A HARDWARE-ENABLED CERTIFICATE OF AUTHENTICITY SYSTEM WITH INTRINSICALLY HIGH ENTROPY

A Dissertation
Presented to
The Academic Faculty

By

Vasileios Lakafosis

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
in
Electrical and Computer Engineering

School of Electrical and Computer Engineering
Georgia Institute of Technology
May 2013

A HARDWARE-ENABLED CERTIFICATE OF AUTHENTICITY SYSTEM WITH INTRINSICALLY HIGH ENTROPY

Approved by:

Dr. Manos M. Tentzeris, Advisor
Professor, School of ECE
Georgia Institute of Technology

Dr. Edward Gebara
Adjunct Professor, School of ECE
Georgia Institute of Technology

Dr. Gregory D. Durgin
Associate Professor, School of ECE
Georgia Institute of Technology

Dr. Darko Kirovski
Quant Researcher
Jump Trading

Dr. Mark Allen
Professor, School of ECE
Georgia Institute of Technology

Date Approved: March 13th, 2013

To my parents, Dimitris and Evgenia, my sister, Paraskevi, and Eleni

ACKNOWLEDGMENTS

Writing down these lines helps me realize how fortunate I am to have met and have been supported in this academic journey of mine by so many people. They have given me so many wonderful moments I will cherish forever. First and foremost, I will always be grateful to Prof. Tentzeris, my advisor, for the many opportunities he so generously provided to me to expand my knowledge and experiences. I deeply thank him for his guidance, his proven trust in me in many aspects of the academic life and often making great challenges look simple. He taught me how important working efficiently and with confidence is to be successful. I would also like to express my gratitude to Dr. Gregory Durgin, Dr. Edward Gebara, Dr. Mark Allen, and Dr. Darko Kirovski for serving as my Ph.D. committee members and for their thoughtful feedback on my Thesis. I am indebted to Dr. Kirovski and Dr. Gebara; their truly uninterrupted support, expert advise, enthusiasm and encouragement have been crucial in the completion of this dissertation. This Ph.D. would have not started at all without the help and encouragement of my undergraduate advisor at the National Technical University of Athens, Nikolaos Uzunoglu. His laconic look and consenting smile at me during our discussions has been a great thrust toward embarking on this journey. I cannot also thank enough Dr. Mostafa Ammar and Dr. Ellen Zegura with the Computer Science department for their valuable time to so kindly provide me with perspectives, when I needed them.

Sangkil Kim, Taoran Le, Trang Thai, Amin Rida, Benjamin Cook, Hoseon Lee, Cong Shi, Danilo de Donno, Daniela Staiculescu thank you all for being great colleagues, lab mates and friends! I owe special thanks to my collaborator and friend, Rushi Vyas, for the endless discussions, the generous help in research and sharing all moments, both the good ones and the difficult ones.

I am also grateful to Microsoft Research, the Georgia Electronic Design Center, the

Cisco Research Center, the New Energy and Industrial Technology Development Organization and the Gerondelis Foundation for providing the grants to support this research work and myself during all these years. It has also been an honor for me to be a Lilian Voudouri fellow. Daniel Alvarez and Suyash Sinha have been great internship mentors at Cisco and Microsoft Research, respectively. I am also thankful to Dimitris Mitsainas, my manager at Intracom Telecom, for his trust in me from the very first moment and his endorsement to pursue graduate studies.

Life in Atlanta was enjoyable because of many friends. I couldn't have hoped for a better roommate the five years of this journey than Vangelis Farantatos. He has supported me more than he thinks, especially with his great memory! I also need to thank Niko Vasiloglou and Vicki Papanikolaou for so generously offering me my first and last "home" in Atlanta; as well as... their cars whenever I asked – no questions asked! Their house always offered a family atmosphere in Atlanta. I have many great times to remember with Giorgos Stefopoulos, George Georgoulas, Michael Balchanos, Yannis Doudalis, Yorgos Amanatidis, Yannis Raptis, Spyros Pavlidis, Yorgos Drakopoulos, Andreas Katsiamis, Ioanna Dafermou, and Stephane Ntwoku. I would have never expected to say that in my first year, as my then roommates Ola Gustafson and Philipp Andersch can attest, but Atlanta has been a super cool city! Jonathan Pan you contributed to this too man! The time outside Atlanta and all over the world has been exciting because of Babis Papamanthou (at Seattle and at Mountain View with his invaluable support during tough times), Luca Amati (at the Bay Area), Dr. Yoshihiro Kawahara, Dr. Tohru Asami, Hiroshi Nishimoto, Yun Li, Tashi Phuntsho and Lyubo Valnarov (at Tokyo) and my friends in Greece George Sobonis, Kostas Zachos, Dimitris Kyriakopoulos, and Kostas Kremyzas. Since my early undergraduate times and regardless of the distance, Giannis Giannakakis has always been a friend to talk to on the other line of the phone and a continuous source of joy.

I owe too much to my parents, Dimitris and Evgenia, for their endless love and numerous sacrifices. The education they were able to provide me with, the values they instilled

in me and the motivation they gave me have been the greatest gifts. My appreciation, of course, goes to my sister Evi, with whom I wish I could be spending a lot more time.

This final paragraph is for my beloved Eleni. No words can express my deepest gratitude for everything that has kept me going; her love, patience, support, and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

Counterfeiting affects many different sectors of the world trade, including the pharmaceutical and the aerospace industries, and, therefore, its impact is not only of financial nature but can also have fatal consequences. The objective of the proposed research is the design and fabrication of a novel stand-alone wireless robust system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities. The system consists of two major components: (a) the near-field certificates of authenticity, which serve as authenticity vouchers of the products they are attached to, and (b) a microcontroller-enabled, low-power and low-cost reader.

Out of the plethora of objects in nature that are of random, but unique, shape and composition, and hard-to-copy at some degree, passive physical structures that behave as extremely reliable *certificates of authenticity* (*CoA*) or *instances of proof of value* are identified. Specifically, the two different types of small-sized physical three-dimensional structures identified are composed of extremely cheap conductive and dielectric material. These structures are shown to yield a unique and repeatable RF signature in a small portion of the spectrum, when brought in the reactive and radiating near-field regions of an array of miniature antennas. The multidimensional features of these CoAs, or in other words their *signature* or *fingerprint*, are cryptographically signed and stored into any type of tiny embedded storage chip preferred to ensure reliable and convenient offline validation. Eventually, the certificate instances of fixed dimensions may be integrated as an inseparable part of the surface of a physical object or may simply be attached as a tag, a label or a seal to objects, the value of which is to vouched for.

The contactless signature validation procedure, in which an attempt to associate the near-field signature response of the physical CoA with the digitized signature that is signed by the issuer and stored into the aforementioned tiny embedded storage chip, is carried out by a reader. Toward the goal of a widest application adoption possible, the third and

latest generation reader designed and fabricated operates autonomously and in an offline (no Internet connectivity) fashion, exhibits enormous performance robustness, in terms of accuracy, consistency and speed of capturing of the signatures, has dimensions comparable to that of a human palm and also meets the requirement of low cost.

The system comprising the above two major components is fully characterized and its feasibility and performance robustness is rigorously assessed with a wide array of tests. Based on these results, the similarity detection threshold used during the validation procedure is evaluated and determined to be in the vicinity of the boundaries of the physical limitations of the reader hardware. Moreover, the entropy, or uncertainty, of the signatures generated by the NF-CoA system are empirically quantified and verified with the existence of a point on the receiver operating characteristic curve that almost corresponds to the (0, 1) "perfect classification" point within the context of the binary classification problem of the verification procedure. Furthermore, the feasibility of the "null hypothesis," according to which the NF signatures are potentially generated by a true random number generator, is supported by conducting and passing the majority of the tests of one of the most stringent and highly regarded, by industry and research community alike, test suites, the National Institute of Standards and Technology Statistical Test Suite (NIST STS). Finally, an example of a real super-positioning attack launched that the NF-CoA system successfully withstands is presented.

On top of the main functionality of the NF-CoA instances and given that the integration of localization into tiny sensors is rapidly becoming a necessity, the addition of location tracking capabilities to the NF-CoA instances is sought after. Within the context of this effort, the first two real-world WSN-enabled multi-lateration localization testbeds to evaluate the provision of an accurate location estimate of the certificate instances are built.

CHAPTER 1

INTRODUCTION

1.1 Problem Statement

In contrast to *piracy*, where the customer knows that the object he is buying is not genuine usually because of its very low price, in *counterfeiting* the adversary fools the buyer into believing that the merchandise is authentic and, as a result, the counterfeiter collects significant profit margins.

Counterfeiting exists since the very first days of trading and exchanging. For example, historians possess evidence of counterfeit coins of the world's first coin, the Lydian electrum trite [2], made of a gold and silver alloy and minted by King Alyattes in Sardis, Lydia, Asia Minor back in circa $610-600$ BC. Greek drachma and Roman denarius fourrée coins, i.e., coins made from a base metal core that has been plated with a precious metal to look authentic [3], have also been found. Revealing the interior metal with test cuts, that is, slashing of the surface of a coin with a hammer, was the first counterfeit detection procedure [4]. To try to prevent detection, early counterfeiters made coins that already had engraved fake test cuts.

There is no doubt that counterfeiting has a huge economic impact. The World Customs Organization estimated counterfeiting as a $512 billion market in 2004 [5]. The Counterfeiting Intelligence Bureau estimated that nearly 8% of world trade every year concerns counterfeit goods [5]. Undoubtedly, counterfeiting amounts to a huge economic impact on industries, such as the entertainment, fashion, and software. The organization for Economic Cooperation and Development (OECD) has dissected the effects of counterfeiting, among others, on innovation and growth, employment, trade, and on governmental operations, such as tax collection and corruption [6]. The volume of counterfeits is estimated nowadays to be in the range of half a trillion U.S. dollars annually, or roughly about one

quarter of the gross domestic product of the entire African continent. A 2010 study estimated that the volume of counterfeit U.S. currency in the form of banknotes, i.e., paper currency, in circulation worldwide is in the neighborhood of $60 to $80 million [7]. In Europe, almost one million counterfeit euro banknotes were removed from circulation just in 2011 by the European Central Bank [8]. Approximately 8.1 million Americans, or 3.5% of the total U.S. population, experienced fraud in 2010 [9]. At a global level, the "Global Card Fraud" Nilson Report estimated card fraud losses at $6.89 billion on $14.6 trillion in purchases of goods and services and cash advances in 2009 and projected the amount of fraud losses to rise to $10 billion by 2015 [9].

Unfortunately, however, the impact of counterfeiting is not only one of a financial nature. The numbers get scary when counterfeiters attack industries, such as the pharmaceutical and aerospace industries. In a study of Glaxo-Smith-Kline with the U.S. Food and Drug Administration it was estimated that counterfeit drugs make up 10% of the global pharmaceuticals market [10]. The U.S. Federal Aviation Authority estimated that each year, 2% (520,000 parts) of the 26 million parts installed on airplanes are counterfeit [11]. From 1973 to 1993, fake parts were responsible for at least 166 U.S.-based aircraft accidents. Four of these accidents involved commercial carriers that resulted in six deaths [11].

The aforementioned tremendous impact of counterfeiting is also reflected in the emergence of the *Anti-Counterfeiting Trade Agreement* (*ACTA*) [12], a multinational treaty that creates a new governing body. As expected, large intellectual property based organizations have been active in the development of ACTA. Despite the criticism the treaty is still receiving, ACTA supporters have described the agreement as a response to "the increase in global trade of counterfeit goods and pirated copyright-protected works."

Consequently, solutions that can address these problems are needed. In the battle against counterfeiting, traditional two-dimensional solutions, such as black-and-white and color barcodes, watermarks or holograms, or radio frequency identification (RFID) tags with encoded digital information cannot be relied upon since they can easily be replicated,

altered or distorted. Instead, extremely reliable and robust certificates of authenticity, or, in other words, instances of proof of value, that can be used conveniently may prove valuable. Motivated by the recent patent of DeJean and Kirovski [13], this dissertation attempts to further study, substantiate, realize, prove and, eventually, advance the exploitation of the intrinsically highly complex to predict near-field electromagnetic scattering effects toward creating inexpensive physical objects that are both digitally and physically unique and behave as certificates of authenticity (NF-CoAs). The full implementation of a novel *near-field* (*NF*) anti-counterfeiting system that aims to address counterfeiting in a hardware-based way is presented in this document. As demonstrated, this system enables the offline verification of the authenticity of a product within its near field with extremely low probability of a false alarm.

1.2 Research Objectives

The objectives of this research work can be summarized into the design and fabrication of a novel and robust stand-alone wireless system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities. The novelty of this system is the exploitation of the intrinsically highly-complex near-field (reactive and radiating) electromagnetic scattering effects that enable the creation and verification of hard-to-forge objects.

The majority of the objects in nature are of random, but unique, shape and composition, and hard-to-copy at some degree. Therefore, investigating passive physical structures that behave as extremely reliable and robust *certificates of authenticity* (*CoA*) or *instances of proof of value* constitutes a major effort of the proposed research. Essentially, the unique, conductive and dielectric, physical three-dimensional structure of the certificate instances is to yield a unique and repeatable RF signature in a small portion of the spectrum when the certificate is brought in the reactive and radiating near-field areas of an array of miniature antennas. The multidimensional features of these CoAs, or in other words their *signature* or *fingerprint*, are to be cryptographically signed and stored into any type of tiny embedded

storage chip to ensure reliable and convenient offline validation. The certificate instances of fixed dimensions may be integrated as an inseparable part of the surface of physical objects or may simply be attached as a tag, a label or a seal to objects that are to be protected. Despite the very low cost of the instances on the order of a few cents of U.S. dollars, it is highly desired that it is infeasible or prohibitively expensive for an adversary to reproduce the electromagnetic fingerprint of an NF-CoA with enough accuracy.

The contactless validation procedure, in which an attempt to associate the near-field signature response of the physical CoA with the digitized signature that is signed by the issuer and stored into a complementary tiny embedded storage chip, is to be carried out by a reader. As in the case of the certificate instances and for a wide adoption to be possible, the reader may also meet the requirement of low cost (on the order of less than 75 U.S. dollars). Meanwhile, it is also required that the reader can operate autonomously and in an offline (no Internet connectivity) fashion, exhibits enormous performance robustness, in terms of accuracy, consistency and speed of capturing the signatures, and has dimensions comparable to that of a human palm.

The system comprising the two major components of CoAs and the reader is to be characterized and its performance is to be thoroughly tested. The system assessment is required to involve rigorous empirical analysis, with regard to uniqueness among different instances and repeatability robustness for same instance, entropy estimation making use of the most reliable statistical methodologies and universally respectable third-party test suites and a study on how the system can withstand potential malicious attacks.

On top of the main functionality of the NF-CoA instances and given that, according to the vision of the *Internet of Things*, the integration of localization into tiny sensors is rapidly becoming a necessity, the addition of location tracking capabilities to the NF-CoA instances is to be sought after.

1.3 Dissertation Outline

The outline of the remaining parts of the dissertation is as follows.

A thorough literature survey that summarizes the related state-of-the-art research work efforts in the areas of anti-counterfeiting and highlights the differentiation and novelty of the NF-CoA system is presented in Chapter 2.

The many-fold rationale behind focusing on the near-field observation of the electromagnetic phenomena is presented in Chapter 3. In the same chapter, NF-CoA-related definitions that are necessary for the remainder of the document are provided.

The design and fabrication of two different types of NF-CoA instances that yield unique and highly-divergent NF fingerprints are presented in Chapter 4. Regardless of the type, the entire life cycle of a certificate instance, spanning from the fabrication process (issuing) to the point where it is used for identity validation or genuineness authentication (verification process), is also outlined in the same chapter.

The NF-CoA reader is introduced in Chapter 5. In particular, the evolution over three different generations of mixed-signal boards is presented, emphasizing on the advancements brought by each generation. The full characterization of the analog and digital parts is described and the operational state diagram of the firmware algorithm developed is illustrated.

A wide array of measurements and tests to assess the feasibility and performance of the proposed authenticity certification system is presented in Chapter 6. Among these tests are the uniqueness of each NF signature among different signatures and the repeatability robustness, according to which the same certificate instance always yields nearly exact replicate signatures.

Two major independent attempts to empirically quantify the entropy, or uncertainty, of the signatures generated by the NF-CoA system are elaborated in Chapter 7.

Potential key attacks are set forth in Chapter 8. In the same chapter, an example of a real attack launched against the NF-CoA system is presented.

Finally, the main outcomes and contributions of this research work are summarized in Chapter 9, where future research directions are also indicated.

In the Appendix, a localization service for the location estimation of the NF-CoA instances and two of its real-world realizations are presented.

CHAPTER 2

LITERATURE REVIEW

2.1 Anti-counterfeiting Techniques

2.1.1 Two-dimensional Printed Solutions

The majority of the anti-counterfeit methods that have been implemented in the market to this point are of a two-dimensional (2D) style. Black-and-white or color barcodes, magnetic strips, watermarks and holograms constitute such examples that have been successfully attacked, i.e. copied, altered or distorted.

2.1.2 Software-only-based Solutions

Moreover, researchers soon realized that software-only-based solutions could also not be relied upon in the fight against counterfeiting. The use of RFID tags against counterfeiting has been proposed in the past. Traditional RFID tags with encoded digital information can easily be replicated, which means that a complete image of the memory of the RFID tag chip in bit level can be extracted and copied onto other blank RFID tag chips, regardless of if its content is encrypted, signed and/or hashed. On top of that, security groups have demonstrated successful attacks against even enhanced "symmetric-key" RFID tags that are capable of computing cryptographic symmetric-key functions [14]. The same survey, however, cites research proposals to close these security gaps.

2.1.3 Fiber-based Solutions

It was soon concluded that hardware-based CoAs comprise a more effective solution to the problem. Bauder [15] and Simmons [16] proposed CoAs that consist of fibers, the positioning of which is fixed. The principle of operation is based on illuminating one end of a fiber and detecting the resulting glow on the other end using photo detectors. Among only few other efforts, Church et al. [17] proposed the extraction of the random optical-fiber patterns as a currency anti-counterfeiting application and Chen et al. [18] combined for the

first time the fiber-infused paper solution with public key cryptography. While efficient and inexpensive, this category of fiber-based CoAs does not provide a "physical one-way function." In other words, given the fingerprint of a particular fiber-based CoA, it is not computationally difficult to construct an object of the same fixed dimensions that yields an almost identical fingerprint. This is primarily due to the linearity of the CoA as a system and the lack of interdependence among the responses of distinct fibers; since the glowing of a single fiber does not dependent on the response of the remaining fibers of a fiber-based CoA, an adversary can launch a super-positioning attack, i.e., a simple search process that orients these fibers one by one.

Loading magnetic nanoparticles in cellulose fibers with the purpose to produce paper with super-paramagnetic properties that can serve as a signature for authentication purposes has also been proposed [19, 20]. The solutions incur not only a high cost for fabricating the certificate instances, involving processes, such as in situ synthesis and lumen loading methods [20], but also the authentication methods under this category are limited to the detection of just the presence of the magnetic loading.

2.1.4 Physical Unclonable Functions

The so-called *physical unclonable functions* (*PUF*) constitute essentially a mapping between a set of specific challenges applied to a physical, complex structure and their corresponding responses and are used to produce unclonable tokens for identification purposes. Pappu [21] proposed speckle scattering as one example of physical unclonable functions. Pappu focused on the natural randomness collected from a speckle pattern; a random intensity pattern produced by the mutual interference of coherent wavefronts that are subject to phase differences or intensity fluctuations. Skoric [22] was able to show experimental and theoretical results on the randomness yielded by speckle-formed keys that are in good agreement. Since speckle scattering is sensitive to small spatial differences in the placement of the source of scattering and requires an expensive micro-fabrication technology, building such CoAs that satisfy robustness seems to be a difficult task; in addition, speckle filtering

is not clearly shown to guarantee repetitiveness robustness of the extracted fingerprint.

Under the same PUF category falls also the proposal of Tuyls and Batina [23] to fabricate RFID-tags, the microchips of which are equipped with an additional PUF physical structure that inherently incorporates unpredictable, manufacturing process inaccuracies. Although not supporting off-line scenarios as in [23], an actual fabrication of a PUF-enabled RFID chip in 0.18 μ technology is presented in [24]. The operation of this type of CoAs is not passive as it consumes small, yet perhaps not negligible, power from the tag chip, hence potentially decreasing its read range. Their fabrication is also coupled with the RFID tag chip fabrication process. Furthermore, all the above PUF-based CoAs require access to non-reusable, one-time challenge-response pairs through online Internet connections with the potential added overhead of recharging the online challenge-response database. As a result, the PUF solutions also rely on some kind of cryptographical encryption to ensure the security of the Internet online query transactions.

2.1.5 Far-field-based Solutions

In the far-field communication domain, researchers proposed identifying an individual UHF RFID tag and a tag's manufacturer based on timing, power, and voltage features extracted from the tags' transmitted signals [25]. Researchers have also proposed applications that detect the response of the random structure of the certificate over the expensive millimeter wave frequency range [26].

Under the same far-field category also fall the chip-less RFID tags proposed for authentication applications. However, their common main shortcoming is that the entropy they provide is only limited to a two-digit bit-sequence. For instance, Preradovic et al. [27] demonstrate a printable chip-less RFID tag for secure banknote applications in the 5 GHz to 7 GHz frequency band, the anti-counterfeiting robustness of which relies on a bit sequence formed by a multi-resonating circuit and CrossID, Inc [28] has tested a chip-less, chemical-material-based RFID tag using 3 GHz to 10 GHz readers with each of the 70 different chemicals being assigned its own position in a 70-digit binary number.

The major limitations of the above far-field authentication schemes are the requirement of a constant distance with the same reference between the reader and the certificates for signature repetitiveness and potential interference, eavesdropping and/or malicious jamming of the far-field channel. Moreover, the entropy results of the work in this area typically exhibits relatively low true positive rates (TPRs – see Chapter 7).

2.1.6 Near-field-based Solutions

Finally, regarding the **near-field domain** under which the NF-CoA system also falls, researchers have attempted to quantify the electromagnetic characteristics of the near-field coupling nature of ISO 14443 RFID transactions [29] or chip-less RFID tags for counterfeit detection applications. The researchers actually make use of expensive real-time oscilloscopes with a sampling rate of 20 GHz to measure a fine electromagnetic signature that consists of the fundamental and harmonics up to the ninth harmonic of a 13.56 MHz RF carrier. This method not only incurs a very high cost for the "reader" but also requires a closed-loop, synchronized control system between the RFID reader and an oscilloscope in addition to potential RFID reader software modifications.

2.1.7 Summary/Comparison

Table 1: Anti-counterfeiting techniques

Category	*Technology*	*Limitations*
Two-dimensional (2D) Printed Solutions	Black-and-white or colorful barcodes, magnetic strips, watermarks and holograms	⇒ Successfully attacked (copied, altered or distorted)
Software-only-based Solutions	Traditional RFID tags with encoded digital information	⇒ Easily replicated (regardless of encrypted, signed and/or hashed content)
	Symmetric-key RFID tags (computing symmetric-key functions)	⇒ Already successfully attacked [14]
Fiber-based Solutions	Optical fibers fixed on an object (yield random optical-fiber patterns)	⇒ Easy to attack with inverse design via super-positioning (linearity, no interdependency of fibers)
	Magnetic nanoparticles in cellulose fiber	⇒ Detection of just the presence of the magnetic loading ⇒ Expensive in situ synthesis and lumen loading methods
Physical Unclonable Functions (PUFs)	Optical speckle scattering	⇒ Sensitive to small spatial differences in the placement of the source of scattering ⇒ Repetitiveness fully addressed? ⇒ Expensive micro-fabrication technology ⇒ CoA fabrication coupled with microchip fabrication process ⇒ Need to contact online challenge-response database (no offline authentication) ⇒ Overhead of (re)charging the database with non-reusable, one-time PUF pairs
	RFID-tags in 0.18μ technology equipped with an active circuit structure	

Far-field-based Solutions	Over UHF measuring timing, power, and/or raw signal features	⇒ Constant distance with same reference required ⇒ Interference, eavesdropping and malicious jamming of the far-field channel ⇒ Typically low TPRs ⇒ Average characteristics of random discrete scatterers ⇒ Expensive if conducted over the millimeter-wave (typically > 60 GHz)
	Chip-less RFID tags with multi-resonating circuits printed on banknotes (5 - 7 GHz) Chip-less, chemical-material-based (70 different chemicals) RFID tag using 3 - 10 GHz readers	
	Millimeter wave (mm-Wave) frequency range	
Near-field-based Solutions	Coupling of ISO 14443 RFID transactions measuring the fundamental and harmonics up to the 9^{th} harmonic of a 13.56 MHz RF carrier	⇒ Expensive real-time oscilloscope (sampling rate of 20 GHz) needed ⇒ Closed-loop, synchronized control system between the RFID reader and an oscilloscope ⇒ RFID reader software modifications
	Chip-less RFID tags	

2.2 Differentiation/Strength of the NF-CoA System

The realized NF-CoA system, the operation of which relies on the near-field observation of the electromagnetic scattering effects on the physical three-dimensional objects that serve as certificate instances, possesses some important qualitative features not exhibited by other types of CoAs. The superiority of the designed, proposed, developed, and tested NF-CoA technology over other proposed hardware-based CoAs or PUFs is summarized in the following points:

- The detection of the random structure and signature of a CoA does not occur in the far field, which
  - represents averaged-out characteristics of random discrete scatterers [30],
  - can be eavesdropped,
  - can be subject to interference or can be maliciously jammed,
  - is very expensive if conducted over the millimeter-wave (typically 60 GHz) frequency range.
- The NF-CoA solution relies on the near-field observation of the electromagnetic scattering effects on the CoAs, where the relationship between the electric field component $\overline{E}$ and the magnetic field component $\overline{H}$ becomes often too complex to predict, as described in detail in Section 3.5.
- The NF-CoA system can withstand a wide range of considered attacks that can be launched by malicious counterparts, including data replication of the stored digitized NF signature or replacement of the latter with another signature, numerical computation of a captured (with an NF-CoA reader) valid NF signature and the superpositioning attack in an effort to obtain a desired near-field response. For a detailed analysis see Chapter 8.

