value of self-inductance. As stated in Section 1.5, the self-inductance needs to be strong enough to emit a very large magnetic field and at the same time be weak (sensitive) enough to receive data from the tag. Based on the antenna we created with the greatest range, this value should be somewhere around 0.9859 $\mu$H.

During experiment 3, we used no spacing be-

[36] http://miniradiosolutions.com/wp-content/uploads/2015/09/NFC-Reader-Design-II-Antenna-design-considerations-Public.pdf

tween the cards. Research could be done into determining if adding a certain amount of spacing between the cards would make the cards identifiable.

Finally, experiment 1 of this research could be redone by researchers that have an oscilloscope available. This device could then be used to identify the reason that the smart card couldn't be identified at particular ranges.

# References

[Finkenzeller et al., 2011] Finkenzeller, K., Pfeiffer, F., and Biebl, E. (2011). Range extension of an iso/iec 14443 type a rfid system with actively emulating load modulation. In *Smart Objects: Systems, Technologies and Applications, Proceedings of RFID SysTech 2011 7th European Workshop on*, pages 1–10. VDE.

[Mareli et al., 2013] Mareli, M., Rimer, S., Paul, B., Ouahada, K., and Pitsillides, A. (2013). Experimental evaluation of nfc reliability between an rfid tag and a smartphone. In *AFRICON, 2013*, pages 1–5. IEEE.

[Mourad et al., 2014] Mourad, O., Le Thuc, P., Staraj, R., and Iliev, P. (2014). System modeling of the rfid contactless inductive coupling using 13.56 mhz loop antennas. In *Antennas and Propagation (EuCAP), 2014 8th European Conference on*, pages 2034–2038. IEEE.

[Ok et al., 2012] Ok, K., Coskun, V., and Ozdenizci, B. (2012). Near field communication: From theory to practice.

[Oren et al., 2012] Oren, Y., Schirman, D., and Wool, A. (2012). Rfid jamming and attacks on israeli e-voting. In *Smart Objects, Systems and Technologies (SmartSysTech), Proceedings of 2012 European Conference on*, pages 1–7. VDE.

[Oren et al., 2013] Oren, Y., Schirman, D., and Wool, A. (2013). Range extension attacks on contactless smart cards. In *European Symposium on Research in Computer Security*, pages 646–663. Springer.

[Palit, 2015] Palit, A. K. (2015). Extraction of 13.56 mhz nfc-reader antenna parameters for matching circuit design.

[Paret, 2016] Paret, D. (2016). *Antennas designs for NFC devices.* John Wiley & Sons.

[van Dijk and Sangers, 2016] van Dijk, R. and Sangers, L. (2016). Portable rfid bumping device. UvA.

# 9 Appendices

## 9.1 Appendix I

This appendix contains the tables with exact measurement values. These values were measured during the execution of the first experiment.

| Range | Times of successful identification |
|---|---|
| 1 cm | 2 |
| 2 cm | 2 |
| 3 cm | 2 |
| 4 cm | 2 |
| 4.7 cm | 2 |
| 4.8 cm | 0 |
| 4.9 cm | 0 |
| 5 cm | 0 |
| 6 cm | 0 |

Table 4: Experiment 1: exact measurement results antenna 1. The ranges have a measurement error of 5 mm.

| Range | Times of successful identification |
|---|---|
| 1 cm | 2 |
| 2 cm | 2 |
| 3 cm | 2 |
| 4 cm | 2 |
| 5 cm | 2 |
| 6 cm | 2 |
| 7 cm | 2 |
| 8 cm | 2 |
| 9 cm | 2 |
| 10 cm | 2 |
| 11 cm | 1 |
| 12 cm | 2 |
| 12.8 cm | 2 |
| 12.9 cm | 1 |
| 13 cm | 0 |
| 14 cm | 0 |

Table 5: Experiment 1: exact measurement results of antenna 2. The ranges have a measurement error of 5 mm.

| Range | Times of successful identification |
|---|---|
| 1 cm | 2 |
| 2 cm | 2 |
| 3 cm | 2 |
| 4 cm | 2 |
| 4.9 cm | 2 |
| 5 cm | 0 |
| 6 cm | 0 |

Table 6: Experiment 1: exact measurement results of antenna 3. The ranges have a measurement error of 5 mm.

| Range | Times of successful identification |
|---|---|
| 1 cm | 2 |
| 2 cm | 2 |
| 3 cm | 2 |
| 4 cm | 2 |
| 5 cm | 2 |
| 6 cm | 2 |
| 7 cm | 2 |
| 8 cm | 2 |
| 9 cm | 2 |
| 10 cm | 2 |
| 11 cm | 1 |
| 12 cm | 2 |
| 13 cm | 2 |
| 13.4 cm | 2 |
| 13.5 cm | 0 |
| 13.6 cm | 0 |
| 13.7 cm | 0 |
| 13.8 cm | 0 |
| 13.9 cm | 0 |
| 14 cm | 0 |
| 15 cm | 0 |

Table 7: Experiment 1: exact measurement results of antenna 4. The ranges have a measurement error of 5 mm.