- The overall cost of a complete NF-CoA system is extremely low. In particular, even before considering the *economies of scale* for massive fabrication of the readers, the sum of the cost of all the components of the designed and fabricated NF-CoA reader does not exceed 75 U.S. dollars. Regarding the cost of a single certificate, that is lower than the price of a typical passive RFID tag on the order of a few cents of U.S. dollars.

- No expensive micro-fabrication technology is required for the certificates. In addition, the fabrication of the CoAs is decoupled from the potential accompanying RFID chip fabrication process.

- The operation of the NF-CoA reader can be low power.

- The NF-CoA physical identifiers are completely passive, i.e., not consuming any power from the potential accompanying embedded storage chip or RFID tag chip and, as a result, not decreasing the latter's back-scattered power and, effectively its "read" range.

- The NF-CoA solution is compatible with any RFID technology or other physically small and low-cost embedded storage devices with "read" capabilities. In the RFID case, any RFID tag of any frequency can be used with a reasonable amount of RFID tag chip storage, as discussed in Section 4.2.

- No physical certificate "wear and tear" is expected since the NF-CoA signature readout does not involve physical contact with the reader.

- In the case of relying on the RFID technology, no reader software modifications are required.

- No oscilloscope or other expensive high-frequency reader is required to capture any frequency harmonics.

- The NF-CoA authentication and issuance processes are meant to take place entirely locally and off-line, without looking up an online database.

- The NF-CoA technology does not rely on non-reusable, one-time, PUF-style challenge-response pairs. On top of that, the overhead of charging and recharging the challenge-response database, as is the case with the PUF solutions, does not exist.

- The NF-CoA technology requires no closed-loop, synchronized control system between the technology, wired or wireless, that is used to extracted the bit sequence of the stored signed signature, such as an RFID reader, and an oscilloscope or any other expensive measurement instrument.

- Electromagnetic compatibility (EMC) issues (both potentially caused by the NF-CoA system and received by third-party sources) are not expected both because of the low signal power levels transmitted and because the antenna array slot and the back side of the reader can be shielded.

CHAPTER 3

THE NF-COA SYSTEM

3.1 Near-field (NF) Electromagnetic Characteristics

The space around an antenna is subdivided into the reactive near field, the radiating near field, and the far field. No rigid boundaries between these regions exist. The fields do not change abruptly from one region to the other, but undergo a very gradual transition [31]. Nevertheless, distinguishing these regions simplifies the formulation to yield closed-form solutions of Maxwell's equations. Several boundary distinction criteria have been established [32]. Two of the most popular are described below.

According to the most popular approach, the boundary between the near and the far field is the distance from the antenna at which the wave impedance, i.e., the ratio of the electric field magnitude $\overline{E}$ to the magnetic field magnitude $\overline{H}$, changes [31, 33]. In the far field, $\overline{E}$ and $\overline{H}$ are related by the characteristic impedance of the medium, which is $\eta = 120\pi\ \Omega$ for a vacuum. Conversely, in the near field, the wave impedance is not constant; the wave impedance is high (high $\overline{E}$ and low $\overline{H}$) when the radiator is a dipolar source and low (low $\overline{E}$ and high $\overline{H}$) for a loop-like structure [34]. This approach is valid for most practical antennas with a maximum dimension D greater than a wavelength λ ($D > \lambda$). In this scenario, a maximum total-phase error of $\pi/8$ rad (22.5°) is not very detrimental in the analytical formulations [31].

For electrically small antennas ($D < \lambda$), an alternative approach based on the power density dissipation behavior of the fields is more appropriate for defining the electromagnetic region boundaries [33]. In the near field, the small fractional values of the distance of the observation point from the source r cause the near-field magnetic and electric fields to exhibit $1/r^3$ and $1/r^2$ behavior, respectively. As the distance from the antenna increases, the $1/r$ term dominates in the far field for both $\overline{E}$ and $\overline{H}$ and the $1/r^3$ and $1/r^2$ terms attenuate rapidly. The distance where the $1/r$ and $1/r^2$ terms are equal is the most commonly

used boundary between near and far field. For an electric dipole, this distance is referred to as the radian distance, and this distance is equal to $\lambda/2\pi$. The sphere with radius equal to $\lambda/2\pi$, i.e., referred to as the radian sphere, defines the region within which the reactive power density is greater than the radiated power density [35].

More specifically, the three regions that surround an antenna are:

- **Reactive near field**: The area that immediately surrounds the antenna. The outer boundary of this area is at the distance of $r = 0.62\sqrt{D^3/\lambda}$ from the antenna surface [36, 37, 38, 39], where λ is the wavelength and D is the largest dimension of the antenna. For electrically small antennas, the more appropriate boundary is $r < \lambda/2\pi$ ($kr < 1$). The energy in this region is basically imaginary; the energy is stored, but not radiated. The reactive near field can be defined in terms of planar, cylindrical, or spherical modes [40].

- **Radiating near field (Fresnel)**: The inner boundary of this intermediate area is the same as the outer boundary of the reactive near field. The outer boundary of the same intermediate area is at the radial distance of $2D^2/\lambda$ from the antenna [36, 37, 38, 39]. Although for electrically small antennas this region may not exist at all [36], the more appropriate boundary is $r > \lambda/2\pi$ ($kr > 1$). This region is also called Fresnel, because the field expressions in this region reduce to Fresnel integrals. Here, the radiating power density is greater than the reactive power density, and the angular field distribution, i.e., the shape of the antenna field pattern, is dependent upon the distance from the antenna. Additionally, there is no reactive power any more, and the wave impedance is equal to η. The electric and magnetic fields tend to propagate predominantly in phase, but do not exhibit e^{ikr}/r dependence until the far field is reached. The r variations of the $\overline{E}$ and $\overline{H}$ field components are not separable from those of θ and ϕ. Finally, no transverse electromagnetic (TEM) wave exists in this region, and the radial field component may be substantial [31].

- **Far field (Fraunhofer)**: The area that extends from $2D^2/\lambda$ to infinity. For electrically small antennas, the more appropriate boundary is $r \gg \lambda/2\pi$ ($kr \gg 1$). E_θ and H_ϕ are the components of the spherical wave, and E_r is negligible. In other words, the electric and magnetic fields are transverse, and the wave front is plane. The radiation pattern is independent of the distance from the antenna, and the radial dependence of electric and magnetic fields varies approximately as e^{ikr}/r.

The antenna radiation pattern changes in shape, as the observation moves from the near field to the far field. The pattern is nearly uniform in the reactive near-field region and only begins to form lobes in the radiating near-field region [31, 41].

The boundary values of the three electromagnetic regions following both popular aforementioned approaches for an antenna element with its maximum dimension equal to $\lambda/8$ are provided in Table 2. This antenna dimension and, consequently, the frequency operation have not been chosen randomly. The folded shorted-patch antenna element of the antenna array of the NF-CoA reader has a frequency of operation that ranges from 5 GHz to 6 GHz.

Table 2: The boundaries of the reactive near-field, the radiating near-field (Fresnel), and the far-field (Fraunhofer) areas surrounding the antenna element of the reader array are shown in this table. The largest dimension of the element is equal to D.

$D = \lambda/8 = 6.81$ mm	Frequency (GHz)				
	5.00	5.25	5.50	5.75	6.00
Wavelength λ (mm)	59.96	57.10	54.51	52.14	49.97
Reactive near field up to (mm)	1.42	1.46	1.49	1.53	1.56
Radiating near field up to (mm)	1.55	1.63	1.70	1.78	1.86
Radian distance $\lambda/2\pi$ (mm)	9.54	9.10	8.68	8.30	7.95

As noted previously, the boundaries of the different radiation regions are in no case abrupt or even totally agreed upon by different researchers. Actually, there is a large set of definitions of the near-field/far-field boundaries in the literature [33]. In addition to the two most popular approaches described above, Yaghjian [40] and Huang and Boyle [42]

introduce corrections, $2D^2/\lambda + \lambda$ and $\max\{3\lambda, 2D^2/\lambda\}$ respectively, to cover the possibility of the maximum dimension of the antenna being smaller than a wavelength. The boundary between near and far field is 3λ in [38, 43] when D is not a lot larger than λ. According to section C of a U.S. military standard [43], the near-field/far-field boundary is $2D^2/\lambda$ if the maximum dimension of the transmitting antenna, d, is less than 40% of the maximum dimension of the receiving antenna D, otherwise the boundary is $(d + D)^2/\lambda$. The same boundary should also be considered according to section D of the same standard [43], but only if $d > 10 \cdot D$. Kaiser [44] suggests $4D^2/\lambda$ for high-accuracy antennas. Three different sets of boundaries of the electromagnetic regions (with the corresponding factors of the wavelength ranging from 1.6 to 12) are provided for short, $\lambda/2$, and λ dipoles in [45]. Finally, Kraus [37] and White [38] conclude that for different boundaries chosen ($\lambda/16$, $\lambda/8$ and $\lambda/4$) yield different measurement error (≤ 0.1 dB, ≤ 0.3 dB and ≤ 1 dB respectively).

The performance test of Section 6.2.2 sheds light on the dependence of the entropy of the signature response of the proposed certificate instances on the distance between the antenna array and the instance itself. Based on the results of this test, the optimum distance, in terms of a highest randomness in the signature response as possible, is chosen.

3.2 Electromagnetic Scattering

Whenever electromagnetic radiation encounters an obstacle, the radiation may be deflected or absorbed. For large objects, the deflection is considered to arise from reflection and refraction. These phenomena can be described with the aid of ray tracing or geometrical optics only if the far field is considered. Still, ray tracing and geometrical optics do not completely describe the interaction [46]. Diffraction, that is, the spreading out of radiation past a narrow aperture or across an edge as a result of the interference between the wave forms produced, also occurs. When the object is less than or of the order of the wavelength (λ), the interpretation is not simple, because wave optics analysis is required. The deflection process here is referred to as scattering. Scattering by obstacles depends upon their size, shape, and refractive index.

The exact solution to the problem of electromagnetic wave scattering relies on Maxwell's equations together with the associated boundary conditions. First, the example of a wave impinging upon the surface of a conducting wire scatterer is considered (Figure 1). Part of the incident electric field $E_i(r)$ impinges on the wire and induces a current density J_S (A/m) on the surface of the wire. For non-perfect conducting wires, as is the case in the real world, some part of the impinging field is absorbed. The induced current density reradiates and produces an electric field that is referred to as the scattered electric field $E_s(r)$. At any point in space, the total electric field $E_t(r)$ is the sum of the incident and scattered fields, or $E_t(r) = E_i(r) + E_s(r)$.

The incident and scattered electric and magnetic fields are represented by the following radiation integrals:

$$\overline{E} = -j\omega\overline{A} - j\frac{1}{\omega\mu\varepsilon}\nabla\left(\nabla\cdot\overline{A}\right) \tag{1}$$

$$\overline{H} = -j\omega\overline{F} - j\frac{1}{\omega\mu\varepsilon}\nabla\left(\nabla\cdot\overline{F}\right) \tag{2}$$

where the vector potential A for the electric current source J is a solution of the inhomogeneous vector wave equation of

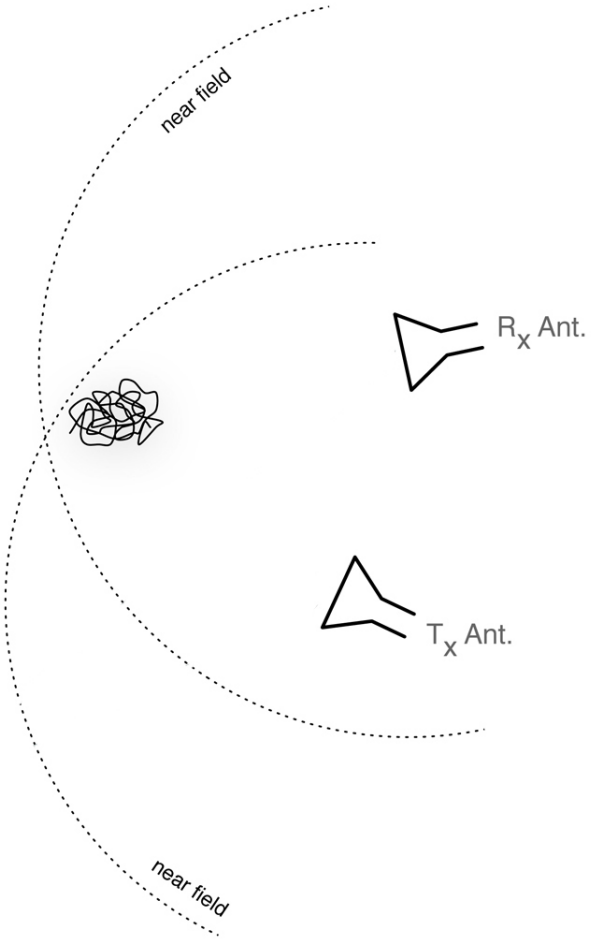


Figure 1: The schematic representation shows the near-field electromagnetic scattering on a randomly-shaped wire that is placed within the near field of a transmit (Tx) and a receive (Rx) antenna element.

$$\nabla^2 \bar{A} + k^2 \bar{A} = -\mu \bar{J} \tag{3}$$

and the vector potential F for the magnetic current source M is a solution of the inhomogeneous vector wave equation of

$$\nabla^2 \overline{F} + k^2 \overline{F} = -\varepsilon \overline{\mathrm{M}} \tag{4}$$

Especially for the scattered field, the electric vector potential stems from the aforementioned induced current J_S. Approximations regarding this current density are not possible

as this is not linear across any single Cartesian axis, the wire cannot necessarily be considered very thin so that an independence from the azimuthal angle ϕ can be assumed; not to mention that in some cases the wires are bent in such a degree that they assume a spheroidal or ellipsoidal form.

For an introduction to basic scattering theory regarding a more generic case, the Green's function needs to be introduced first. Although this function is primarily the solution of the field equation for a point source, the principle of linear superposition to find the solution of the field due to a general source can be used [47]. If the source is placed at a position represented by the primed vector r', as shown in Figure 1, the free space dyadic Green's function is given by

$$\overline{\overline{G}}\left(\overline{r},\overline{r}'\right)=\left(\overline{\overline{I}}+\frac{1}{k_o^2}\nabla\nabla\right)\frac{e^{ik_o\left|\overline{r}-\overline{r}'\right|}}{4\pi\left|\overline{r}-\overline{r}'\right|} \tag{5}$$

The Huygen's principle, which is an exact relation that expresses the field in a region of space as the fields on the surface that encloses this region, is derived from the vector Green's theorem. This means that the fields at any point in space can be determined if the surface fields are known. The relation that is known as the Huygen's principle is

$$\overline{E}_s\left(\overline{r}'\right)=\int_{S_1} dS\left[\overline{\overline{G}}\left(\overline{r},\overline{r}'\right)\cdot\widehat{n}\times i\omega\mu\overline{H}_i\left(\overline{r}\right)+\nabla'\times\overline{\overline{G}}\left(\overline{r},\overline{r}'\right)\cdot\widehat{n}\times\overline{E}_i\left(\overline{r}\right)\right] \tag{6}$$

It should be repeated that with this rigorous approach one needs to first specify $\widehat{n}\times\overline{E}$ on the surface S and then solve $\widehat{n}\times\overline{H}$ based on the boundary value problem before using the Huygens principle to calculate the fields everywhere.

In the above analysis, only single scattering has been considered, where the radiation is only obstructed by a single scatterer. In other words, the fact that the radiation may scatter many times as a result of spatially grouped-together, multiple scatterers (multiple scattering) has not been considered. For instance, in the example of the conducting wire described above, the presence of another wire in close proximity to the first one could also be assumed. In this scenario, the reradiated wave would also impinge on the second wire and would induce a current density J_{S_2} on the surface of the latter.

Of course, since a near-field approach has been opted for, no far-field approximations can be applied to the above equations. On the contrary, the difficulties in obtaining closed-form solutions that are valid everywhere, and even more anywhere between the boundaries of the reactive and radiating near-field regions, stem from the inability to perform the integration of the vector potentials $\overline{A}$ (3) and $\overline{F}$ (4).

3.3 The Near-field CoA Fingerprint

When the NF-CoA instance is brought in the near field of an array of miniature antennas, the *near-field* (*NF*) electromagnetic scattering effects are extracted in the form of unique and repeatable (reproducible) patterns of scattering parameters (S_{11} or S_{21}) (or even phase information) that constitute an electromagnetic signature response from the NF-CoA . Essentially, a set of these scattering parameters comprises the NF fingerprint or NF signature of the NF-CoA technology. In a more rigorous definition, the NF fingerprint of an NF-CoA $x_f \in \mathbb{R}^{N_{freq} \cdot \binom{M}{2}}$ is a set of S_{21} parameters over a frequency range and corresponding to a subgroup of or all available $\binom{M}{2}$ antenna couplings of the antenna array of a reader with M antenna elements. $\binom{M}{2}$ is the binomial coefficient that is equal to $M!/[2! \cdot (M-2)!]$.

A graphical representation of this fingerprint is shown in Figure 2 as extracted from the custom fabricated reader for all different antenna element permutations of the reader (here 72) using a signal-processing method described in detail in Chapter 5. The signature can be plotted over frequency (as in Figure 2) or alternatively over antenna couplings (as shown

in Chapter 6).

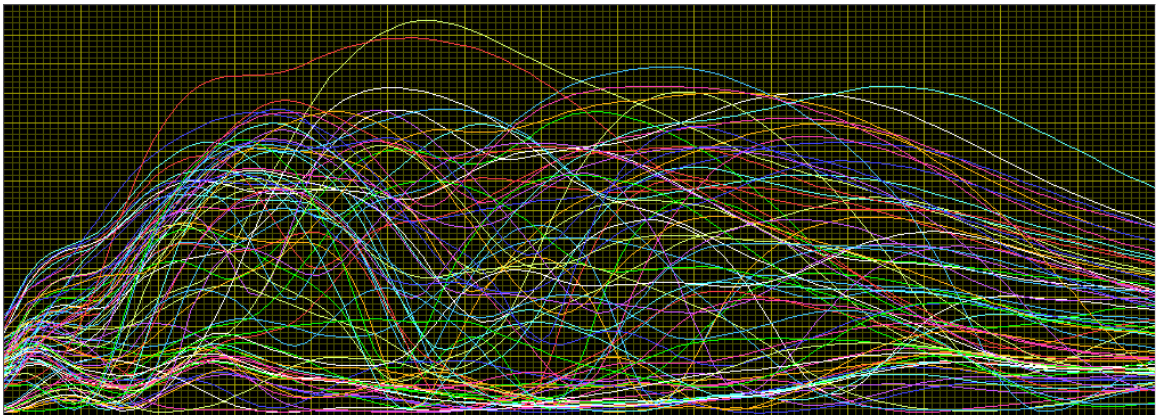


Figure 2: A graphical representation of an NF fingerprint, as extracted by the custom fabricated reader for all different antenna element couplings of the reader.

3.4 Definitions of the Major Components of the NF-CoA System

Certificate of Authenticity (CoA): A physical object that either vouches for its own genuineness and, as a consequence, also proves the genuineness and value of the product it accompanies or can serve as a seal proof.

NF-CoA : A physical CoA instance that consists of an extremely difficult to replicate, random arrangement of scatterers that produces a unique and repeatable response in the near field for anti- counterfeiting purposes. Because of its slim profile, the NF-CoA may be attached as a tag, a label or a seal to a physical object or may be integrated as an inseparable part of the surface of an object.

Near-field Electromagnetic Scattering: The deflection of an electromagnetic wave as it impinges upon an object (scatterer), when the latter has a size of less than or of the order of the wavelength and is located in the (reactive or radiating) near field of the transmitting antenna element.

NF Fingerprint / Signature / Response: A set of S_{21} parameters over a frequency range that corresponds to a subgroup of or all available antenna couplings of an array of a reader, when the NF-CoA is placed in the near field of the array.

NF-CoA Reader: A low-cost reader that can extract the signature of an NF-CoA instance, can verify the issuer of the content of the potentially accompanying storage chip or RFID tag and validate or not the authenticity of the instance.

3.5 Leveraging the Unique Near-field Scattering Properties for Increased Entropy

As will be described in detail in Chapter 4, the physical CoA instance consists of an extremely difficult to replicate, random arrangement of a conductive material, such as copper wire, mixed with a firm dielectric material, such as plastic PET mold, that produces a unique and repeatable response. For purposes of both mechanical practicality and higher complexity in theoretical analysis of the signature extraction that yields the security of the NF-CoA system, the CoAs have been deliberately brought in the near field of the antenna array of the reader; including both the reactive and the radiating areas presented in detail in Section 3.1 [48]. More specifically, the rationale behind opting for the near-field observation of the incurred electromagnetic effects is many-fold:

- Electric and magnetic fields require separate path link equations for like (electric-electric or magnetic-magnetic) and unlike (electric-magnetic or magnetic-electric) antenna links [49] that are different from the Friis Law [50]. Reception and transmission of an electric-field signal requires an electric antenna (e.g. a dipole), whereas reception and transmission of a magnetic-field signal requires a magnetic antenna (e.g. a loop).

- Within the near-field region, the relationship between the electric field component $\overline{E}$ and the magnetic field component $\overline{H}$ often becomes complex to predict, because either field component can dominate at any particular point [51]. Very close to the

antenna, the energy level can rise dramatically with only a small additional movement toward the antenna.

- The near-field observation enables relatively high variance of the EM field, causing better discriminating characteristics compared to the far-field responses.

- Measurement of both $\overline{E}$ and $\overline{H}$ is required to determine the power density, because the wave impedance in the near field is not constant (e.g. $\neq \eta = 120\pi\ \Omega$ in free space for vacuum) [51].

- The near-field antenna element coupling is complex. The coupling between the antennas affects the impedance of both antennas and the field distribution around them and the several near-field tangential and radial electric and magnetic field components can all contribute to coupling [52].

- The different definitions of the EM field boundaries render the prediction/simulation of near-field scattering effect very difficult. This complexity is more pronounced if the region, where the scatterer, is brought is very close to the boundary.

- In the near field the waves are spherical and not yet converted to plane waves, so there is no polarization.

- It is hard to eavesdrop or maliciously jam near-field communication, compared to far-field communication, which is prone to both potentially devastating attacks.

- The theory, measurements, and computer programming required to accurately characterize antennas by near-field scanning is considerably more extensive than for conventional far-field measurement [40].

3.6 Potential Applications

The NF-CoA instances, as vouchers for authenticity, are an essential security tool in a huge number of transactions and validations occurring on a daily basis. What enhances the applicability of the NF-CoA system and makes it particularly attractive for several applications [53] is the following set of features:

- The short physical profile, on top of the small 2D projection dimensions and negligible weight of the instances enables different ways of attaching the instances to products or documents, such as fastening them as labels, affixing them onto surfaces, or even embedding them inside the outer shell of various products.

- The NF-CoA instances can withstand wear-and-tear, mainly as a result of the contactless signature readout mechanism, as well as the firmness of their 3D structure.

- The cost of a single NF-CoA instance is expected to be on the order of a few U.S. dollar cents, and the prototyping cost of a single reader is lower than 75 U.S. dollars. Moreover, the implementation potential of the NF-CoA system is great considering that a) the low cost of the NF-CoA system can be pushed even further down with economies of scale and b) a significant part of trade losses can be eliminated as a consequence of counterfeiting.

- The issuing and verification procedures are inexpensive and very fast.

- The NF-CoA issuing can be realized either by storing the NF fingerprint into a large remote Internet database – the database could be queried to vouch for the authenticity of this tag, or by digitally signing the fingerprint using a public-key cryptosystem, such as RSA [54], and storing the signature into the storage associated with the tag, such as a barcode, an RFID chip, etc. While the first approach requires connectivity of the verification device, the latter can validate the authenticity of a given tag off-line, without any other additional communication device.

Depending on the additional information associated with an NF-CoA certificate instance, a vast array of applications can be supported. To provide a rough categorization of these applications, the objective of such a CoA is either to present value on its own (e.g., identity card, credit card, currency bill, ticket, warranty, etc.) or to be associated with a product whose genuineness it is aiming to certify. In the latter case, the tag can be attached (i.e., clothing, jewelry) or jointly molded with the product (i.e., packaging of an electronic device or medication) and cannot be reassembled if opened or torn.

CHAPTER 4

NF-COA INSTANCES

The *Certificate of Authenticity* (*CoA*) is defined as a physical object that may be integrated as an inseparable part of the surface of a physical object or can simply be attached to the object as a tag, a label, or a seal. The certificate can prove its own authenticity and, as a consequence, can also prove the authenticity and value of the product to which it is attached. In this chapter, the passive physical structures that behave as CoAs in an electromagnetic field, i.e., yield a unique signature in a portion of the electromagnetic radiation spectrum, are investigated.

The unique physical structure of the certificate instance is an arbitrary constellation of small, thin pieces of metallic conductors and/or one or more dielectric materials that are randomly dispersed and spatially fixed into a three-dimensional (3D) RF-wave-permeable dielectric fixative. The conductors may be copper, aluminum or other metal filings, and particle scatterers. The list of candidate materials for fabrication of these unique identifiers may also include non-linear materials, such as *ferrites* (ceramic compounds with ferromagnetic properties that show various kinds of anomalies in their power absorption at high microwave signal levels [55]) and *metamaterials* (artificial materials, the permittivity and permeability of which are both negative, resulting in a negative index of refraction, and, thus, in a phase velocity that is anti-parallel to the direction of the Poynting vector [56]).

The proposed NF-CoA is the first extremely low-cost physical object that enables unique identification and anti-counterfeiting capabilities based completely on the hardware implementation of the object. Not only do these completely passive, random unique physical NF-CoA structures cost a few cents of U.S. dollars, but also, because each NF-CoA instance is different, it is almost always infeasible or prohibitively expensive for an adversary to reproduce an NF-CoA with enough accuracy to successfully mimic the electromagnetic fingerprint that certifies authenticity. It is these benefits of physical near-field

authentication and the resiliency to potential attacks, as discussed in Chapter 8, that render the NF-CoAs ideal counterfeit deterrent candidates.

4.1 CoA Design and Fabrication

The design of the unique identification and anti-counterfeiting hardware certificates is challenging and has to be optimized as it determines the discrimination capability of the system, i.e., the entropy. At the same time, as described above and in Section 4.2, the cost of the CoA has to be on the order of a few cents of U.S. dollars.

A sine-qua-non design requirement is the "three-dimensionality" of the CoAs. This requirement is translated to a required thickness of at least 0.75 mm, in order to prevent the possibility of the use of inexpensive two-dimensional (2D) scanning technologies. This three-dimensionality requirement and the random three-dimensional (3D) topology of the mixture of the conductive and dielectric material give rise to the immense uncertainty of the near-field electromagnetic response of the NF-CoAs. The second important design requirement is rigidness. This requirements implies that, although an instance can be curved as discussed in Section 4.1.3, the certificate instance should not be flexible and, thus, should not be forced out of initial shape.

Although there are numerous ways of creating these certificate instances, the first-of-their-kind objects that have been tested and successfully used as NF-CoAs can be divided into two main categories: those that are inkjet-printed and those that are copper-based.

4.1.1 Inkjet-printed Paper-based CoAs

For the realization of the first generation of certificate objects, a silver nano-particle inkjet-printing technique [57, 58] on organic substrates was chosen as a direct-write technique. According to this technique, the design pattern is transferred directly onto regular off-the-shelf photo paper by means of multiple conductive inkjet-printed layers, eliminating many of the more expensive and multistep fabrication processes currently utilized by cleanroom-based photolithography methods for depositing multiple materials on a substrate. This

technique results in a very fast, low-cost, and in-house process that helps investigate the establishment of simple inkjet-printed conductive structures as CoAs and assess the robustness achieved when deploying the 2D-to-3D transition by simply stacking 2D paper-based CoAs.

The design of an inkjet-printed paper-based single layer (2D) of a CoA [59] is shown in Figure 3. The conductive inkjet-printed nano-particle material of the, single or eventually multiple-stacked, 2D CoAs occupies the whole area of $L_2 \times W_2 = 31.65$ mm $\times 31.6$ mm of the five by five antenna array of the NF-CoA reader (see Section 5.2.1). The dimensions of the whole surface of the CoA that also includes the through holes for fastening onto the NF-CoA reader are $L_1 \times W_1 = 55$ mm $\times 53.5$ mm. The number of silver nano-particle inkjet-printed layers on the photo paper substrate is seven. The curing time for optimal sintering of the conductive material is seven hours at $120°C$. The dielectric constant ϵ_r of the photo paper is approximately 3.2 [58] in the neighborhood of 5.5 GHz.

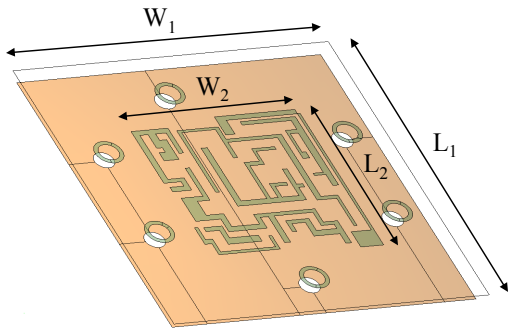
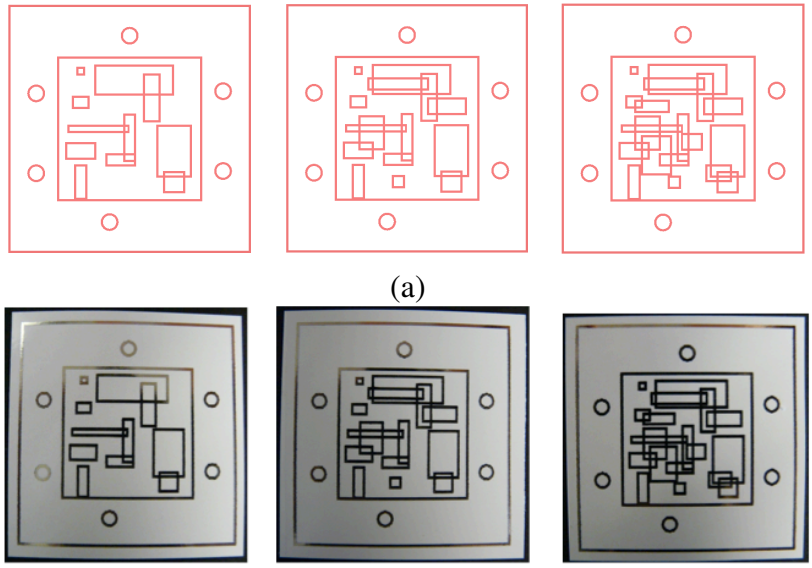


Figure 3: Design of a single paper-based layer (2D) of an inkjet-printed CoA.

Under this category of inkjet-printed paper-based CoAs, three distinct types of geometries for the NF-CoA design have been designed and fabricated. The resonance and interference of the individual scatterers was the design factor that was given the most attention. An example of such an inkjet-printed NF-CoA instance with a single substrate layer that consists of overlapping rhombic loop conductors is shown in Figure 4. Each loop is assigned a random aspect ratio and different overall circumference, so that the average loop circumference is 18.6 mm (approximately between a half and a quarter of wavelength in electrical length given that λ ranges from 59.96 mm to 49.97 mm in the 5 GHz to 6 GHz frequency range as shown in Table 2). Other factors considered included the dimensions of the spaces between conductors as a fraction of the wavelength of the reader and how the non-periodicity of the scatterers of the NF-CoAs affects the NF response for varying densities. As shown in the examples of Figure 4, the inclusion and disruption of periodicity was achieved by randomizing the position of the loops and varying the number of loops (1, 6, 11, 15, 19, 24, and 29). Similarly, the second type of inkjet-printed NF-CoAs consists of folded lines of different length and thickness (0.1 mm, 0.2 mm, 0.25 mm, 0.5 mm, and 0.75 mm); three such examples are shown in Figure 5. The folded shape was chosen for dimensional miniaturization and density maximization purposes. Finally, random constellations of 1 mm by 1 mm pixels that trace the form of the final geometry were also printed.

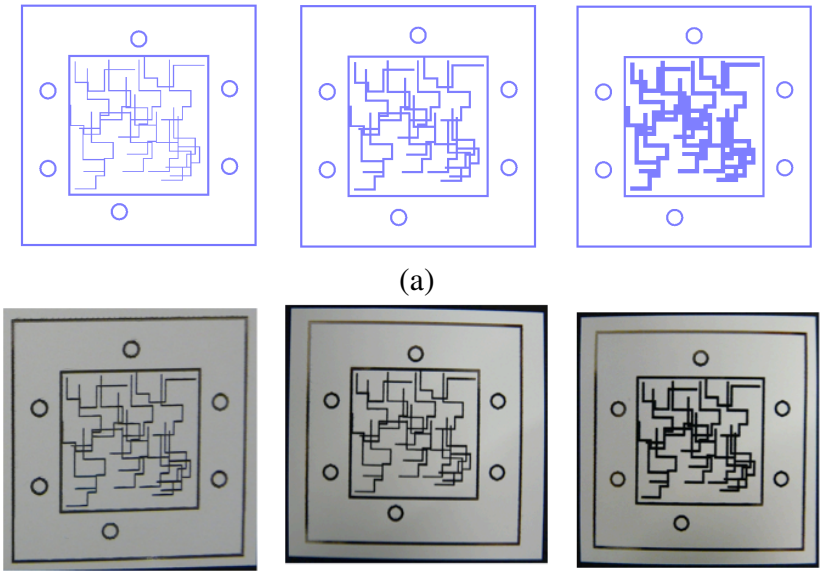
As mentioned previously, the final 3D structure of a physical identifier can be created by tightly stacking multiple 2D CoAs one on top of the other, as shown in Figure 6.



(a)

(b)

Figure 4: (a) Design and (b) fabrication of 2D NF-CoAs consisting of conductive rhombic loops inkjet-printed on a single photo paper substrate layer with varying metal density in terms of number of loops (11, 15, and 19).



(a)

(b)

Figure 5: (a) Design and (b) fabrication of 2D NF-CoAs consisting of conductive lines inkjet-printed on a single photo paper substrate layer with varying metal density in terms of line thickness (0.25 mm, 0.5 mm, and 0.75 mm).

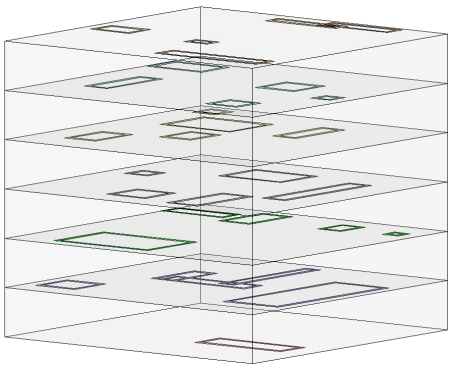
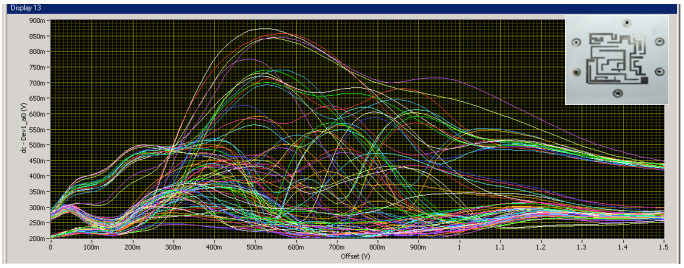
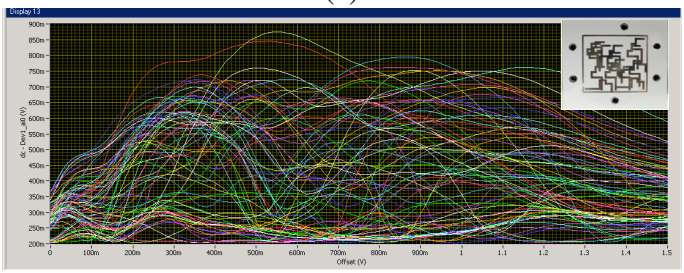


Figure 6: Separate 2D photo-paper-based layers with inkjet-printed rhombic loops that, when stacked, form a 3D NF-CoA instance.

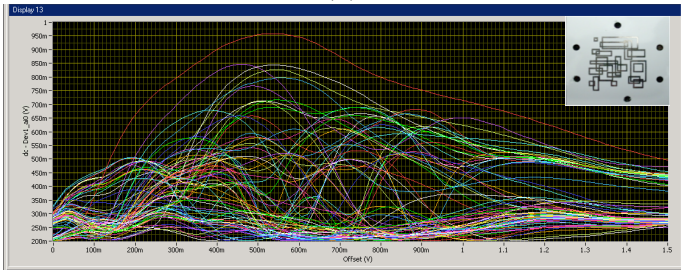
A preliminary graphical evaluation of the NF signature entropy yielded by only a single layer of this category of inkjet-printed CoAs is demonstrated with the highly-varying signatures yielded that are shown in Figure 7. For a thorough performance evaluation and entropy estimation of the complete NF-CoA system see Chapters 6 and 7.



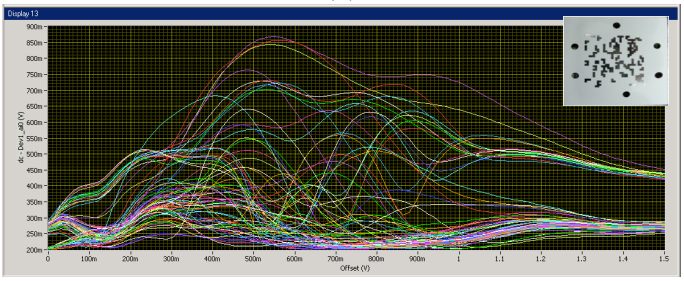
(a)



(b)



(c)



(d)

Figure 7: A preliminary graphical evaluation of the NF signature entropy achieved by four separate single-layered inkjet-printed CoAs shows highly-varying signatures yielded.

4.1.2 Copper-based CoAs

The copper-based NF-CoA instances are constructed by immersing randomly entangled and squished metallic hair into a dielectric substrate. The mixture of arbitrary 3D shape is then molded into a fixed dielectric material with a single constraint; the thinnest dimension of an NF-CoA should be substantial, e.g., at least 0.75 mm [60]. This constraint is imposed to prevent from counterfeiting NF-CoA instances via printing them using inexpensive 2D replication technologies, that is, it ensures that the adversary needs to master manufacturing of NF-CoA-like objects in three dimensions. The key outcome obtained is that these physical NF-CoA objects consist of an extremely difficult to replicate, random arrangement of scatterers that produces a unique and repeatable response in the near field.

Examples of these copper-based CoAs are shown in Figures 8 and 9. These particular instances have been fabricated in collaboration with an injection-molding company [61]. Essentially, the process involves the encapsulation of thin "hair" of copper wire of variable mass in grams per meter (2 g/m, 3 g/m, and 4 g/m) into a heated plastic mold that is hardened to maintain the position of the wires. This process helps the CoA instances withstand humidity and temperature. Randomness in the shape of the submerged metallic hair is introduced by applying techniques that are absolutely non-deterministic, including the use of large air fans and blending with different speeds and for different amounts of time.

Contrary to the inkjet-printed CoAs, the copper-based NF-CoAs are designed to occupy a smaller area (approximately 27 mm $\times$ 27 mm) with the aim to increase their practicality and ease of attachment to physical objects. These are shown in Figure 9. Any potential effect of the size reduction on the entropy of the signatures yielded is examined in Section 6.2.3. The lateral surface of these smaller-sized square-shaped CoAs is rotated around the central axis of the antenna array of the NF-CoA reader (see Figure 10), so that the radiation of as many antenna elements as possible that are closer to the periphery of the array is "disturbed" by the NF-CoA. Certificates *I* (of Figure 8) and *J*, however, comprise the exceptions, since their cross-section areas intentionally exceeded those of the antenna

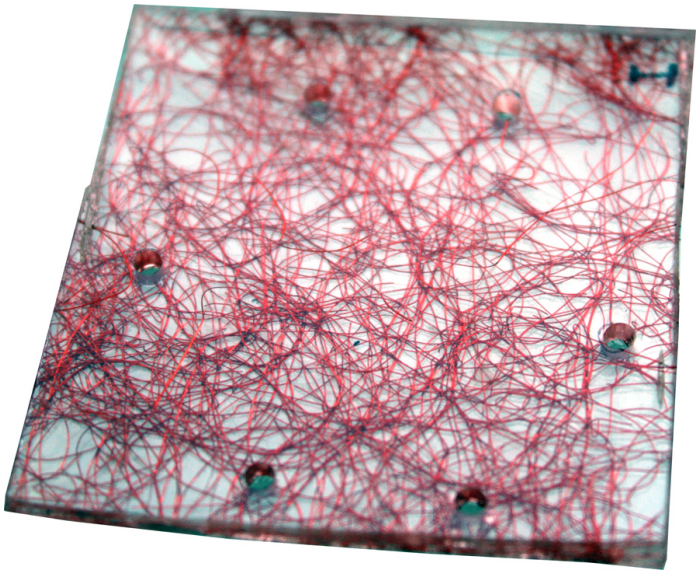
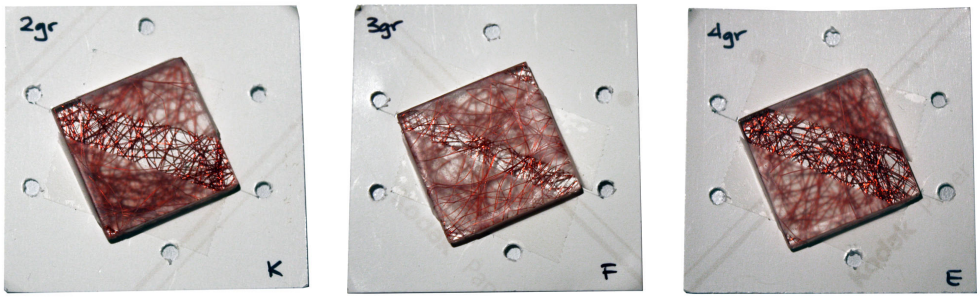


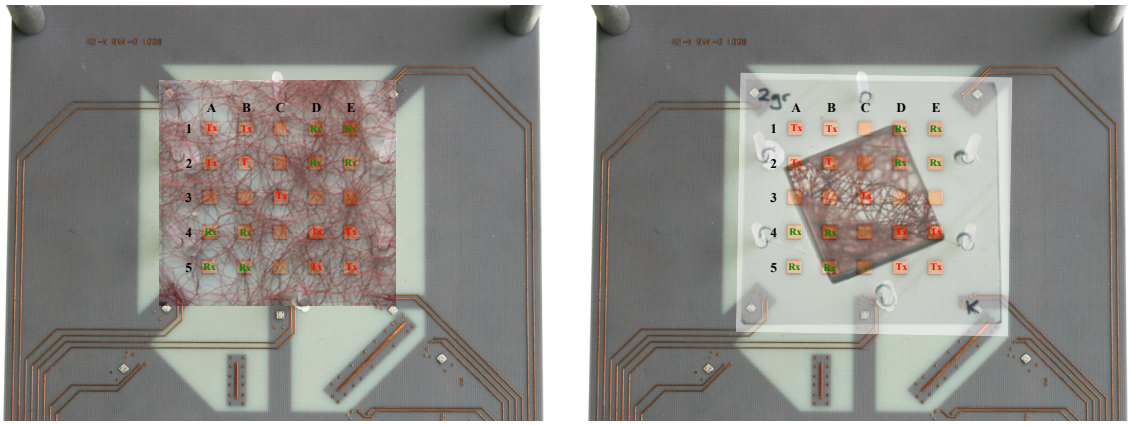
Figure 8: The inner semi-transparent three-dimensional structure of a 56 mm × 56 mm "full-sized" copper-based NF-CoA instance.



(a) (b) (c)

Figure 9: Copper-based 27 mm × 27 mm NF-CoAs of different mass per meter (2 g/m, 3 g/m, and 4 g/m).

array for testing purposes. In particular, the dimensions of these two certificates are approximately 56 mm × 56 mm and holes for the plastic poles of the reader had to be drilled through them (see Figure 8).



(a) (b)

Figure 10: Top view of the NF-CoA reader with (a) a small-sized and (b) a full-sized copper-based certificate instance fastened to the annotated antenna array slot.

After an NF-CoA has been fabricated, regardless of if it is a copper-based or an inkjet-printed one, its NF response has to be captured, digitized and stored. If the capability of offline verification is desired, one of the tools that can be used is traditional asymmetric key cryptography. The digitized NF-CoA signature is digitally signed by the original issuer. This issuing process takes place in the controlled environment of a fabrication facility and is discussed in detail in Section 4.2.1.

4.1.3 CoA Instances on Flat and Cylindrical Surfaces

The design of the NF-CoA instances does not constrain them to necessarily be part of only flat surfaces. As long as curved arrays of antennas are developed, the CoAs can also be mounted on rigid curved surfaces.

To better illustrate this, concept photos are provided in Figure 11.

(a) (b)

Figure 11: Concept photos of copper-based CoAs attached on rigid cylindrical surfaces.

4.2 NF-CoA Instance Life Cycle

In an effort to provide all aspects of the proposed complete authentication and anti-counterfeiting solution, this section presents the entire life cycle of an NF-CoA instance spanning from the fabrication process to the point where a citizen has his identity card or passport authenticated or a client checks out a product. Examples of the fabrication processes followed to realize the first two generations of prototype CoAs have been provided in the previous section. Regardless, however, of the exact fabrication process used, the two succeeding stages that a certificate goes are the issuing and the verification processes if offline authentication is desired.

The verification of a certificate instance in the framework of the NF-CoA system can happen either in an *online* or an *offline* fashion. Essentially, the difference between these two types of verification is that the online one is conducted by contacting and accessing a remote Internet-based central database that keeps a record of all the queries in the past and is able to tell if one particular serial number has been queried about its authenticity more than once in the past. On the contrary, the offline process makes use of no intranet, i.e., corporate, or Internet connection whatsoever and is entirely carried out locally and almost instantly by the standalone reader itself. Although one can naively argue that the physical CoA is not required in the online verification process, this argument is, of course, not true. Relying on just monitoring if one bit sequence, e.g. a serial number, has been queried more than once (N times) in the past would only allow the original issuer to know there exist $N - 1$ counterfeits; in fact, the issuer would not be able to track down which exact is the genuine, and who $N - 1$ counterfeiters to legally pursue.

In this chapter, the focus is given on the more attractive offline scenario, as this is applicable to a significantly broader range of applications. The traditional asymmetric key cryptography shown below is only one of the large array of possible cryptosystem candidates.

4.2.1 NF-CoA Issuing Process

The first main process, which takes place in the controlled environment of a fabrication facility right after the fabrication is complete, is the NF-CoA issuing process [62, 48]. This process consists of a number of steps that are listed below and shown in Figure 12. The certificate issuer follows these steps to digitally sign the NF fingerprint of the instance using traditional and long-trusted cryptography.

① First, the NF-CoA reader is used to digitize the unique NF fingerprint of the newly fabricated NF-CoA instance. This digitized bit sequence, which consists of 12-bit accuracy readings at f_{MAX} frequency steps in the spectrum neighborhood of 5.5 GHz for all N_{coupl} antenna permutations has, initially, an overall raw size of $(12 \times 65 \times 72)/8 = 7020$ bytes. This bit sequence may be compressed, using any of the numerous available lossless compressing algorithms, into a reduced and fixed-length bit string (f). In case, for example, the UHF EPC Class 1 Gen 2 RFID standard [63] is used, this protocol can handle multiple fragmented packets and, additionally, the RFID chip manufacturers do provide 4 Kbytes or more of non-volatile high capacity memories in their chips.

② The information (*data*) associated with the owner of the protected document, such as personal details and bio-metric data, or the product itself, including product ID, color, and expiration date, is afterward appended to the bit string f.

③ A copy of the resulting composite bit string *payload* is directly stored to onto the accompanying tiny embedded storage chip or an RFID tag chip, as shown in the diagram of Figure 12.

④ A copy of bit string *payload* is hashed using a cryptographically strong algorithm, with SHA256 [64] being a very good such candidate.

⑤ This hash is subsequently signed (s) by applying a *public-key cryptosystem* (*PKCS*),

such as RSA [54], digital signature algorithm (DSA) proposed by the National Institute of Standards and Technology (NIST) [65] or other cryptographic routines based on elliptic curves, such as EC-DSA [66], and using the issuer's private key. The use of asymmetric key algorithms that involve the use of a public key known to everyone, and a secret private key is the distinguishing characteristic of public key cryptography. The keys are related mathematically, but it is virtually impossible to deduce the private key from the public key [54]. As a consequence, in the NF-CoA application only the issuer can digitally sign the NF-CoA with the secret private key.

⑥ As was the case with the plain initial bit string w, the hashed and signed version s is also directly encoded onto the same embedded storage chip or RFID chip.