## 9.2 Appendix II

In this section we included the results of the measurements we did on changing the angle and rotation of the smart card.

| Orientation | Times of successful identification |
|---|---|
| 0° | 2 |
| 10° | 2 |
| 20° | 2 |
| 30° | 2 |
| 40° | 2 |
| 50° | 2 |
| 60° | 2 |
| 70° | 2 |
| 80° | 2 |
| 90° | 2 |
| 100° | 2 |
| 110° | 2 |
| 120° | 2 |
| 130° | 2 |
| 140° | 2 |
| 150° | 2 |
| 160° | 2 |
| 170° | 2 |
| 180° | 2 |
| 190° | 2 |
| 200° | 2 |
| 210° | 2 |
| 220° | 2 |
| 230° | 2 |
| 240° | 2 |
| 250° | 2 |
| 260° | 2 |
| 270° | 2 |
| 280° | 2 |
| 290° | 2 |
| 300° | 2 |
| 310° | 2 |
| 320° | 2 |
| 330° | 2 |
| 340° | 2 |
| 350° | 2 |
| 360° | 2 |

Table 8: Experiment 2: measurements rotation. The orientation has a measurement error of 5°.

| **Angle** | **Times of successful identification** |
|---|---|
| 0° | 0 |
| 10° | 0 |
| 20° | 0 |
| 30° | 0 |
| 40° | 0 |
| 50° | 0 |
| 55° | 2 |
| 60° | 2 |
| 70° | 2 |
| 80° | 2 |
| 90° | 2 |
| 100° | 2 |
| 110° | 2 |
| 120° | 2 |
| 130° | 2 |
| 135° | 2 |
| 140° | 0 |
| 150° | 0 |
| 160° | 0 |
| 170° | 0 |
| 180° | 0 |
| 190° | 0 |
| 200° | 0 |
| 210° | 0 |
| 220° | 0 |
| 230° | 0 |
| 235° | 2 |
| 240° | 2 |
| 250° | 2 |
| 260° | 2 |
| 270° | 2 |
| 280° | 2 |
| 290° | 2 |
| 300° | 2 |
| 310° | 2 |
| 315° | 2 |
| 320° | 1 |
| 330° | 0 |
| 340° | 0 |
| 350° | 0 |

Table 9: Experiment 2: measurements angle. The angle has a measurement error of 5°.

## 9.3 Appendix III

In this section we included the results of the measurements we did during experiment 3.

| **Range** | **Times of successful identification** | **Card identified** |
|---|---|---|
| 1 cm | 2 | Middle |
| 2 cm | 2 | Middle |
| 3 cm | 0 | None |
| 4 cm | 0 | None |
| 5 cm | 0 | None |
| 6 cm | 0 | None |
| 7 cm | 0 | None |
| 8 cm | 1 | Top |

Table 10: Experiment 3: exact measurements of three smart cards within the range of the NFC antenna. The smart cards are placed above each other. The ranges have a measurement error of 5 mm.

| **Range** | **Times of successful identification** | **Card identified** |
|---|---|---|
| 1 cm | 2 | Middle |
| 2 cm | 1 | Middle |
| 3 cm | 1 | Middle |
| 4 cm | 2 | Middle |
| 5 cm | 1 | Middle |
| 6 cm | 1 | Middle |
| 7 cm | 0 | None |
| 8 cm | 1 | Middle |

Table 11: Experiment 3: exact measurements of three smart cards within the range of the NFC antenna. The smart cards are placed next to each other. The ranges have a measurement error of 5 mm.

| **Range** | **Times of successful identification** | **Card identified** |
|---|---|---|
| 1 cm | 0 | None |
| 2 cm | 0 | None |
| 3 cm | 0 | None |
| 4 cm | 0 | None |
| 5 cm | 0 | None |
| 6 cm | 0 | None |
| 7 cm | 0 | None |
| 8 cm | 0 | None |

Table 12: Experiment 3: exact measurements of three smart cards within the range of the NFC antenna. The smart cards are placed on top of each other. The ranges have a measurement error of 5 mm.