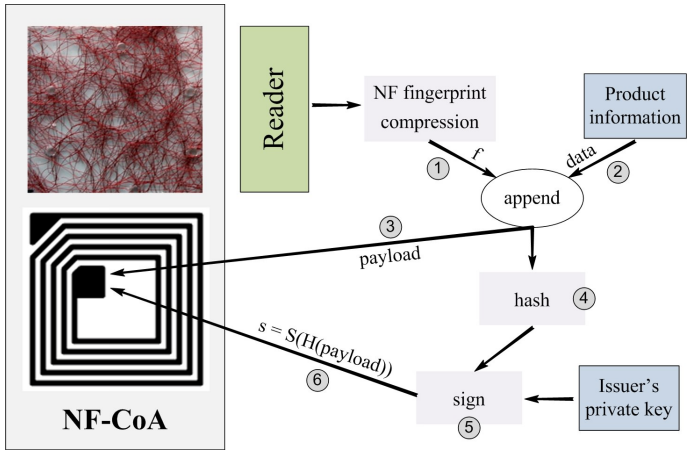


Figure 12: The NF-CoA issuing process

4.2.2 NF-CoA Verification Process

The NF-CoA verification process [62, 48] is almost the inverse process of the certificate-issuing process, discussed previously, and it is conceptually shown in Figure 13. Here the similarity level between the signed and stored signature is checked. This process can take place, for example, at passport checkpoints and customs offices, during the check-out process of a product or drug with a cashier or during the arrival of merchandise at a distribution center or a warehouse.

The digitally-encoded information mentioned in the previous subsection, which essentially results from the concatenation of a plain and a signed version of the identity or product information and the NF signature of the CoA, i.e., $s||w$, is used to validate whether or not a document is valid or a product is authentic or not. The steps of the verification process are

① A regular wired or wireless storage chip reader or RFID reader is used to extract the bit string *payload*, which contains *data* and its signed and hashed version s.

② The integrity of the plain bit string *payload* is verified with respect to its encrypted and signed version (s) using the corresponding well-known issuer's public key. If the integrity test is successful, then the verifier can be confident that no one else, except for the possessor of the matching private key, has encrypted the information and, as a result, the original compressed NF fingerprint f, and the object *data* are extracted.

③ The extracted fingerprint f is afterward compared with a new read-out of the NF-CoA that the verifier extracts himself with his own NF-CoA reader. The comparison/matching is done based on the same distance metric at each antenna coupling (out of N_{coupl}) and frequency point individually (out of f_{MAX}). Only if the values of the distance between these two, read and extracted, fingerprint curves is smaller than a threshold value all across the frequency range, i.e., the similarity exceeds a certain level, does the verifier declare that the certificate and, thus, the product is authentic. For more details about the determination of this threshold δ_T see Sections 6.2.5.1 and 7.1.

As shown in the entropy quantification analysis of Chapter 7, this level of similarity corresponds to a worst-case maximum probability for a false alarm of 10^{-200}, which is virtually impossible.

One last note that relates to the ease of use and portability of the NF-CoA reader within store premises or industrial facilities is that the microcontroller unit chip of the last two generations of the reader can provide wireless connectivity and relay of the extracted CoA data

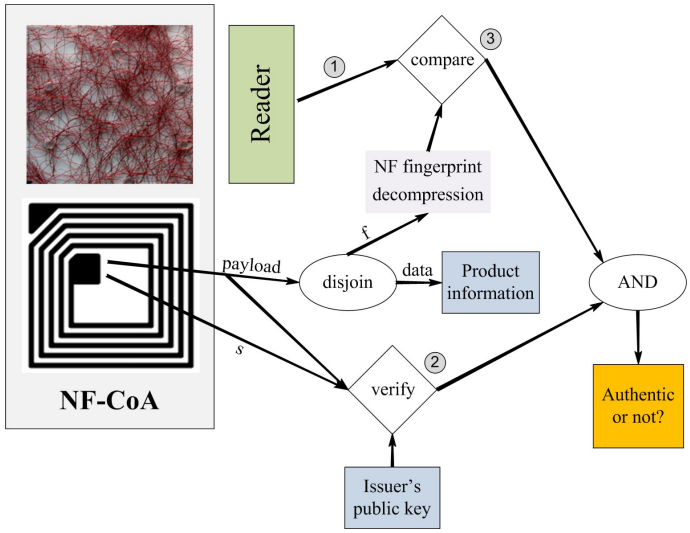


Figure 13: The NF-CoA verification process

on top of the standardized and highly-reliable Zigbee Pro and Bluetooth wireless networking standards to a central location and a mobile device, respectively, over *AES* (*Advanced Encryption Standard*)-128 bit encrypted wireless links. Further details about how the proposed NF-CoA reader architecture enables wireless networking are provided in Section 5.3.4.

CHAPTER 5

NF-COA READER DESIGN AND DEVELOPMENT

The NF-CoA reader is an important component of the NF-CoA system. The reader is used to reveal the fine near-field electromagnetic effects resulting from the impingement of electromagnetic energy on a certificate instance and, thus, derive the fingerprint of a certificate instance. In particular, during the contactless validation procedure, carried out by the reader, an attempt is made to associate the near-field signature response, extracted with the help of $K \times K$ matrix of antennae that latches onto an NF-CoA instance, with the digitized signature that is signed by the issuer and stored into a complementary tiny embedded storage chip.

The extraction of the unique signature of an NF-CoA object is performed as follows: electromagnetic power in the neighborhood of 5.5 GHz is emitted from a particular element of the antenna array of the reader, this radiation impinges upon an NF-CoA instance placed at a distance of 2 mm up to approximately 6 mm away from the array, as long as this distance is kept the same across different CoAs and different reader measurements and allowing for ±0.3 mm vertical displacement, and eventually the near-field effects, discussed in Chapter 3, are captured by another antenna element.

As in the case of the certificate instances and for a wide adoption to be possible, the reader is required to meet the requirement of low cost (with the sum of its analog and digital components being on the order of less than 75 U.S. dollars). Meanwhile, it is also required that the reader can operate autonomously and in an offline (no Internet connectivity) fashion, exhibits enormous performance robustness, in terms of accuracy, consistency and speed of capturing of the signatures, and has dimensions comparable to that of a human palm.

Despite the low accuracy provided by the out-of-the-shelf analog and digital circuitry used and the noise due to external factors, the major objectives of the reader design are to

→ maximize the entropy, i.e., randomness, of the near-field response of the CoA

→ guarantee the extraction robustness of the NF signature of the same CoA by different readers. In other words, the reader has to exhibit consistency of the extracted NF fingerprint across multiple readings of the same NF-CoA , as well as across readings of the same NF-CoA tag by different readers despite the low accuracy provided by the out-of-the-shelf analog and digital circuitry used and the noise because of external factors.

The hardware aspects of the fabricated reader, including its design and fabrication, as well as its operating details are presented in this chapter.

5.1 The NF-CoA Reader Generations

The design and fabrication of the NF-CoA reader has evolved over three different generations of mixed-signal boards. All board generations consist of four metallic and three substrate layers of variable thickness, as depicted in Figure 14. Of the two inner conductive layers, *M2* houses all DC lines that power the active components of the reader and *M3* serves as the ground plane. As opposed to the case of the first-generation NF-CoA reader (see Section 5.1.1), the ground layer of the second and third generations (see Sections 5.1.2 and 5.1.3) is not contiguous. Instead, on layer *M3* reside two separate and unconnected ground planes; one for the upper half of the board that houses the antenna array and one for the lower half of the digital control plane of the board. The antenna array resides on layers *M1* and *M2*.

The thickness of the dielectric layers is $T_{D1} = T_{D3} = 0.254$ mm $= 0.010$ inch and $T_{D2} = 0.889$ mm $= 0.035$ inch and the thickness of the conductor layers is $T_{M1} = T_{M4} = 0.046$ mm $= 0.0018$ inch and $T_{M2} = T_{M3} = 0.018$ mm $= 0.0007$ inch. As a result, the total thickness of the board does not exceed 1.6 mm. The substrate of the board is *FR-408* with relative dielectric constant $\epsilon_r = 3.715$ in the near-field *super high frequency* (*SHF*) band of interest, namely 5 GHz to 6 GHz, relative permeability $\mu_r = 1$ and loss tangent $tan\delta = 0.01$.

The copper conductivity is 5.88×10^7 S/m (or 1.493×10^6 S/inch).

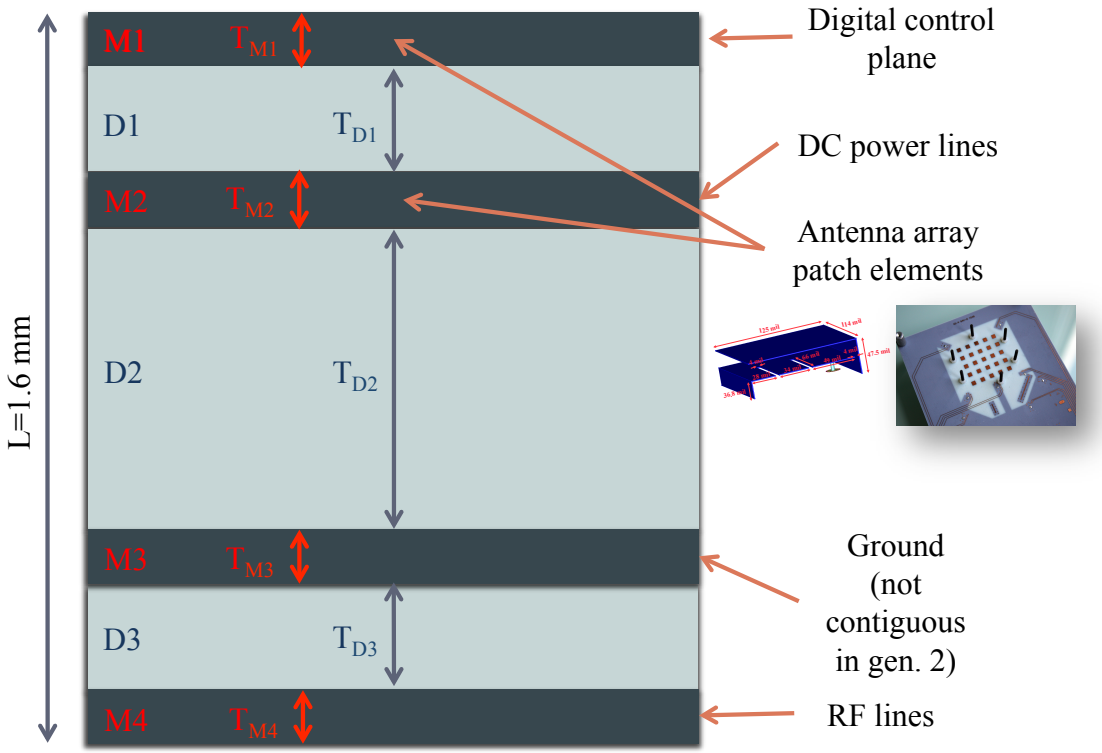


Figure 14: The four metallic (M*X*) and three substrate (D*X*) layers of the NF-CoA reader board.

5.1.1 First-generation NF-CoA Reader

During the design of the first generation of the NF-CoA board reader [59], the attention was almost exclusively concentrated on the SHF plane. A significant effort was made to optimally place the SHF components in order to maintain the signal integrity of the NF fingerprint.

The circuit design of the first generation NF-CoA reader is shown in Figure 15. Figure 16 shows the board schematic design. In both figures, the major analog and digital components are annotated. The circuit part that is colored with pink lines in the diagram of Figure 16 corresponds to the digital part. The SHF circuit part is shown with turquoise lines. The dimensions of the board are 12.85 cm $\times$ 16.50 cm.

The SMA female connectors attached on each side of the fabricated first generation board, as shown in Figure 17, only serve for characterization and verification purposes. Of course, special provisioning was required in terms of both additional SHF lines and low-capacitor structures to assist in re-routing of the SHF signal path for testing. The characterization results are provided in the next section. Under this approach, the SMA connectors should be considered removed during normal operation of the board.

For this first prototype implementation, an external data acquisition board [67] is used to generate the 16-bit sequence that dictates the path of the SHF signal through the two-layer SP4T switch hierarchy, controls the frequency output of the *voltage-controlled oscillator* (*VCO*) through the corresponding input voltage and measures the power detected by monitoring the output voltage of the *power detector* (*PD*). This data acquisition board is connected to the set of pins shown in the lower half of Figure 17b.

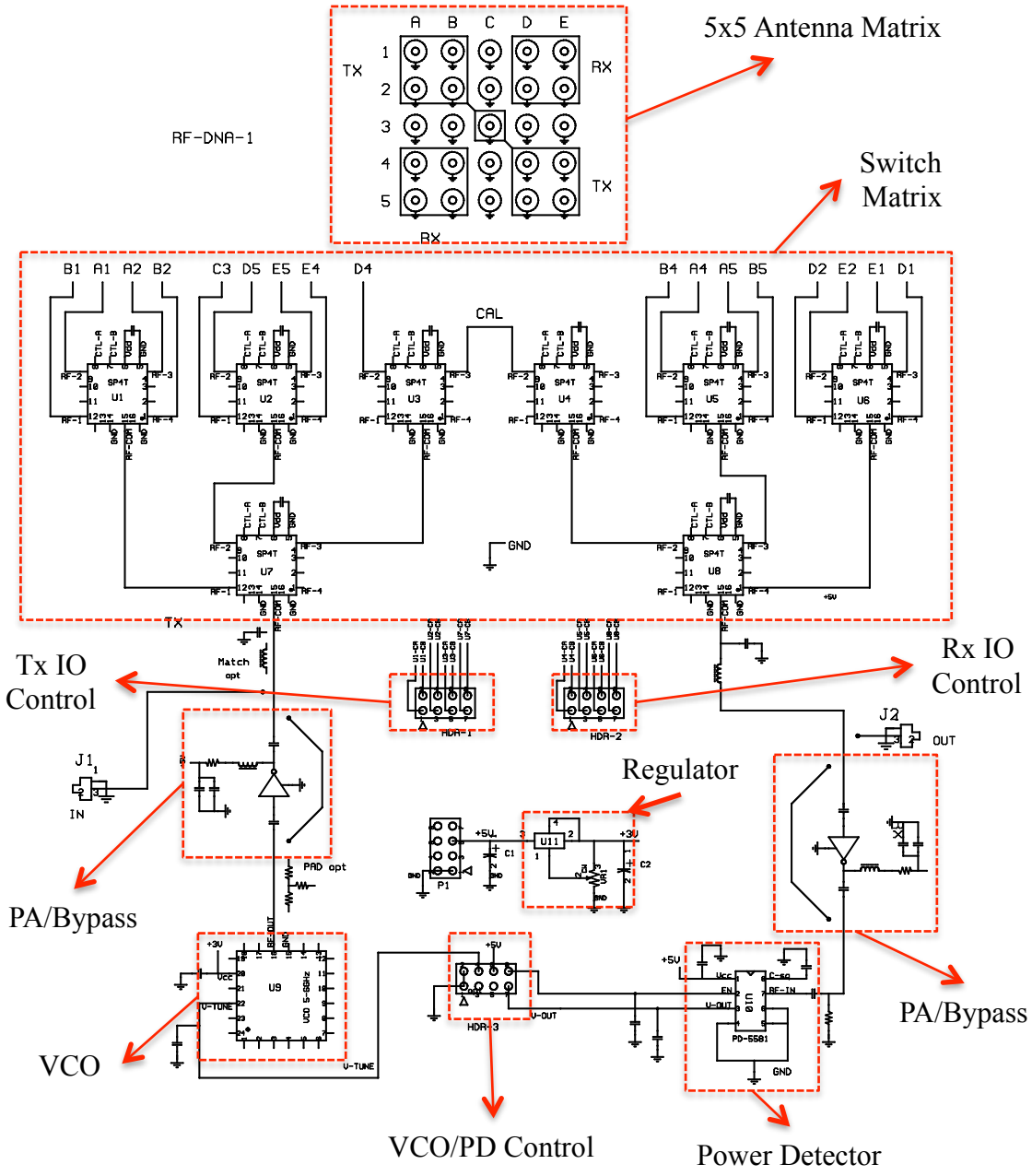


Figure 15: The circuit design of the first-generation NF-CoA reader.

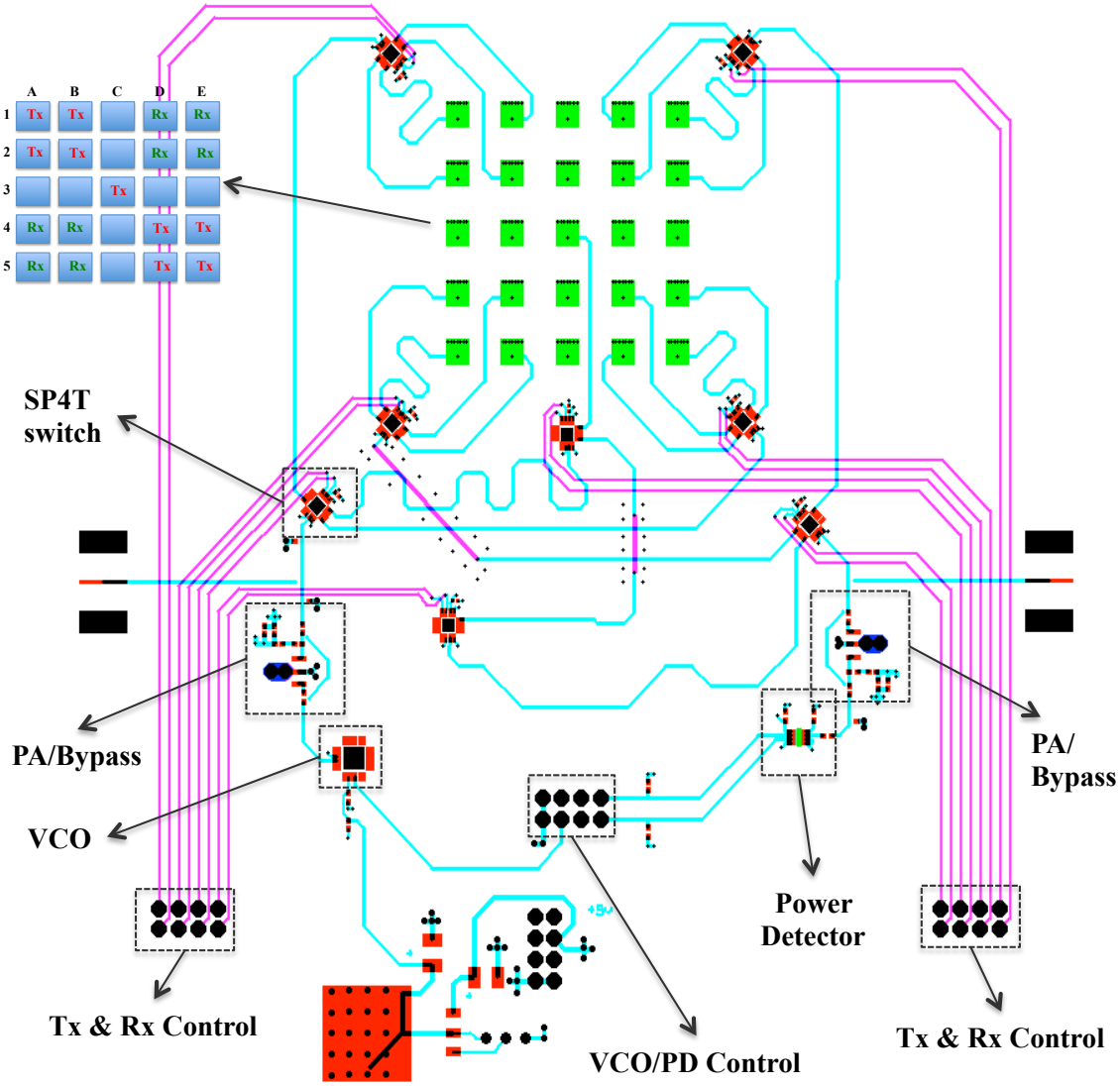
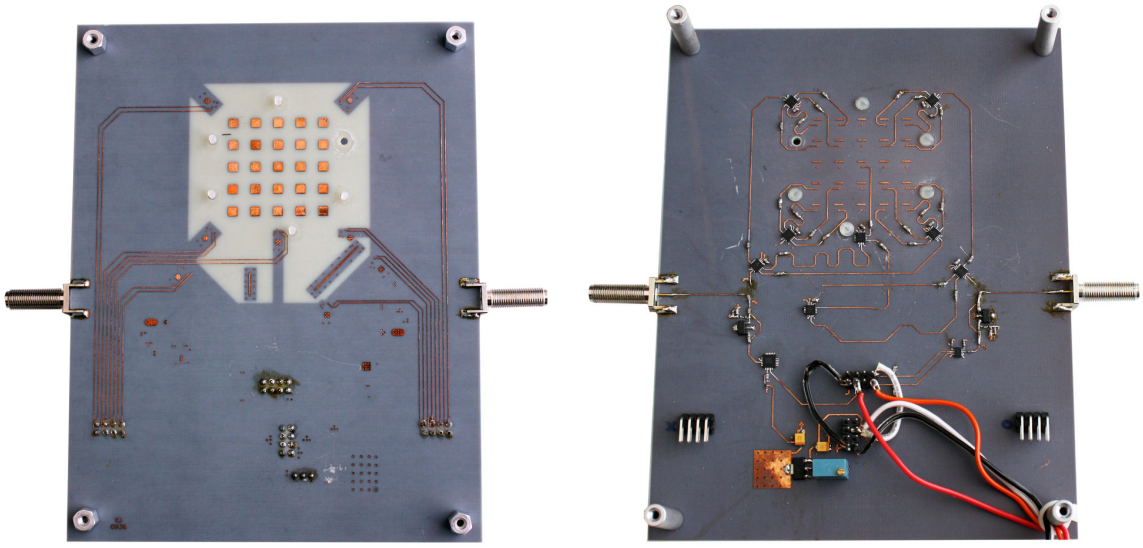


Figure 16: The board schematic design of the first-generation NF-CoA reader.



(a) (b)

Figure 17: The (a) top and (b) bottom view of the 12.85 cm × 16.50 cm fabricated first-generation NF-CoA reader.

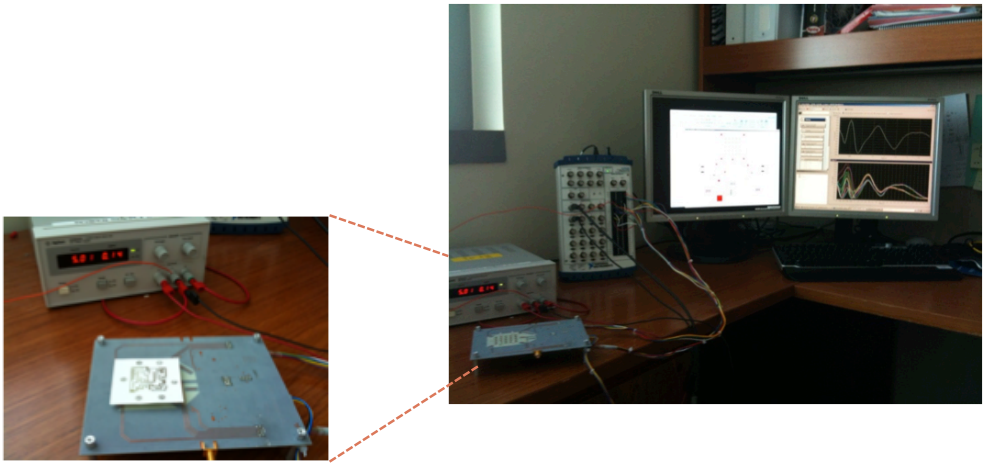


Figure 18: The original test setup of the first-generation NF-CoA system. The reader control and NF-CoA signature extraction is performed by the National Instruments data acquisition board.

5.1.2 Second-generation NF-CoA Reader

The board schematic design of the second-generation NF-CoA reader [60, 53] is shown in Figure 19. The major analog and digital components of the reader are annotated in the same figure.

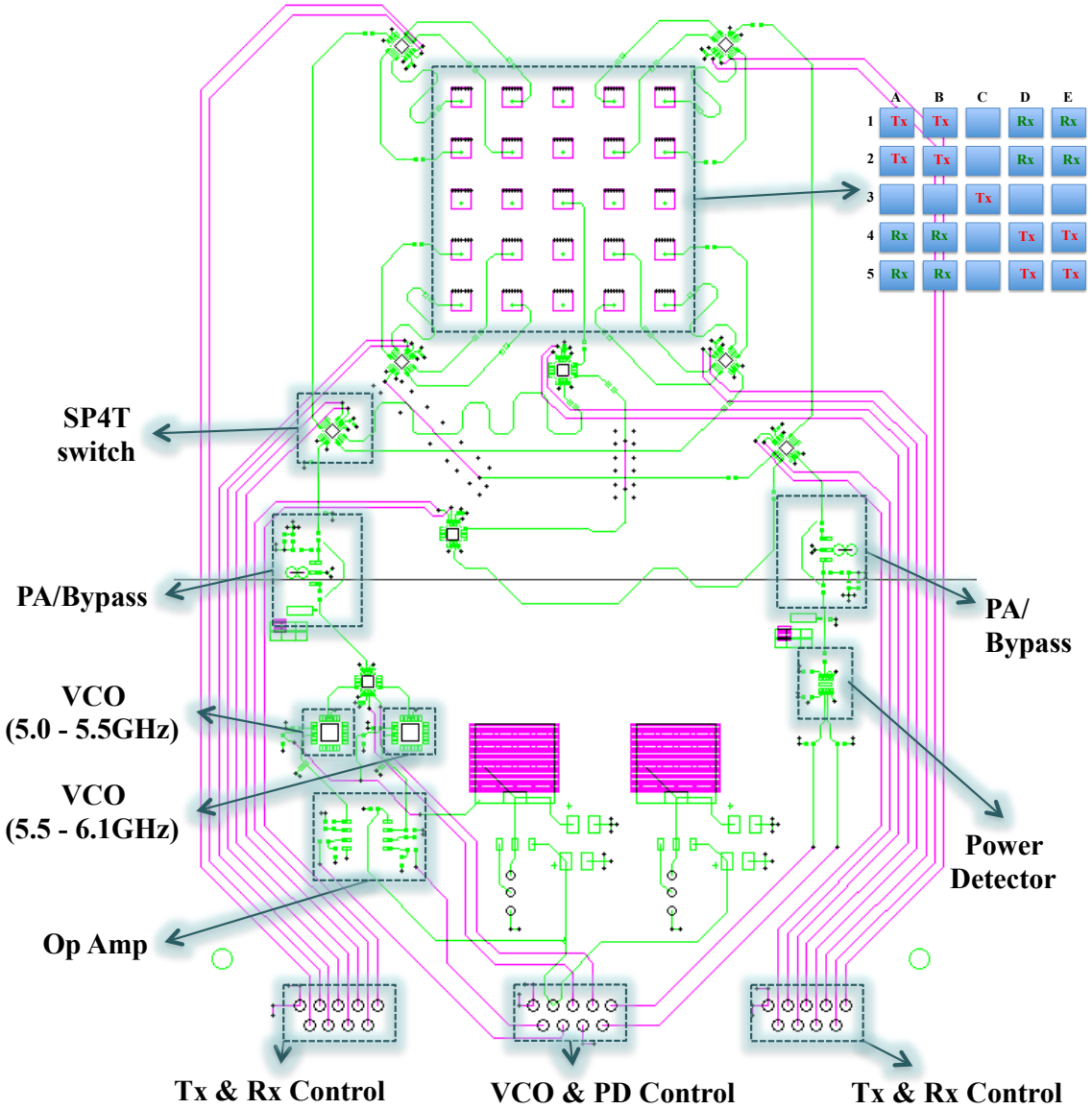
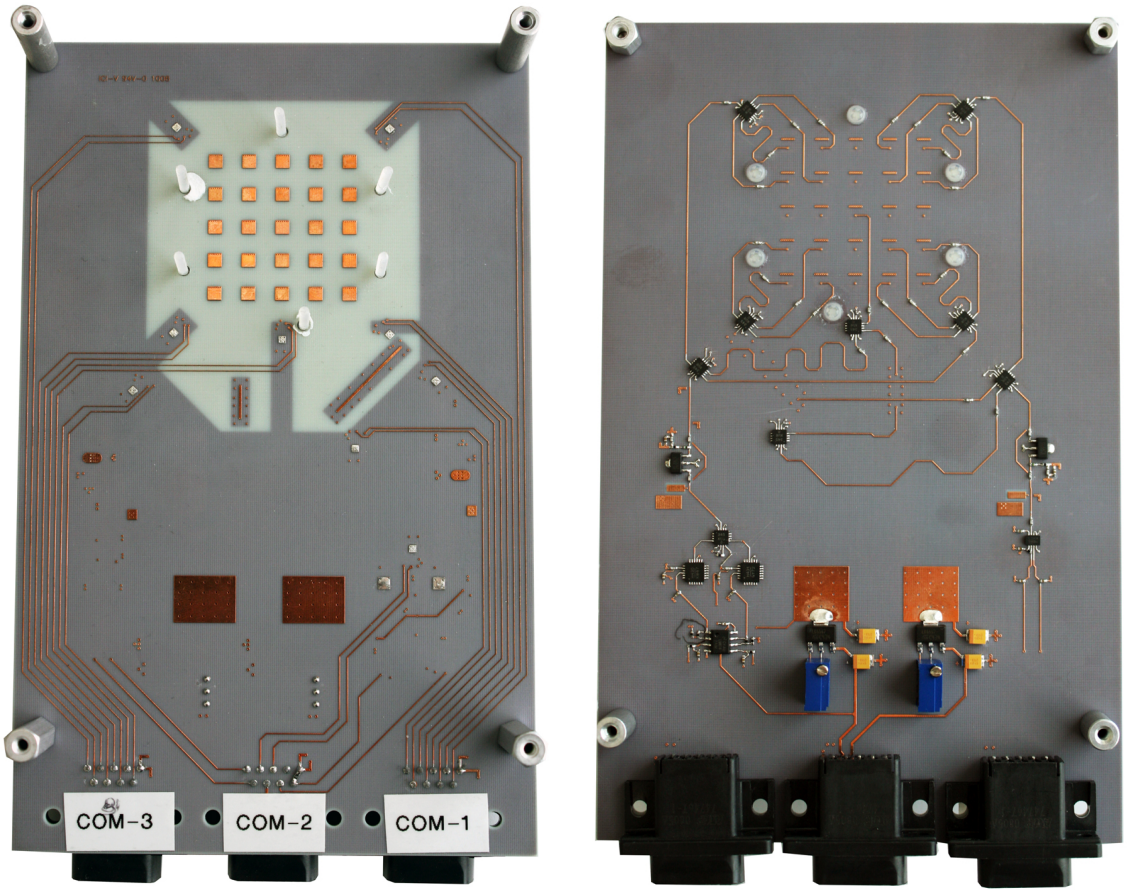


Figure 19: The board schematic design of the second-generation NF-CoA reader.

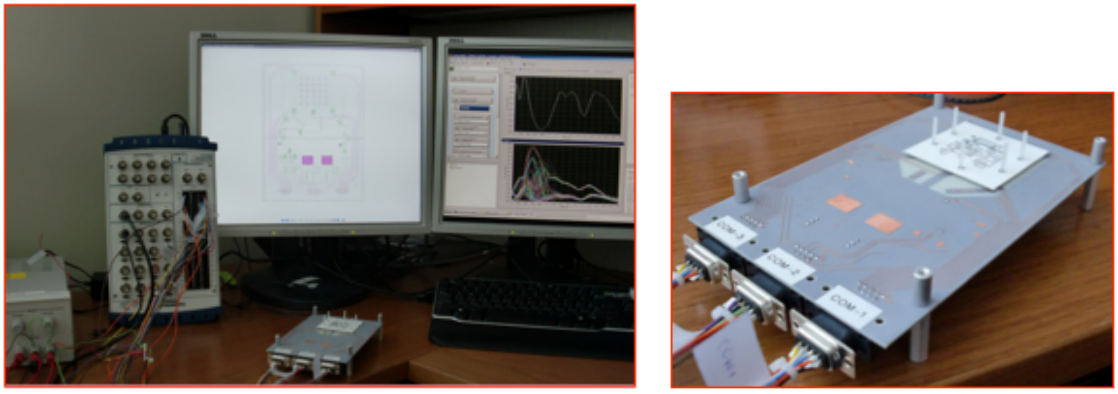
The most important advancement in regards with the first-generation board is that this design does not rely on a single VCO but two of them, namely the HMC430LP4 [68] and

HMC431LP4 [69], which both together optimally cover the 5.0 GHz to 6.1 GHz frequency band. Additionally, this board is narrower, occupying 16% less space; the dimensions of the second–generation board are 10.8 cm $\times$ 17.2 cm. Moreover, the operation of this board is, for the first time, controlled by an external *micro-controller unit* (*MCU*) board [70] that provides not only a very fast means of capturing the NF fingerprint, but also the accuracy required toward an effort to maximize the fingerprint's entropy. The state diagram of the MCU, which reflects the sequence of all the steps of the NF-CoA signature validation procedure, is discussed in detail in the next section. As a result, the overall reader design consists of a double-stacked layer solution; the SHF plane and the *digital control* plane. As implied by their names, the first layer includes the CoA reading slot, the antenna matrix, as well as all required digital and analog circuitry and the second houses the MCU and the data acquisition interface. The circuit part colored with pink lines in the diagram of Figure 19, corresponds to the digital control plane. The SHF plane circuit part is shown with light green lines.



(a) (b)

Figure 20: The (a) top and (b) bottom view of the 10.8 cm × 17.2 cm fabricated second-generation NF-CoA reader.



(a) (b)

Figure 21: The original test setup of the second-generation NF-CoA system. The control of the reader operation and the NF-CoA signature extraction are here conducted by the NI DAQ board.

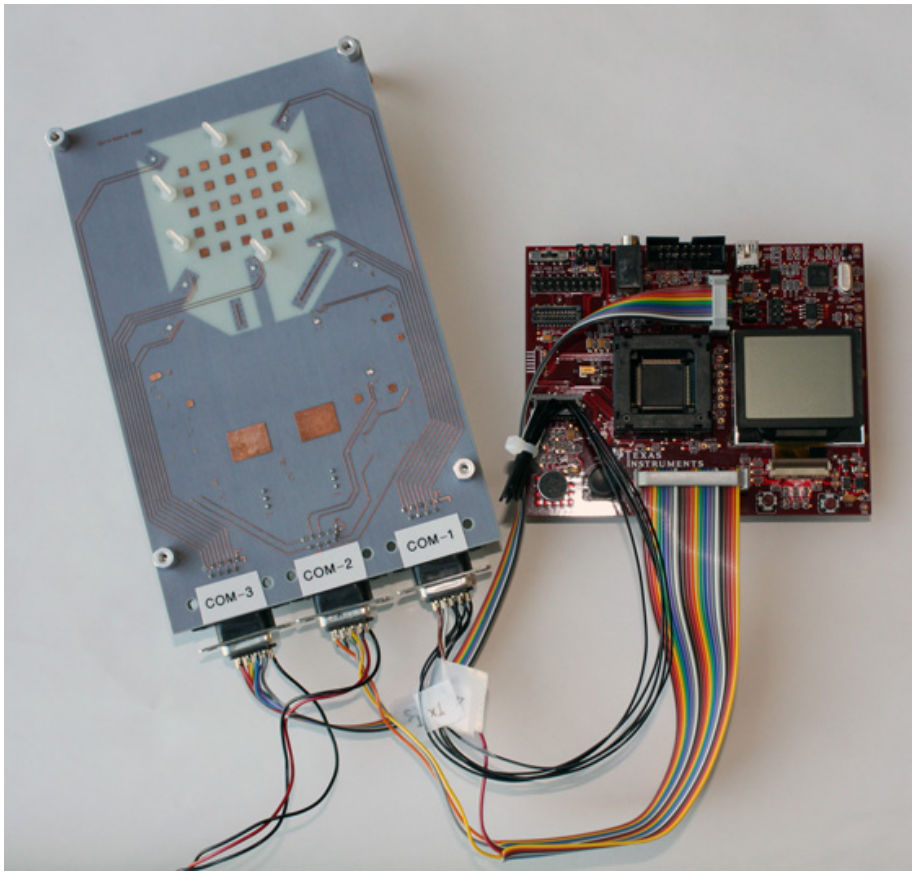


Figure 22: The final test setup of the second-generation NF-CoA system. The fabricated super high frequency plane of the reader is shown on the left and its digital control plane is shown on the right.

5.1.3 Third-generation NF-CoA Reader

The latest generation of the NF-CoA reader [48] represents the first standalone, autonomous reader that does not make use of an external data acquisition board. Instead, a big leap toward unifying the SHF plane and the digital control plane and integrating them on a single board is done. It should be noted that, for this single board solution to be realized and maintain its high efficiency, special care was taken for the optimal placement of the MCU chip, its supporting IC components and the inter-connecting wiring that involved two main goals, namely the isolation, that is, elimination of the electromagnetic interference, between digital and analog circuitry and the signal integrity preservation of the NF fingerprint. A direct result of this single-board approach has been the increase of the length of the board. The board's dimensions are 10.8 cm $\times$ 20.9 cm. The top and bottom views of one of the fabricated third generation NF-CoA readers are provided in Figure 24.

The major analog and digital components of the third-generation NF-CoA reader are annotated on the board schematic design of Figure 23. The SHF lines are on the top layer (turquoise–colored lines in the diagram of Figure 23). The ground plane is placed on the third metal layer and the digital control lines on the bottom layer (gold–colored lines in the diagram of Figure 23).

At the heart of the control plane is the TI MSP-EXP430F5438 MCU [70] that features an up to 18-MHz system clock, high-frequency crystals up to 32 MHz and multiple high-resolution *analog-to-digital converters* (*ADC*). The MCU is accompanied by push buttons and a USB interface for data transfer.

For its powering, the control plane does not rely on batteries, although a two-AA battery option is available. Instead, the current is supplied by the USB cable, which is anyways used for the NF-CoA fingerprint acquisition by a desktop or a laptop computer. When alternatively powered by an AC-to-DC converter, the nominal voltage is 9 V while the measured is 9.19 V with a significant peak-to-peak Voltage variance of 400 mV. When the board is initially connected to a computer through the USB cable it finds itself in the low

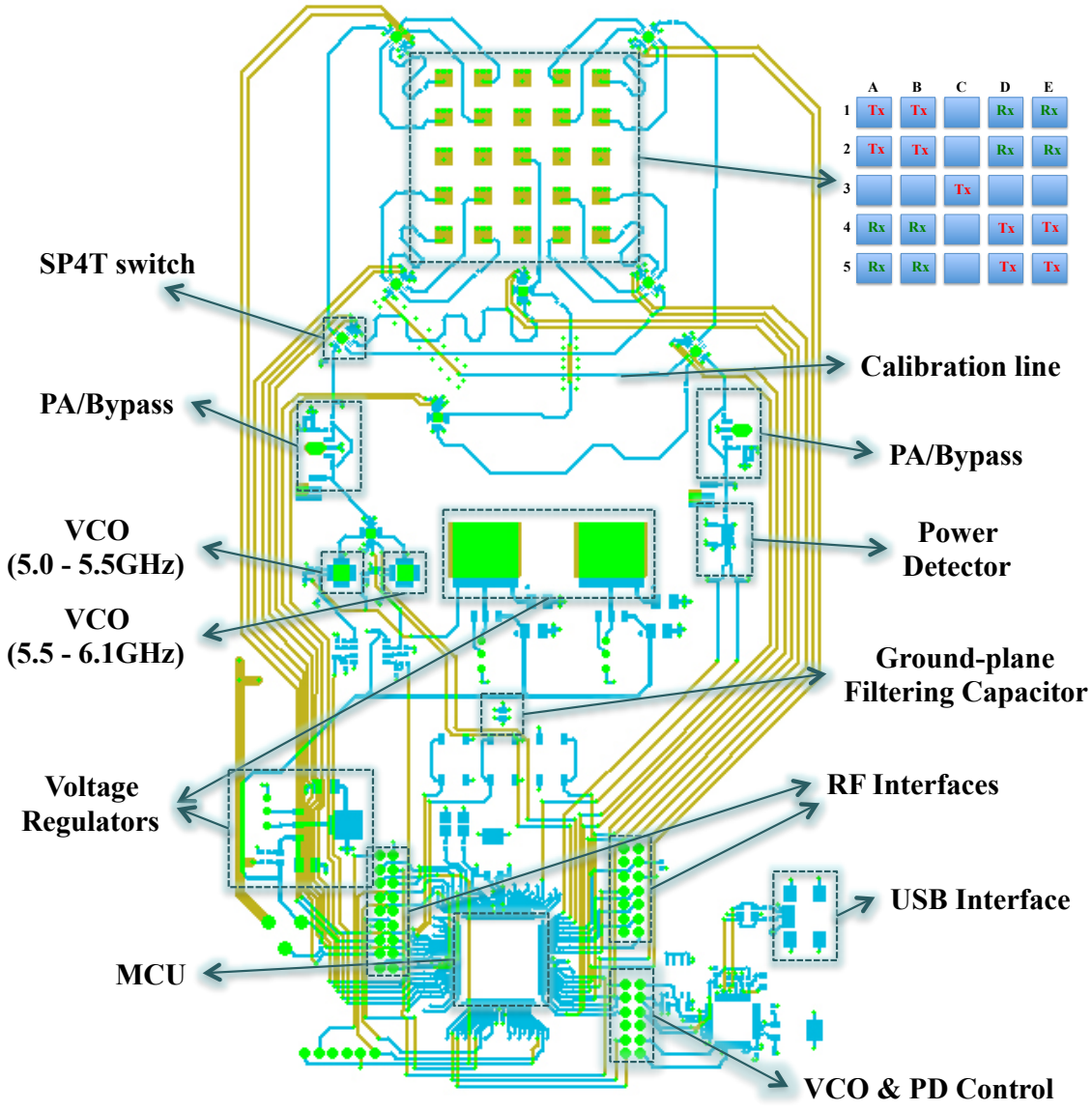
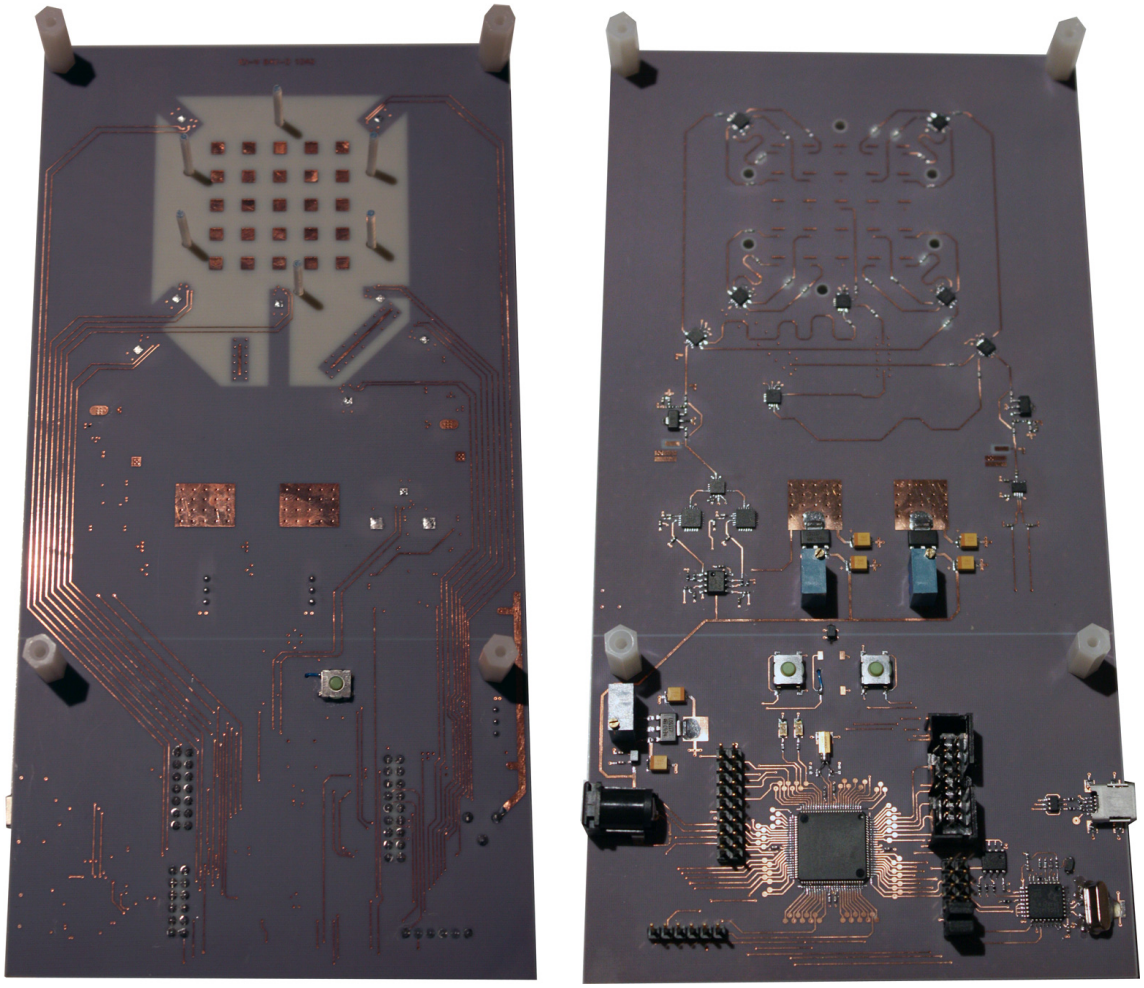


Figure 23: The board schematic design of the third-generation NF-CoA reader.

power mode 4 (LPM4) sleep mode (see next section for more details).



(a) (b)

Figure 24: The (a) top and (b) bottom view of the 10.8 cm × 20.9 cm fabricated third-generation NF-CoA reader.

5.2 Super High Frequency Plane

5.2.1 Antenna Array Elements and Coupling

The antenna elements that comprise the array are individual folded shorted-patch antennas, the 3D design of which is shown in Figure 25. The planar shape of this type of antennas makes them easy to integrate into the "skin" of the NF-CoA reader board, while a relatively high gain with good side-lobe suppression can be achieved.

A trade-off between two contradictory desired features had to be made during the antenna array design. On one hand, since it was desired that the planar dimensions of the first generation of CoAs are approximately 1 inch × 1 inch for practical reasons, such as mounting them on small sized products, and given that the certificate read-out involves the near-field response of its scatterers, the antenna array should also occupy the same area. On the other hand, it was desired that a single NF fingerprint consist of as a large set of scattering parameter (S_{21}) curves of antenna element couplings as possible. These contradictory design requirements necessitated the use of folding and meandering minimization antenna design techniques that enormously help in packing as many individual antennas as possible in the aforementioned area. The technical characteristics and the antenna design strategy has relied on previous research efforts [71, 72]. As a result of the exploitation of the minimization techniques and by choosing an operating frequency range in the neighborhood of 5.5 GHz that yields a half wavelength ($\lambda/2$) of around 2.75 cm, the final planar size of each element is 2.95 mm × 2.988 mm (or 116.142 mil × 117.638 mil corresponding to $x \times y$ of Figure 26) and it is finally possible to fit 25 (with a 5×5 configuration) within an area of 31.70 mm × 31.51 mm (corresponding to $L \times W$ of Figure 26) [59, 60]. The antenna array elements are placed on the top two metal layers of the reader board at planar horizontal and vertical distances of $\Delta_x = \Delta_y = 4.19$ mm between each other, as shown in Figure 26.

During an NF signature read-out, it is ensured that the placement of the NF-CoA instance against the antenna array is fixed and geometrically unique by aligning the CoA

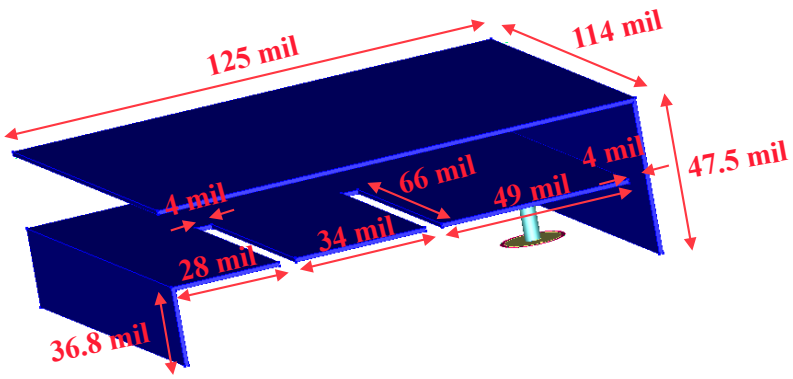


Figure 25: The design of an individual folded shorted-patch antenna.

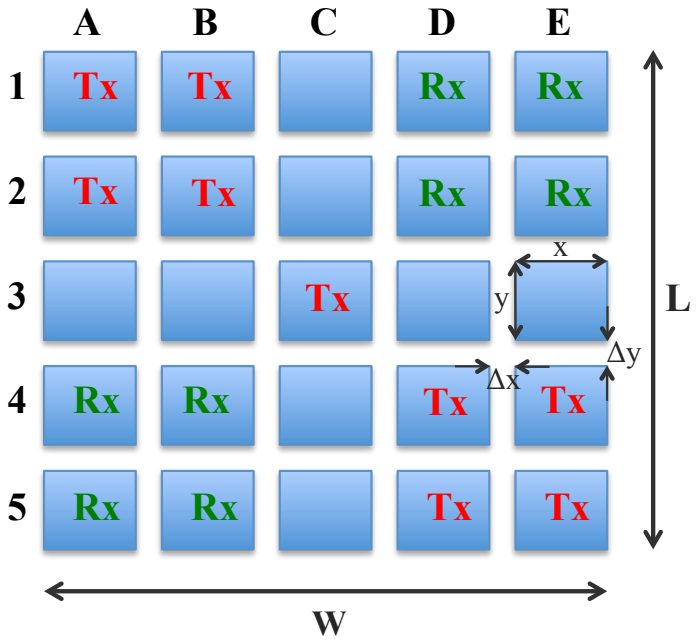
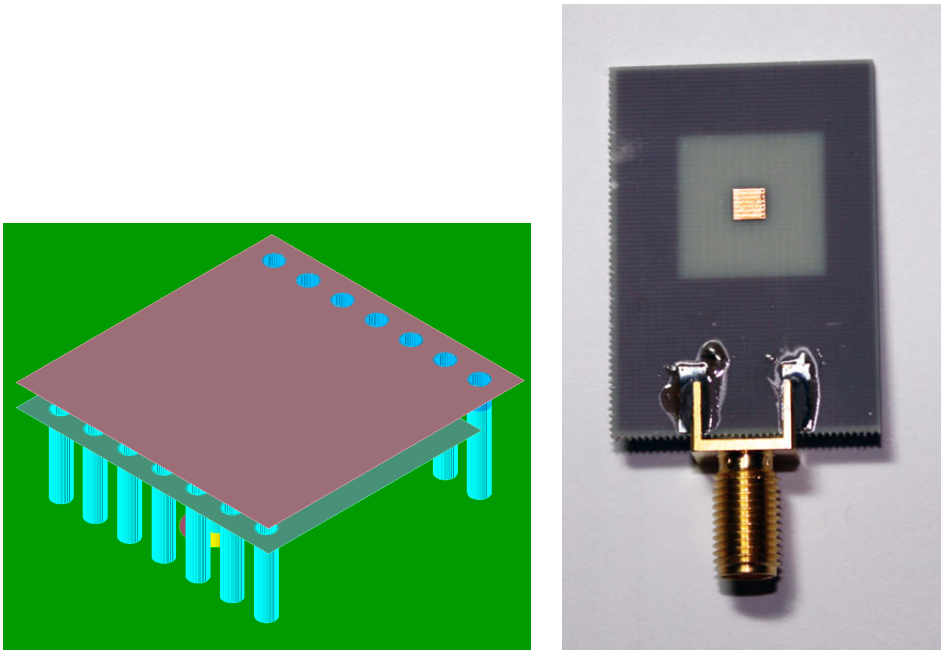


Figure 26: The pattern of the *transmit-only* and *receive-only* elements of the antenna array of the reader.

with short plastic bars (poles), shown in Figure 21b, the relative position of which is non-symmetrical on the array's plane.

The 3D antenna element design is shown in Figure 25 and 27a. A single such element has been measured by itself, i.e., not in the presence of neighboring elements as shown in Figure 27b, and exhibits a return loss of 27.4 dB at a resonant frequency of 5.26 GHz

(measured with a Rohde & Schwarz ZVA 8 Vector Network Analyzer (VNA)), as shown with the solid curve of Figure 29 [59]. The agreement of this measurement with the simulated resonant frequency of 5.33 GHz with a return loss of 13.75 dB, shown with the dotted curve of Figure 29, is relatively satisfying if one considers the inevitable complex 3D manufacturing inaccuracies. Applying, however, the aforementioned miniaturization techniques does not come without cost. The major negative effect is the limited -10 dB bandwidth of this antenna element, which does not exceed 90 MHz (5.21 GHz to 5.30 GHz at -10 dB). Despite this limited bandwidth, the strength of the electric field extracted by these elements, even 500 MHz away from the resonant frequency, is very high ($\geq$ 10 dB), as shown in the performance tests of Section 6.2. This high electric-field strength is, of course, attributed to the very good antenna radiation pattern, simulated with ADS [1] and shown in Figure 28.



(a) (b)

Figure 27: (a) Antenna element simulation setup, (b) Antenna element measurement setup

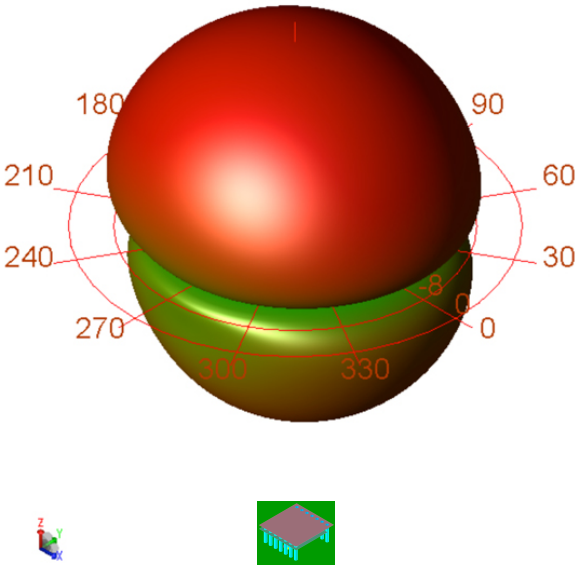


Figure 28: Antenna radiation pattern of an individual element of the antenna array simulated with ADS [1].

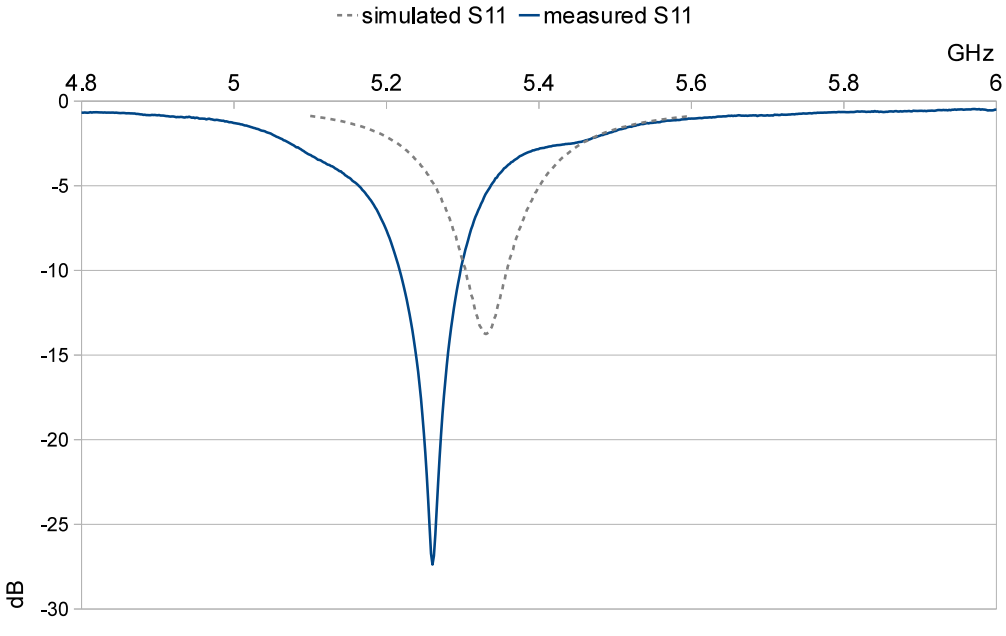
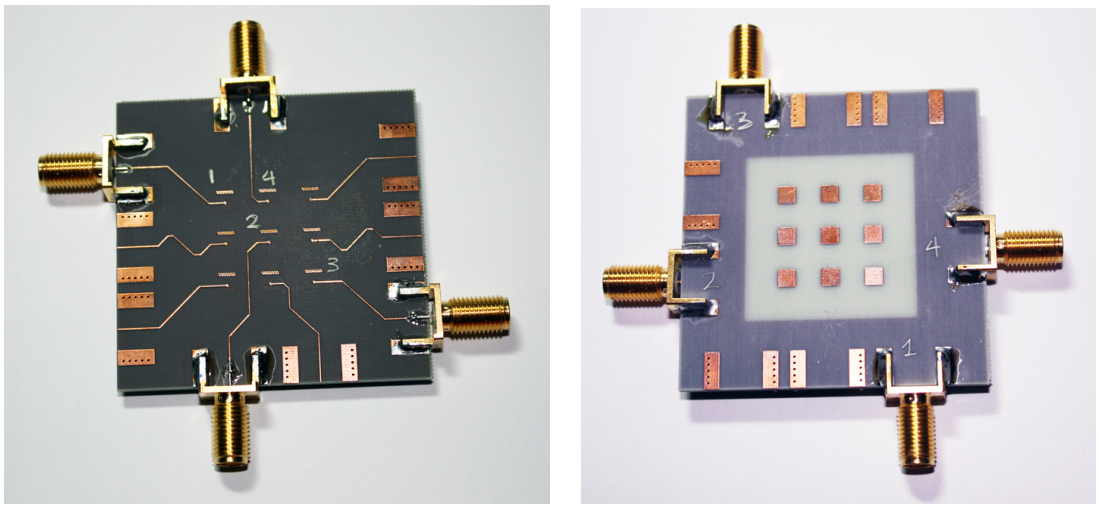
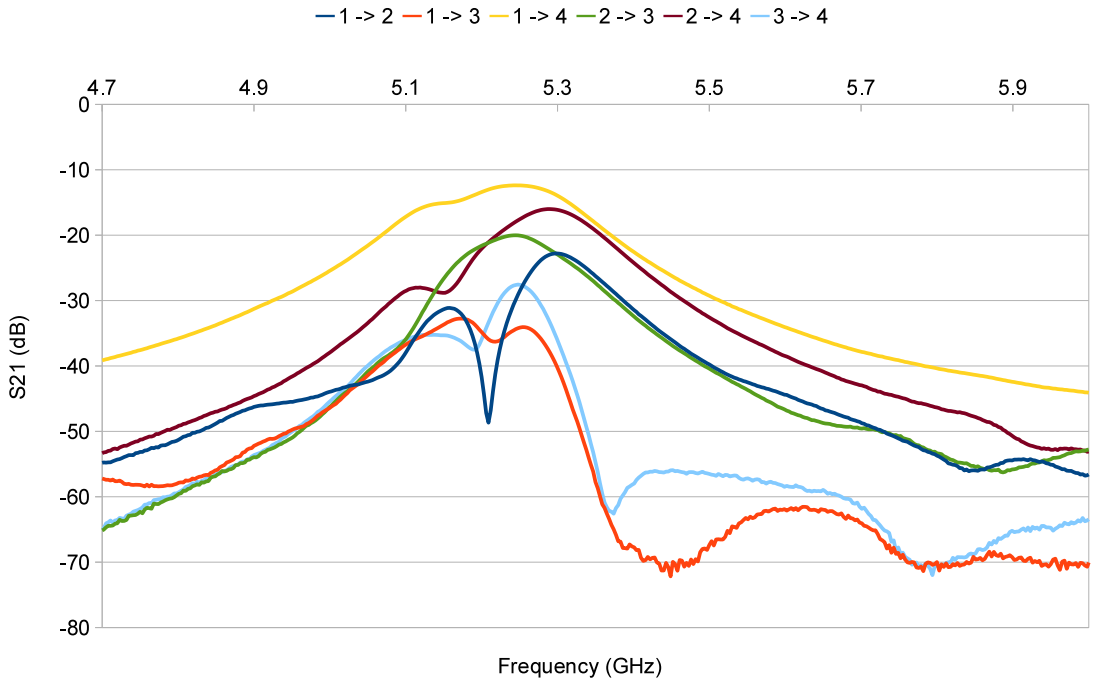


Figure 29: The S_{11} curve of an individual element of the antenna array.

Out of all the 25 elements of the five by five antenna matrix, nine of them operate as *transmit-only* and eight of them as *receive-only*, as shown in the pattern of Figure 26. The transmit- and receive-only elements have been split into four sets of fours, placed as farthest away as possible in the four corners of the array, and the rest eight elements on the virtual cross of the structure are unconnected (not used), with the exception of the central one. This design helps eliminate the need for *single-pole double-throw* (*SPDT*) switches for dual operation of the elements and reduces the number of the required digital input/output control lines. Moreover, the rationale behind this *splitting* is to minimize the coupling that is due to proximity and, thus, attribute most of the coupling measured to the presence of the conductive material of the CoA. To quantify this, the couplings (S_{21} curves) of all possible different antenna element spacing of a subset three by three antenna array, shown in Figure 30a, have been captured over the 4.7 GHz to 6 GHz band at steps of 3 MHz in the absence of any CoA and are presented in Figure 30c [60]. This subset array has been manufactured in the exact same way as the finally used five by five array, so that SMA SHF connectors are available and more intuitive conclusions can be drawn by fewer elements. These six different curves are labeled with a "x $\rightarrow$ y" format; the x corresponds to the transmitting numbered element, as shown in Figure 30a, and the y corresponds to the receiving numbered element. As expected, all curves have their maxima at the range around the resonant frequency of the antenna elements and the shorter the distance between the transmitting and receiving elements the higher this maxima is ($[T_x1 - R_x4] > [T_x2 - R_x4] > [T_x2 - R_x3] > [T_x1 - R_x2] > [T_x3 - R_x4] > [T_x1 - R_x3]$). It should be noted that, given the functionality assigned to the active elements, the worst case scenario for the actual five by five board corresponds to the cases of $T_x1 - R_x2$ (C3-B4) and $T_x2 - R_x3$ (C3-D2), for which the magnitude of the maximum points does not exceed -20 dB. In other words, the maximum coupling between any pair of elements of the 5×5 array in the absence of a CoA never exceeds -20 dB.



(a) (b)



(c)

Figure 30: (a) Bottom and (b) top view of a three by three antenna array fabricated in the exact same way as the five by five array of the NF-CoA reader, (c) S_{21} curves of all possible different antenna element spacing of a subset three by three array in the absence of any CoA.

5.2.2 SP4T Switch Hierarchy

Any particular antenna transmit and receive coupling, out of the 72 possible permutations of the NF-CoA board is chosen by digitally controlling eight identical *single-pole four-throw* (*SP4T*) switches [73], arranged in two hierarchical levels, shown in the block diagram of Figure 31 [60]. Based on this arrangement, there are always two switches preceding the transmit-only antenna element and two switches following the receive-only element. The physical location and order of the switches on the board has been optimized so that the coupling between the SHF lines is minimal. All connections are 50 Ω and it has been ensured that the length of the lines connecting the appropriate switches for any antenna permutation is the same and fixed. The average insertion loss introduced by a single SP4T switch across the 4.5 GHz to 6.5 GHz band has been measured to be 1.07 dB (using the aforementioned VNA). The S_{21} and S_{11} parameters of the two-port system that include the transmit and receive power amplifiers and the intermediate SP4T switch hierarchy are shown in the next section for the case of enabled CAL line.

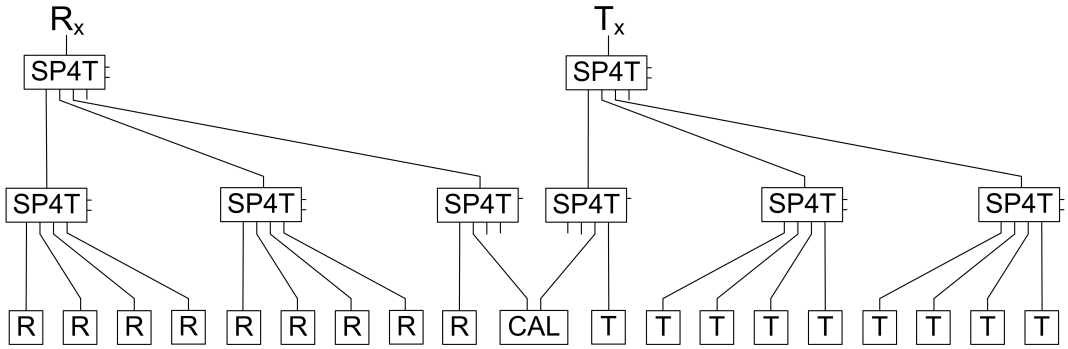


Figure 31: The two-layer SP4T switch hierarchy for enabling any antenna transmit and receive element pair, out of the 72 possible permutations of the NF-CoA board.

The losses introduced by the components of the reader are expected to vary from lot of circuit components to lot and, as a result, from reader to reader. Given that it is very important to achieve consistency and elimination of false negatives among different readers, a calibration technique is deployed. This calibration technique involves measuring all coupling channels (S_{21}) for all possible antenna permutations of each NF-CoA reader over the

entire supported frequency band in the absence of any CoA, namely the "No CoA" curves, and storing these curves into the non-volatile memory of the board. Additionally, a copper line (*CAL line*) that is connecting two unused ports of two SP4T switches, out of the overall four lower-level switches, is also used for calibration purposes. With the help of this *CAL line*, the insertion loss introduced by four consecutive SP4T switches is measured [59]. As shown in Figure 32, the average S_{21} value of -16.57 dB as well as the curve across the 5 GHz to 6 GHz spectrum agree well with the simulated overall loss, which is the sum of the attenuation because of the total line length itself as calculated by ADS [1] and the 4.3 dB attenuation incurred by the four switches.

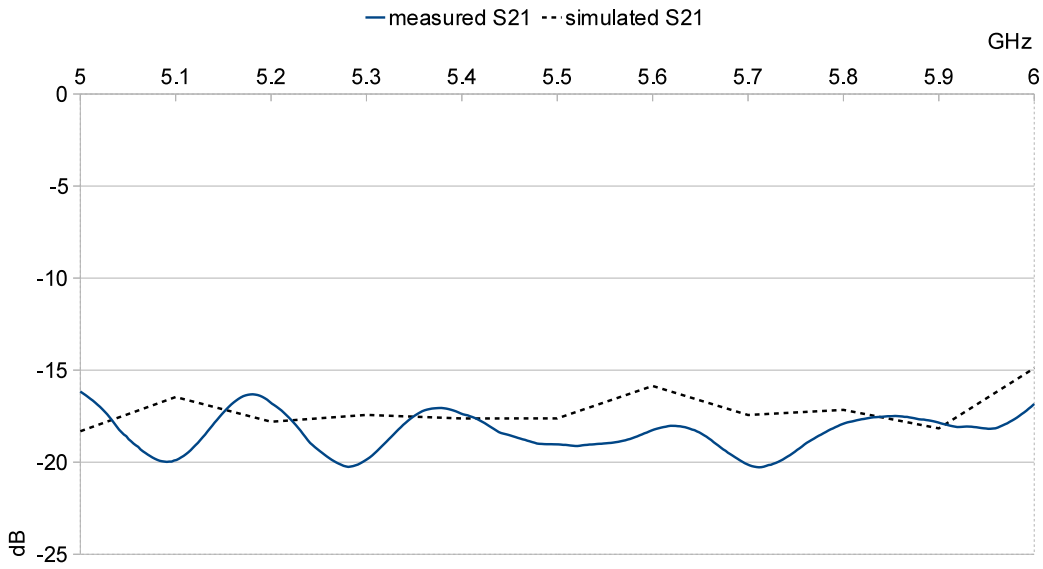


Figure 32: Measured and simulated S_{21} curves of the calibration (CAL) line of the reader board.

5.2.3 SHF Signal Generation and Propagation

The SHF signal radiated toward the NF-CoA instance is generated by selecting any of the two voltage-controlled oscillators (VCOs) [68, 69], which together optimally cover the 5.0 GHz to 6.1 GHz frequency band. The exact mapping of the 0 V to 9.1 V VCO input control voltage range to the VCO output frequency spectrum has been characterized (using the Tektronix RSA 3408A real-time spectrum analyzer (RSA)) and shown in Figure 33.

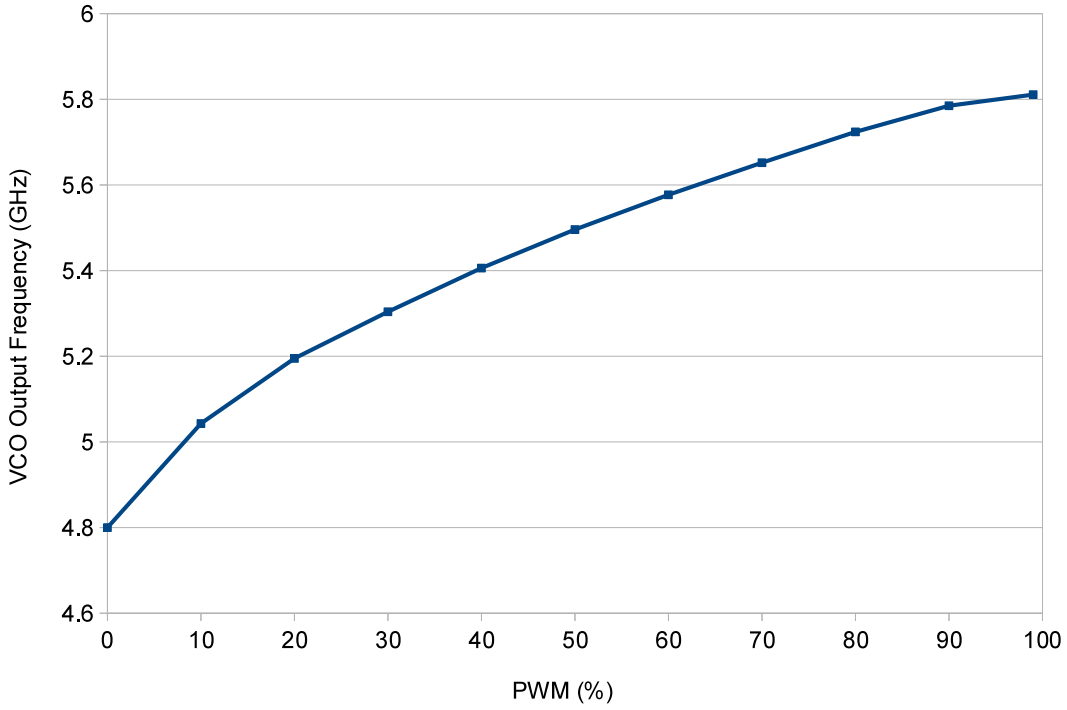


Figure 33: VCO mapping of the 0 V to 9.1 V (0% to 100% PWM) input control voltage range to the 4.8 GHz to 5.8 GHz frequency spectrum.

The peak power of the +2 dBm generated, nearly monochromatic signal, after it is amplified by +11.25 dB by a *power amplifier* (*PA*) [74], is measured 3.94 dBm (using the above RSA) with 50 dB insertion loss. The spectrum content of this SHF signal is shown in Figure 34. The scattered, reflected and refracted signal received is amplified by the same PA and the SHF power is monitored by an RMS PD [75] that yields a ±1 dB accuracy.

According to the data sheet of the PD used [75] for f_{RF} = 5800 MHz, the RF input power range is from −25 dBm to 6 dBm when externally matched to a 50 Ω source and the linear dynamic range for a continuous wave is 31 dB with a ±1 dB linearity error. These values agree very well with a new self-conducted characterization of the PD. Specifically, the voltage output of the PD (approximately 180 mV to 1400 mV) has been accurately mapped to the input generated by a signal generator [76] before the PA ranging from −50 dBm up to 5 dBm for frequency points in the 5 GHz to 6 GHz spectrum and is shown with the graph of Figure 35. Especially for the evaluation of the results of Chapter 6, it is important to estimate the linear dynamic range in mV. Given that the output DC voltage, when no signal is applied to the RF input, is 180 mV and since the output slope is 31 mV/dB, the linear dynamic range in mV is approximately 250 mV to 1211 mV (= 250 mV + (31 dB ∗ 31 mV/dB)). In dB, the linear dynamic range ranges approximately from −35 dBm up to −4 dBm.

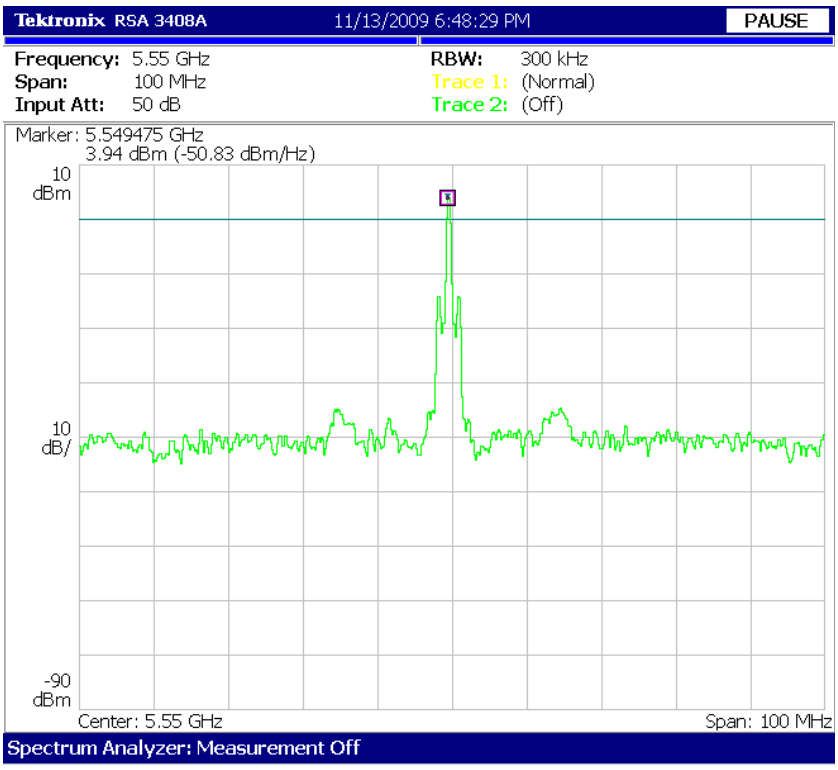


Figure 34: The spectrum content of the super high frequency signal generated by the voltage-controlled oscillator, as captured with a spectrum analyzer

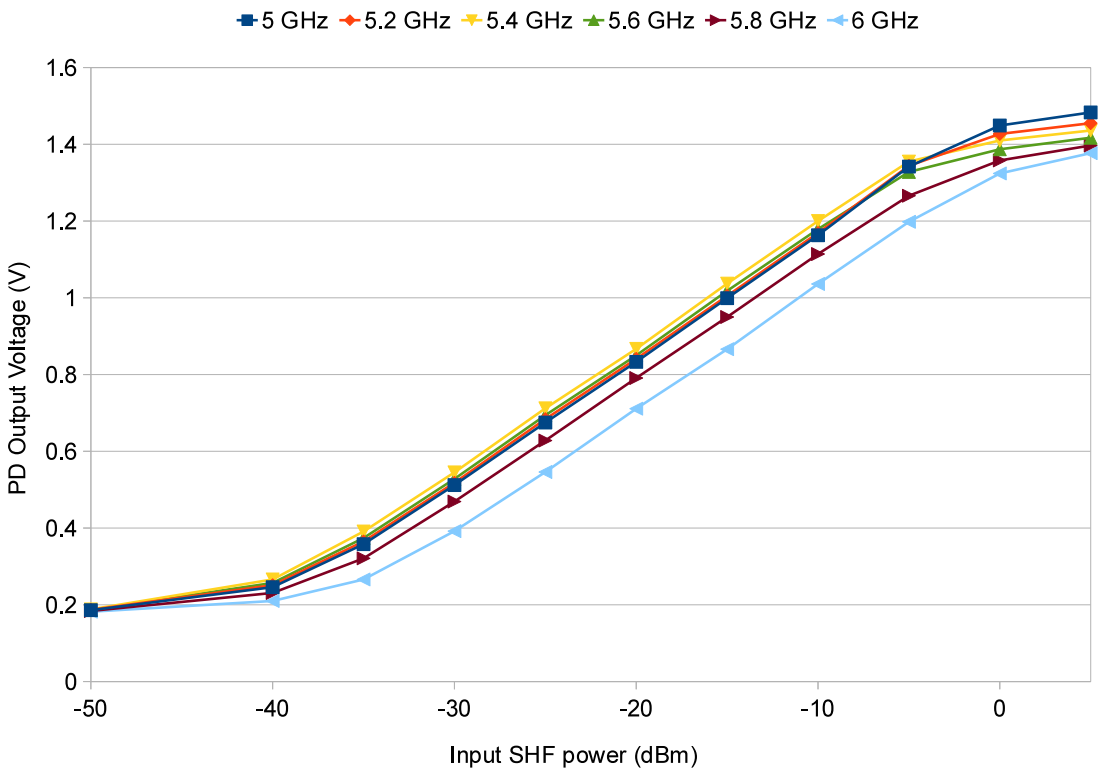


Figure 35: Mapping of the voltage output of the power detector to the input generated by a signal generator.

An example of the clockwise direction of a signal path through the aforementioned and characterized RF components is shown with the red arrows in Figure 36.

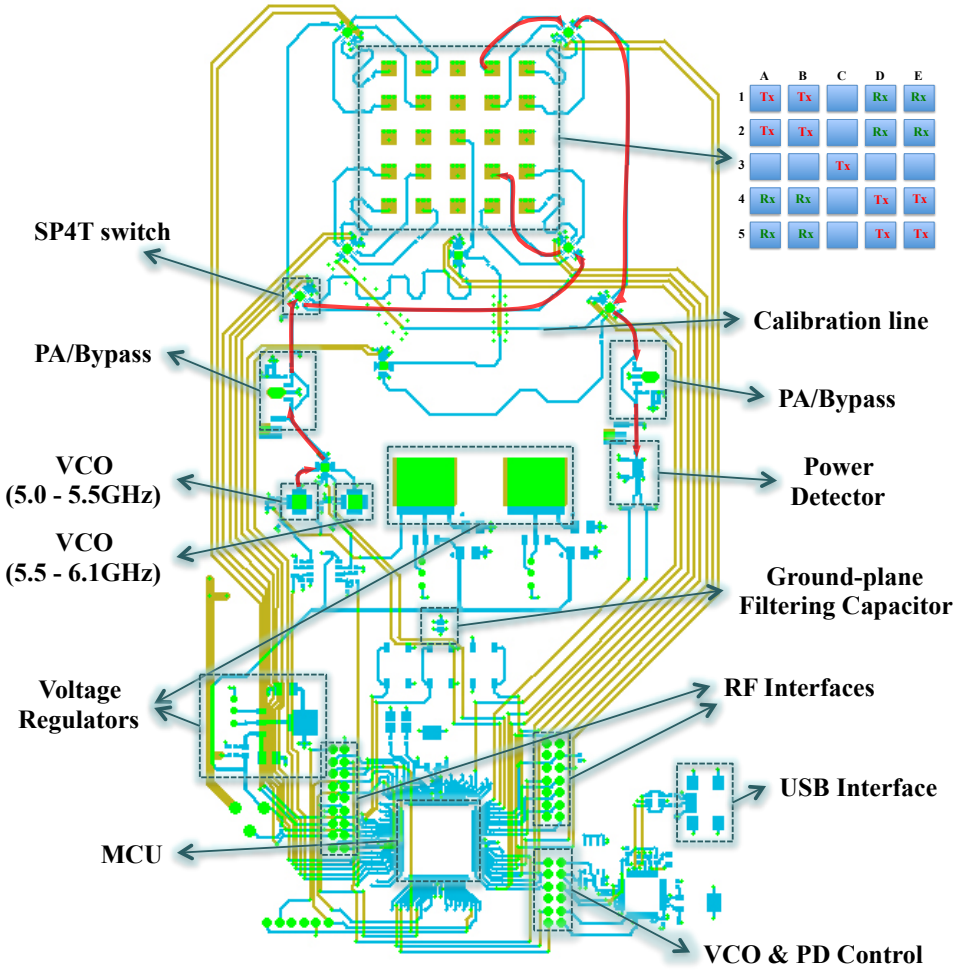


Figure 36: An example of the clockwise direction of a signal path through the RF components of the NF-CoA reader.

5.3 Micro-controller-enabled Reader Operation

The functionality of the NF-CoA reader is summarized in the following four main tasks:

1. generating the appropriate SHF power and controlling the frequency output of the VCO,

2. dictating the path that the SHF signal follows through the two-layer SP4T switch hierarchy and the coupling, eventually, between the T_x and R_x antenna elements,

3. measuring the power captured by monitoring the PD output voltage, and

4. uploading the set of measured data that comprise the fingerprint of the NF-CoA to a computer host or other networked device.

For the last two reader generations, the control of all the digital and analog components of the reader is performed by a 16-bit RISC architecture ultra-low-power TI MCU [77]. The MCU provides multiple digital output pins for controlling the SP4T switches, a connection to a physical push button, a USB interface for data transfer and powering (if battery operation is not desired) and two different RF networking interfaces, briefly described in Section 5.3.4. Of course, a JTAG interface is also provided for re-programming the MCU with the MSP-FET430UIF programmer and the code composer studio (CCS/CCE) Eclipse software development environment.

The algorithm implemented by the developed firmware code in *C* programming language is depicted with the state diagram of Figure 37 [60]. When the power switch of the board is turned on, the MCU finds itself in the low-power mode 4 (*LPM4*) sleep mode. This is the deepest sleep mode with a current consumption of 1.69 μA at 3.0 V, in which the CPU and all clocks are disabled, the crystal oscillator is stopped but the supply supervisor is operational and full RAM memory retention is provided.

In short time intervals the 32 KHz auxiliary clock of the micro-controller is enabled and used to check if the button on the control plane is pressed. Given that a human would

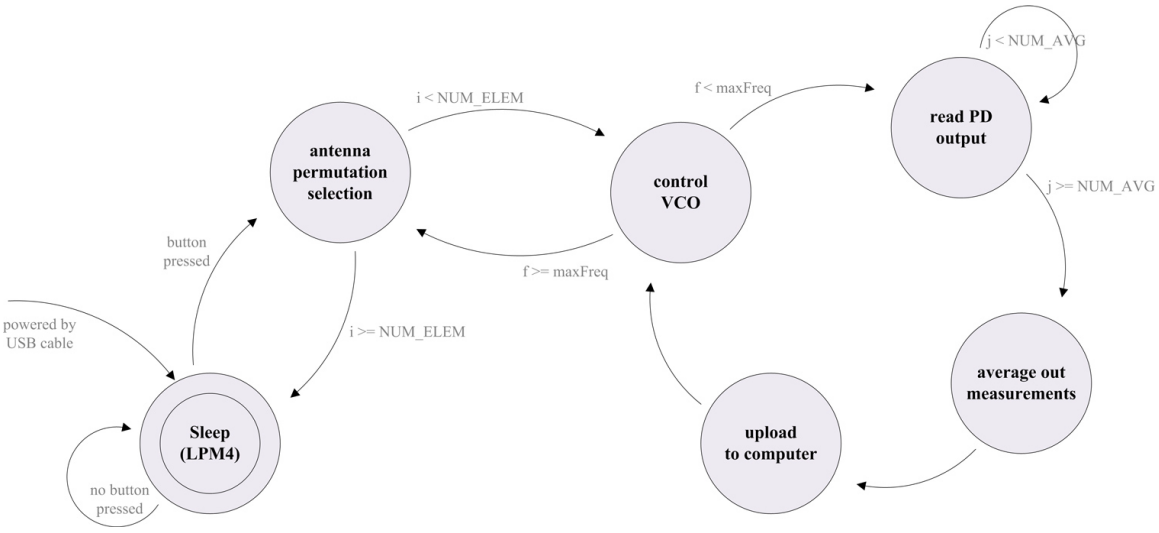


Figure 37: Operational state diagram of the algorithm implemented by the NF-CoA reader.

be pressing the button for at least half a second, the time duration of this button monitoring lasts for only a few milliseconds, leading eventually to a very low duty-cycle monitoring. As soon as a press on the button is detected, the MCU exits the deep sleep mode and transits to the *antenna permutation selection state*. In this state a particular antenna element pair (one antenna element to illuminate the NF-CoA and the other to receive the scattered energy) is selected by appropriately configuring the two digital logic control pins of all the SP4T switches with a 16-bit sequence generated by the digital output pins of the MCU. For instance, coupling $A1 - E1$ is selected with bit sequence 0100000010000001 and $D4 - B5$ with 0011110001001000 . "Logical 0" corresponds to 0 to +0.8 V_{dc} at a current consumption of 5 μA and "logical 1" corresponds to +2.0 to +3.2 V_{dc}, at a current consumption of up to 60 μA (a small fraction of the 2 mA that a single pin of this MCU can drive). This selection remains active until a new bit sequence is generated. The next time the control plane returns to the antenna element pair selection state a check is performed as to whether or not the maximum number of antenna permutations (`NUM_ELEM`), namely 72, has already been selected; in which case the MCU reverts to the sleep mode.

If not all possible antenna element permutations have been enabled, the next step is to generate a sinusoidal power signal at a particular frequency, nearly monochromatic, by controlling the appropriate VCO. The S_{21} NF-CoA fingerprint is captured over the frequency band of 5.1 GHz to 5.9 GHz at 65 steps of 12.3 MHz each. The selection of these steps is achieved by altering the tune voltage of the VCO.

5.3.1 Pulse Width Modulation to Control the VCOs

Since the MCU provides no digital-to-analog (DAC) functionality, the latter is emulated by a high-frequency *pulse width modulation* (*PWM*) signal. In pulse width modulation, the carrier wave is simply a succession of pulses, or a pulse train, and the information modulated onto the carrier is a DC level. Specifically, the output, or average, voltage is configured by a variable duty cycle (D) that can vary from 0 to 1 and is derived from the ratio of the duration of one PWM pulse width (at the level of the USB rail's V_{CC} = 3.2 V) and the time duration of one PWM cycle (*PWM period*), as shown in the following equation

$$V_{out} = D \cdot V_{CC} = \frac{pulse\ width}{PWM\ period} \cdot V_{CC}$$

The averaging out of the PWM waveform cannot only rely upon some property of the load to act as an integrator. Instead, a passive, analog *first order*, or *one pole*, low-pass filter that consists simply of one resistor (R) and one capacitor (C) (see Figure 38) is used [78]. The low-pass filtering, ideally, eliminates the inherent high-frequency harmonic noise components and leaves just the DC content of the waveform.

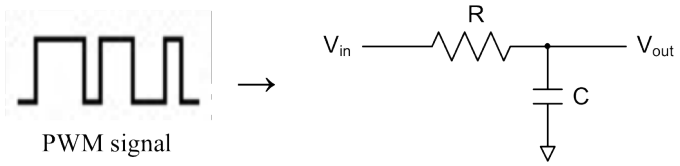


Figure 38: Passive, analog *first order*, or *one pole*, low-pass filter.

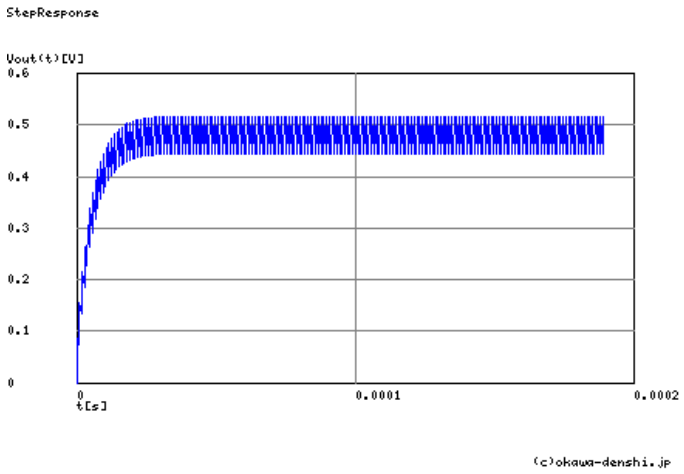
The 3-dB cut off frequency, where the output has dropped by a half compared to the

input, is $f_{cut} = \frac{1}{2\pi RC}$. The product RC is also called the *time constant* (τ) of the filter.

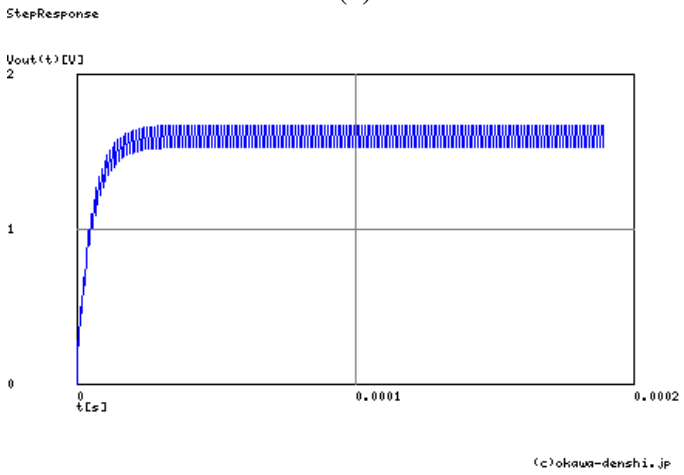
The cut off frequency has to be kept as far away as possible from the PWM carrier wave, or in other words the bandwidth has to be a small fraction of f_{PWM}. The above discussion results in a trade-off between how often it is desired for the NF-CoA reader to perform frequency hopping in the 5 GHz to 6 GHz range and eliminating the ripple effect, as well as making sure the guard delay slot times between consecutive read-outs are maintained, as discussed later with the timing characteristics of the components along the SHF signal path.

Using the sub-main clock (SMCLK) of the MCU, $f_{PWM} \cong 1048$ kHz and the timer period is approximately 488 μs. By picking $R = 53.6\ k\Omega$ (not high so as to keep the system less sensitive to load resistance) and $C = 100$ pF, the cut-off frequency is satisfyingly small $f_{cut} = 29.7$ kHz compared to f_{PWM} and equally significantly the peak-to-peak ripple voltage is $V_{pk-pk} = 0.142$ V for the worst case scenario of $D = 50\%$ [79]. The step response of the used first order filter, i.e., the time description of how it responds to a step input, for different duty cycles, namely 15%, 50% and 99%, is shown in Figure 39. For all three different cases of duty cycles shown, the settling time is $t_r = 12.342\ \mu sec$ to reach the final V_{out} levels of $g(\infty) = 0.48$ V (D = 15%), $g(\infty) = 1.60$ V (D = 50%) or $g(\infty) = 3.168$ V (D = 99%).

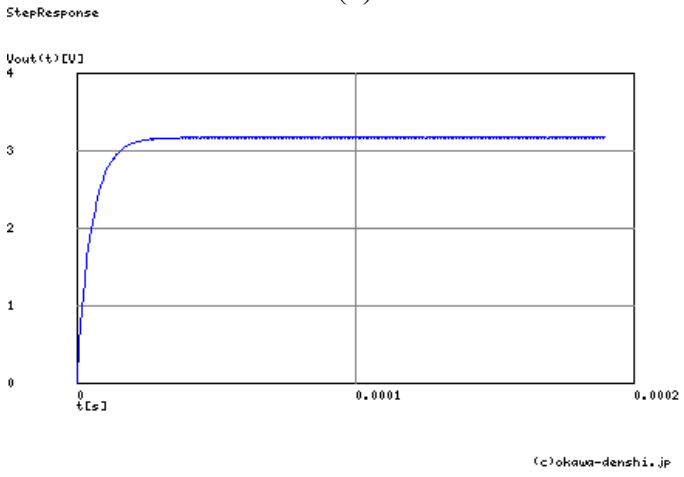
Returning back to the control of the VCOs, the mapping of the 0 V to 3.2 V filtered PWM output signal to the 0 V to 10 V tune voltage range of the VCO is done by an intermediate *non-inverting operational amplifier* (*OpAmp*) [80], the schematic of which is shown in Figure 40. With appropriate biasing ($V_P = 9.19$ V and $V_N = 0$ V), input voltage levels ($V_1 = 0$ V and $V_2 = V_{PWM}$ up to 3.2 V) and resistor values ($R_1 = 15\ k\Omega$, $R_2 = 2.2\ k\Omega$, $R_f = 33\ k\Omega$ and $R_g = 19.1\ k\Omega$), the non-inverting gain (V_{out}/V_2) of the operational amplifier is 2.87 and for the maximum input voltage of $V_2 = 3.2$ V the non-clipped output voltage is 9.18 V. Table 3 provides the PWM and OpAmp output voltage levels for different duty cycles of the PWM, as well as the actual frequency generated by the VCO. A graphical



(a)



(b)



(c)

Figure 39: The step response of the *first order*, or *one pole*, low-pass filter for different duty cycles, namely 15%, 50% and 99%.

representation of the actual generated VCO frequency as a function of the PWM duty cycle is provided in Figure 33.

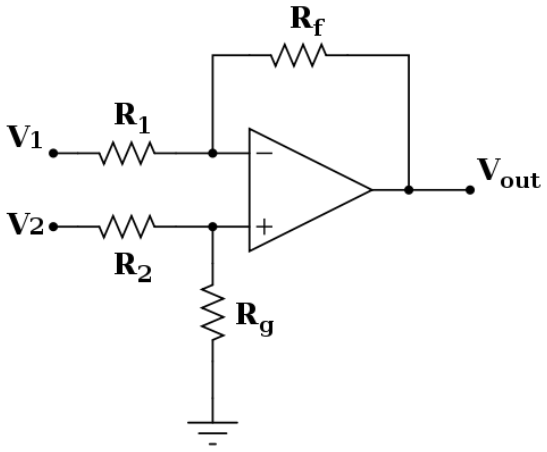


Figure 40: The schematic of the non-inverting operational amplifier that maps the 0 V to 3.2 V filtered PWM output signal to the 0 V to 10 V tune voltage range of the VCO.

Table 3: PWM and OpAmp output voltage levels for different PWM duty cycles.

PWM (%)	PWM Output Voltage (V)	OpAmp Output Voltage (V)	OpAmp Gain Factor	VCO Output Frequency (GHz)
10	0.307	1.018	3.315960912	5.043
20	0.607	1.977	3.257001647	5.195
30	0.907	2.935	3.235942668	5.304
40	1.207	3.895	3.227009114	5.406
50	1.508	4.854	3.218832891	5.496
60	1.808	5.813	3.215154867	5.577
70	2.108	6.77	3.211574953	5.652
80	2.408	7.73	3.21013289	5.724
90	2.708	8.69	3.20901034	5.785
99	2.979	9.1	3.054716348	5.811

The next time the control plane returns to the *control VCO state* a check is performed as to whether or not the maximum number of frequency steps (`maxFreq`), namely 65, has already been reached; in which case the MCU returns to the *antenna permutation selection state*.

5.3.2 Analog-to-Digital Conversion

With the T_x antenna element radiating power toward the NF-CoA that is placed just 2 mm against the antenna matrix, the next step is to amplify the captured reflected and refracted signal and feed it to the power detector of the board. The PD output voltage, which essentially represents the received signal strength, is read by the ADC of the MCU with its highest 12-bit precision mode.

Based on measurements carried out under a controlled environment of pre-configured signal power amplitude and before applying the PWM filtering of the previous section, it has been found that a single analog-to-digital conversion is not enough. In particular, although the voltage reference used (3.2 V) for the ADC and supplied by the USB input has been measured to remain steady over time, AD conversions have been recorded to be as far as 20% off from the same actual input signal for more than 100 duplicate measurements.

In addition, of course, to the inaccuracy introduced by the output of the PD, pointed out above, the two major sources of inaccuracy in the ADC testing of mixed-signal circuits have been identified to be the approximations of IEEE standard for digitizing waveform recorders and IEEE standard for terminology and test methods for analog-to-digital converters [81] and the fact that the DC offset and the amplitude of the input analog signal evaluated on the base of the digital output differ from their true values [82]. However, this deviation easily drops to less than 8% by performing 20 consecutive conversions (measurements) of an NF response at a particular antenna configuration and frequency, storing them in the *successive approximation register* of the MCU and afterward simply averaging them. The latency incurred, as a result of the additional 19 conversions, is totally negligible given that each 12-bit resolution conversion requires only 13 MCU clock cycles, the total time duration of which is 0.65 μsec for a MCU clock speed of 20 MHz. The `NUM_AVG` variable shown in the state diagram of Figure 37 corresponds to the maximum number, that is, 20, of consecutive analog-to-digital conversions before the averaging is performed.

Each payload triplet entry consisting of the antenna permutation, the frequency and the

received power in dB is uploaded to the computer at 57.6 Kbps with the use of the USCI module of the MCU that supports the UART protocol used to communicate with the TI TUSB chip [83].

After the above steps are completed, the MCU algorithm performs a check of whether or not the maximum number of frequency steps has already been reached; in which case the full frequency spectrum for a single antenna permutation has been swept and the MCU jumps to the next antenna permutation. At this point, a check is also done about whether or not the maximum number of antenna permutations has already been selected; in which case the MCU reverts to its LPM4 sleep mode. An LED that remains on until all the aforementioned steps for the NF fingerprint extraction are completed is indicative of the activity of the control plane before it returns back to its sleep mode state.

5.3.3 Component Timing Characteristics

The timing characteristics of all the components across the SHF signal path have to be carefully considered, since the maximum component delay will define the minimum guard time that the NF signature extraction process has to adhere to to guarantee reliability of the measurements.

The power detector [75] requires 8 μs of *fall time* to drop from 90% to 10% of its full dynamic range, 1 μs of *turn-on time* and 1 μs of *settling time*. An SP4T switch [73] requires 50 ns of *rise* or *fall time* (10% to 90% and vice versa of its full dynamic range) and 120 ns of *turn-on* and *turn-off time*. The first order, low-pass filter requires a settling time of 12.342 μsec, as calculated above. So, it is concluded that the source of lag, which overlaps the delay times of all other components, is the PWM filter. The latter's *settling time* eventually determines the guard, i.e., "wait," time of the MCU. For the currently developed and programmed running firmware version, the overall time required to capture a full NF signature of $N_{coupl} = 72$ S_{21} curves is around 30 seconds. This time currently includes additional, significantly conservative long guard times that are maintained between the aforementioned consecutive operations and can be removed from future software versions.

5.3.4 Wireless Network Connectivity

Small *802.15.4/Zigbee* and *Bluetooth* modules can be readily attached to the provisioned 18-pin connector of the second and third generation of the MCU-enabled NF-CoA reader of Chapter 5 to provide the corresponding desired network functionality. Specifically, two compatible wireless networking module options are the TI CC2530 [84] System-on-Chip for 2.4 GHz IEEE 802.15.4/ZigBee and the TI CC2540 [85] for Bluetooth, respectively.

CHAPTER 6

NF-COA SYSTEM PERFORMANCE EVALUATION

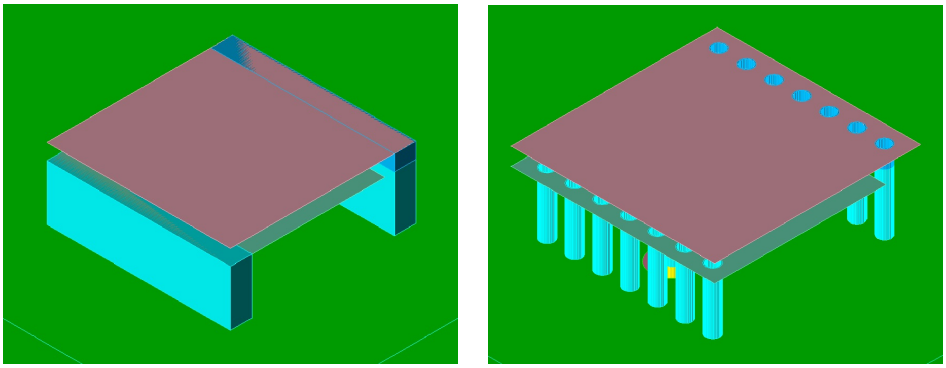
Different types of tests, ranging from near-field (NF) scattering simulations to real inter- and intra-CoA measurements, have been conducted to assess the feasibility and performance of the realized NF authenticity certification technology [60] and are presented in this chapter.

For all tests presented in this chapter, physical objects that are conceptually very close to the final envisioned certificate instance have been used as NF-CoAs. These types of objects, both copper-based and inkjet-printed, are presented in Section 4.1.

6.1 Simulations for Entropy Evaluation

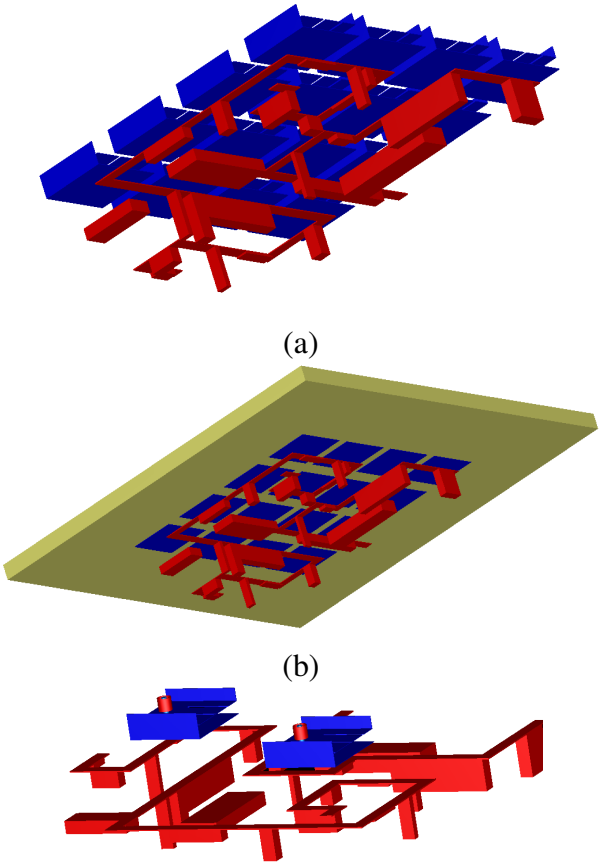
Simulations have been conducted not only for the estimation of the reflection coefficient (S_{11}) of an element of the antenna array (as shown in Section 5.2.1) or the losses introduced by the SP4T hierarchy as the SHF signal propagates through them, but also to obtain a first evaluation of the entropy of the near-field scattering response of a 3D NF-CoA. Toward the latter goal and given the complexity and the time required for the simulation to complete, a simplified structure of an antenna element, shown in Figure 41a, was designed in ADS [1] besides the initially used detailed full structure, shown in Figure 41b. For the same main reason of long simulation required, the simulation results shown below are extracted from a 4 by 4 (instead of 5 by 5) antenna array, depicted in Figure 42. The resolution used for the simulation is 60 cells/wavelength.

The designed 2 mm thick "random" scatterer that is not encapsulated in any dielectric material, but rather is surrounded by just plain air, is shown with red color in Figure 42. In this same figure, the scatterer is placed at a distance of just 1 mm against the antenna array, which is shown with blue color. The FR4 [86] dielectric material shown with golden color in Figure 42b has been removed in 42a for an unobstructed view of the shorted-patch



(a) (b)

Figure 41: (a) Simplified and (b) Detailed design of the structure of an element of the antenna array of the NF-CoA reader in ADS [1].



(a)

(b)

(c)

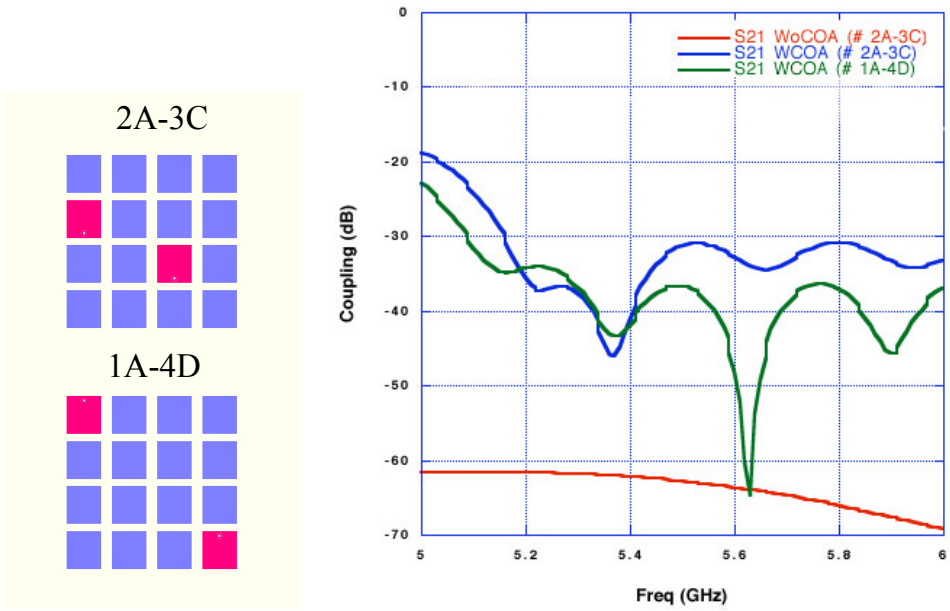
Figure 42: The designed 2 mm thick “random” scatterer that is surrounded by just plain air (shown with red color) is placed at just 1 mm against the antenna array (shown with blue color) in ADS [1].

antenna array consisting of the aforementioned simplified antenna elements.

The NF signature simulation results correspond to two different $T_x - R_x$ couplings, namely $2A - 3C$ and $1A - 4D$ (see Figure 43a). For faster convergence of the ADS simulation, all but the two antenna elements used were removed, as depicted in Figure 42c. The simulated S_{21} curves of Figure 43b in the reactive near-field proximity of the NF-CoA reader (blue line for coupling $2A - 3C$ and green line for coupling $1A - 4D$) exhibit not only significant difference between them but also show a significant variance of almost 30 dB across the 5 GHz to 6 GHz frequency range.

The red curve in Figure 43b corresponds to the simulated coupling of the $2A - 3C$ antenna permutation over the air medium and in the absence of the CoA. It is interesting to note that the magnitude of this curve does not exceed −60 dB despite the short distance of the involved antenna elements, as shown in the top of Figure 43a. In reality, however, and as is shown with the measured results of subsection 6.2.1, the antenna coupling in the absence of any CoA instance is higher and the reason this is not reflected here is due, mostly, to the simplifications made for the simulation, including the absence of the neighboring antenna elements.

The simulation results were encouraging enough and urged the conductance of real measurements of fabricated NF-CoAs, the results of which are presented in the next section.



(a) (b)

Figure 43: The simulated S_{21} curves when a CoA is in the reactive near-field proximity or not of the antenna array of the NF-CoA reader.

6.2 Performance Measurements

For the measurements conducted in this section, both types of NF-CoA instances, namely copper-based and inkjet-printed ones, are attached to the reader antenna slot against the antenna matrix of the manufactured NF-CoA reader through the non-symmetric plastic poles, shown in Figure 44, at a distance of 2 to 3 mm. This short spacing is actually equal to the thickness of the plastic bolts that hold the plastic poles shown in Figure 44. Alternatively, a sturdy dielectric foam material with characteristics close to that of air, i.e., relative dielectric constant ϵ_r close to 1, can be used.

The conductive inkjet-printed nano-particle material of the, stacked or single, paper-based 2D CoAs occupied an area of 31.65 mm $\times$ 31.6 mm centered around the 5 by 5 antenna array, which occupies a lateral area of 31.70 mm $\times$ 31.51 mm.

As for the copper-based CoAs, these were designed to occupy a smaller area of 27 mm$\times$ 27 mm. The reason for the decreased 2D projection area is to increase their practicality

and ease of attachment on physical objects but, in the same time, without sacrificing the entropy yielded, as examined in the following subsections, as well as in Chapter 7. Instead of keeping the sides of the orthogonal NF-CoA instances parallel to those of the antenna array, the position of these certificates has been rotated around the central axis of the array so that the radiation of as many antenna elements as possible closer to the periphery of the array is "disturbed" by the NF-CoA. This is clearly shown in Figure 45a. Certificates *I* and *J*, however, comprise the exceptions since their cross-section area of 56 mm × 56 mm intentionally exceeded that of the antenna array for testing purposes. That is why six holes, as many as the plastic poles of the antenna array of the reader, had to be drilled through certificates *I* and *J* (see Figure 8 and 45b). For the reader's reference, whenever a full-sized CoA is mentioned, either certificate *I* or *J* is referred to.

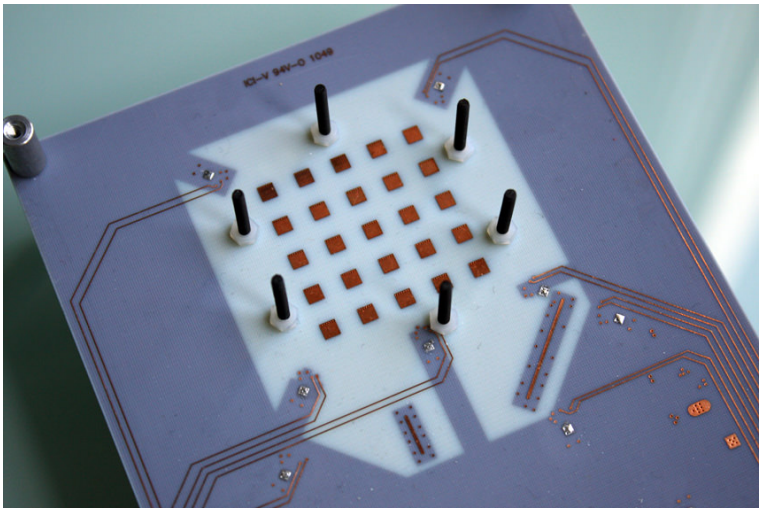
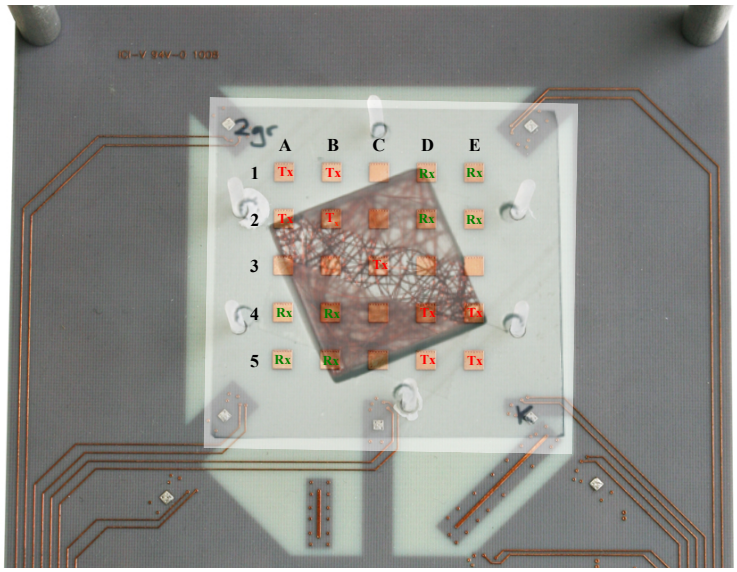
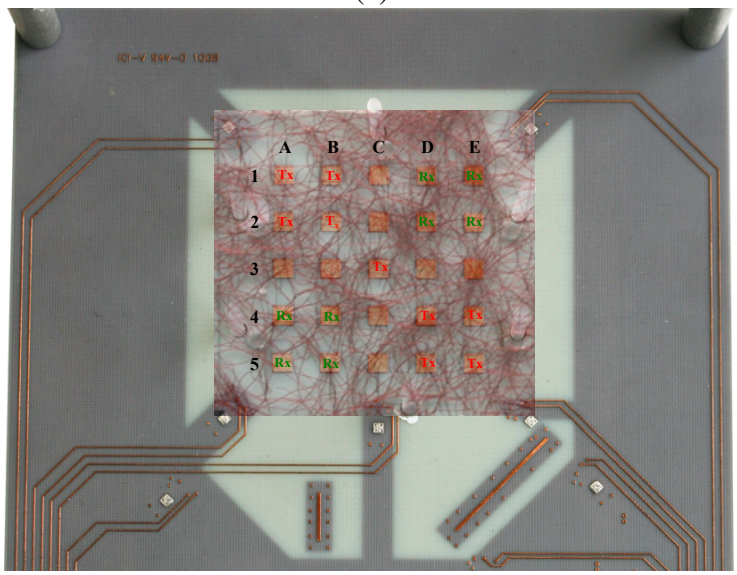


Figure 44: The non-symmetric topology of the plastic poles that form the preliminary certificate slot of the NF-CoA reader against the antenna array.



(a)



(b)

Figure 45: Top view of the NF-CoA reader with (a) a small-sized and (b) a full-sized copper-based certificate instance fastened to the annotated antenna array slot.

The extraction and processing of the certificate fingerprints is done as follows:

- A parser developed with *C#* programming language reads the raw information extracted by the USB-connected reader of Section 5 and converts it to a comma separated value (CSV) sheet that can be imported into Matlab [87].

- Matlab code both helps visualize the entropy through plots, following the procedure

described below, and quantifies the entropy, the results of which are presented in Chapter 7.

In each of the graphs presented hereafter, the y axis corresponds to the output of the power detector (PD) based on its received signal strength of the nearly monochromatic signal. The x axis corresponds to the either different frequency points chosen through the voltage-controlled oscillator (VCO) or all the available antenna couplings chosen through the hierarchy of SPDT RF switches. Although one could say that, visually speaking, two types of NF signatures exist, based on if

- scattering parameter curves of particular antenna couplings are plotted over a spectrum of chosen frequency points, or
- scattering parameter curves of particular frequencies are plotted over all available antenna couplings,

these two types of graphs are essentially the same, since they correspond to the exact same certificate instance measurement. In many tests described below, both types of graphs are provided for a better understanding of the results.

In the first case, the color bar on the right of the graph corresponds to all the available antenna couplings, with numbers ranging from 1 to 72. A mapping of these numbers to the actual antenna couplings of the antenna array of Figure 46 is provided in Table 4. Respectively, in the second type of NF signature graph, the color bar on the right corresponds to the frequency points measured.

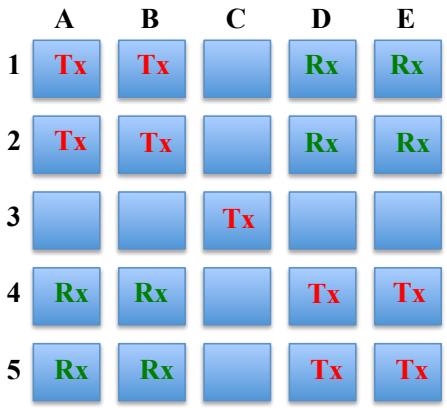


Figure 46: Annotated diagram of the antenna elements of the array of the NF-CoA reader.

Table 4: Numbering of the couplings between antenna elements of the NF-CoA reader.

A1-A4 → 1	B1-B4 → 19	D4-D1 → 37	E4-E1 → 55
A1-A5 → 2	B1-B5 → 20	D4-D2 → 38	E4-E2 → 56
A1-B4 → 3	B1-D1 → 21	D4-E1 → 39	E5-A4 → 57
A1-B5 → 4	B1-D2 → 22	D4-E2 → 40	E5-A5 → 58
A1-D1 → 5	B1-E1 → 23	D5-A4 → 41	E5-B4 → 59
A1-D2 → 6	B1-E2 → 24	D5-A5 → 42	E5-B5 → 60
A1-E1 → 7	B2-A4 → 25	D5-B4 → 43	E5-D1 → 61
A1-E2 → 8	B2-A5 → 26	D5-B5 → 44	E5-D2 → 62
A2-A4 → 9	B2-B4 → 27	D5-D1 → 45	E5-E1 → 63
A2-A5 → 10	B2-B5 → 28	D5-D2 → 46	E5-E2 → 64
A2-B4 → 11	B2-D1 → 29	D5-E1 → 47	C3-A4 → 65
A2-B5 → 12	B2-D2 → 30	D5-E2 → 48	C3-A5 → 66
A2-D1 → 13	B2-E1 → 31	E4-A4 → 49	C3-B4 → 67
A2-D2 → 14	B2-E2 → 32	E4-A5 → 50	C3-B5 → 68
A2-E1 → 15	D4-A4 → 33	E4-B4 → 51	C3-D1 → 69
A2-E2 → 16	D4-A5 → 34	E4-B5 → 52	C3-D2 → 70
B1-A4 → 17	D4-B4 → 35	E4-D1 → 53	C3-E1 → 71
B1-A5 → 18	D4-B5 → 36	E4-D2 → 54	C3-E2 → 72

The conversion of the PD output voltage to a SHF power signal reading (in dB) is based on the PD characterization presented in Section 5.2.3. In particular, the equations that correspond to the curve fitting of Figure 35 at different equidistant points of the frequency range under examination are provided in Table 5. Whenever the Euclidean distance between different NF signatures is considered, the preferred unit on the y axis is mV instead

of dBm. The reason for this is to help the reader gain a better understanding of the actual signature differences with respect to the PD dynamic range, that is, what fraction of the linear and the entire dynamic range of the PD does a particular signature difference correspond to. Of course, wherever deemed necessary (as for example in Section 6.2.5) the actual difference in dB is provided. As for the conversion of the voltage input of the VCO to the frequency of the generated nearly monochromatic signal, that is based on the VCO characterization of Section 5.3.1. The equation that corresponds to the curve fitting of Figure 33 at different equidistant points of the frequency range under examination is provided in Equation (7).

Moreover, it should be noted that the above conversions, and, as a result, the computational burden of calculating the 4^{th} order polynomials, not only are not part at all of the CoA issuing and verification procedures, but also are not run locally on the NF-CoA reader. Instead they are run on a desktop computer with Matlab and the only reason the curve fitting equations are provided here is for clarification purposes in the context of this chapter and so that the reader has a clear view of the real frequency points and the signal power magnitudes involved.

$$Freq_{out}(GHz) = 6 \cdot 10^{-8} \cdot [V_{out}(mV)]^5 - 7 \cdot 10^{-6} \cdot [V_{out}(mV)]^4 + 0.0003 \cdot [V_{out}(mV)]^3 - 0.007 \cdot [V_{out}(mV)]^2 + 0.1048 \cdot V_{in}(mV) + 5.0617 \quad (7)$$

Table 5: 4^{th} order polynomial regression of the power detector output.

Frequency (GHz)	$P_{out}(dB)$
5.0 GHz	$-10^{-4} \cdot [V_{out}(mV)]^4 + 0.0005 \cdot [V_{out}(mV)]^3 + 0.0144 \cdot [V_{out}(mV)]^2 + 0.033 \cdot V_{out}(mV) + 0.1312$
5.2 GHz	$-10^{-4} \cdot [V_{out}(mV)]^4 + 0.0005 \cdot [V_{out}(mV)]^3 + 0.0144 \cdot [V_{out}(mV)]^2 + 0.035 \cdot V_{out}(mV) + 0.131$
5.4 GHz	$-10^{-4} \cdot [V_{out}(mV)]^4 + 0.0004 \cdot [V_{out}(mV)]^3 + 0.0146 \cdot [V_{out}(mV)]^2 + 0.0459 \cdot V_{out}(mV) + 0.123$
5.6 GHz	$-6 \cdot 10^{-5} \cdot [V_{out}(mV)]^4 - 0.0005 \cdot [V_{out}(mV)]^3 + 0.0223 \cdot [V_{out}(mV)]^2 + 0.0176 \cdot V_{out}(mV) + 0.1442$
5.8 GHz	$-3 \cdot 10^{-5} \cdot [V_{out}(mV)]^4 - 0.0014 \cdot [V_{out}(mV)]^3 + 0.0315 \cdot [V_{out}(mV)]^2 - 0.0326 \cdot V_{out}(mV) + 0.1839$
6.0 GHz	$-4 \cdot 10^{-5} \cdot [V_{out}(mV)]^4 - 0.001 \cdot [V_{out}(mV)]^3 + 0.0321 \cdot [V_{out}(mV)]^2 - 0.0654 \cdot V_{out}(mV) + 0.2162$

Essential to the evaluation of the results of the following tests is the *standard deviation* (*std*); the square root of an estimator of the variance of the received signal strength x_i for N different CoAs at the same frequency points and antenna couplings. The most commonly used estimator for σ is an adjusted version (based on estimation theory), the *sample standard deviation*, defined as follows:

$$std \triangleq \left(\frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})^2 \right)^{\frac{1}{2}}$$

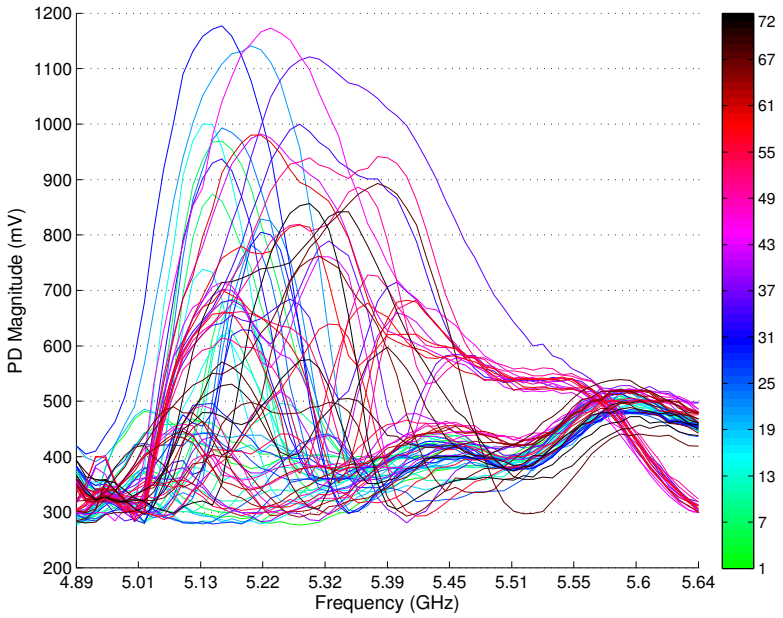
where $\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$. The reason for adopting this estimator is that, when the mean of a population, the variance of which is to be estimated based on samples, is unknown, the sample variance underestimates the true value of the population variance (biased estimator) [88, 89]. Removing this bias from the population variance estimator is done with a correction, known as Bessel's correction [90, 88], which multiplies the standard sample variance by $N/(N-1)$.

6.2.1 NF Response Before and After Attaching an NF-CoA

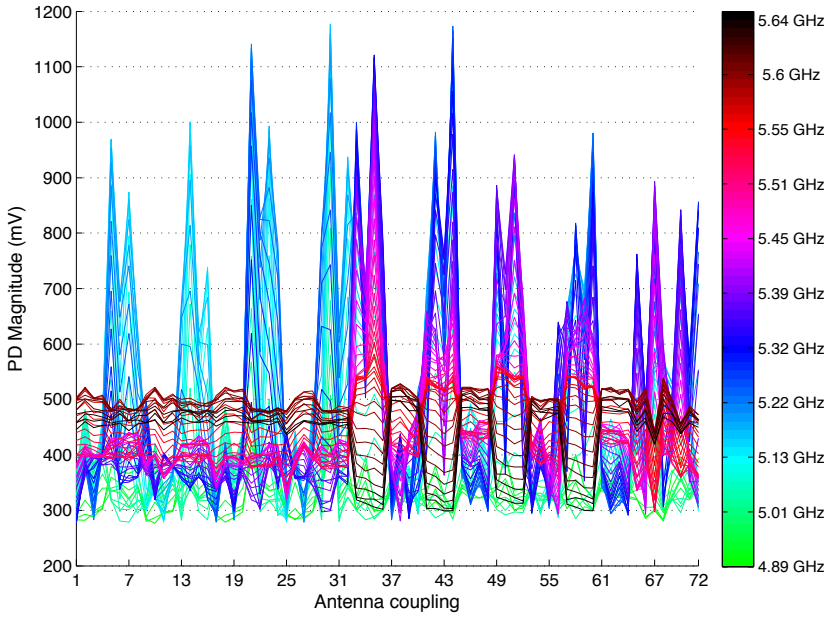
When no certificate instance is attached to the reader, the *No CoA* near-field electromagnetic response comprises the antenna couplings shown in Figure 47. As explained in the introduction of this section, the same *No CoA* signature is shown for both varying frequency points and varying antenna couplings.

As a very first step toward evaluating the performance of the NF-CoA system, what needs to be assessed and verified is that the close proximity of an NF-CoA to the antenna array does significantly disrupt the NF response, compared to the case where no certificate instance is attached to the reader. In this test, the difference between the NF signatures of the *No CoA* case and the signatures of randomly chosen copper-based certificates *2gF*, *2gC*, *2gJ* and *3gJ* is measured and presented in Figure 48. The range of the disruption caused by the presence of the certificate instance exceeds in some cases 650 mV. For a better understanding of how large this disruption is, one should take into account that the linear dynamic range of the used power detector [75], as measured in Section 5.2.3, is 250 mV to 1211 mV and the overall dynamic range is approximately 180 mV to 1400 mV. This means that the differentiation due to the disruption caused by the presence of the copper-based certificate instances is approximately up to 68% of PD linear dynamic range or 53% of PD overall dynamic range.

The same behavior is also noticed when paper-based NF-CoAs, specifically *B*, *C*, *D*, and *I* are used, as shown in Figure 49. The range of the disruption caused by the presence of the certificate instance exceeds in some cases 850 mV. Consequently, the differentiation due to the disruption caused by the presence of the paper-based certificate instances is approximately up to 88% of PD linear dynamic range or 70% of PD overall dynamic range.

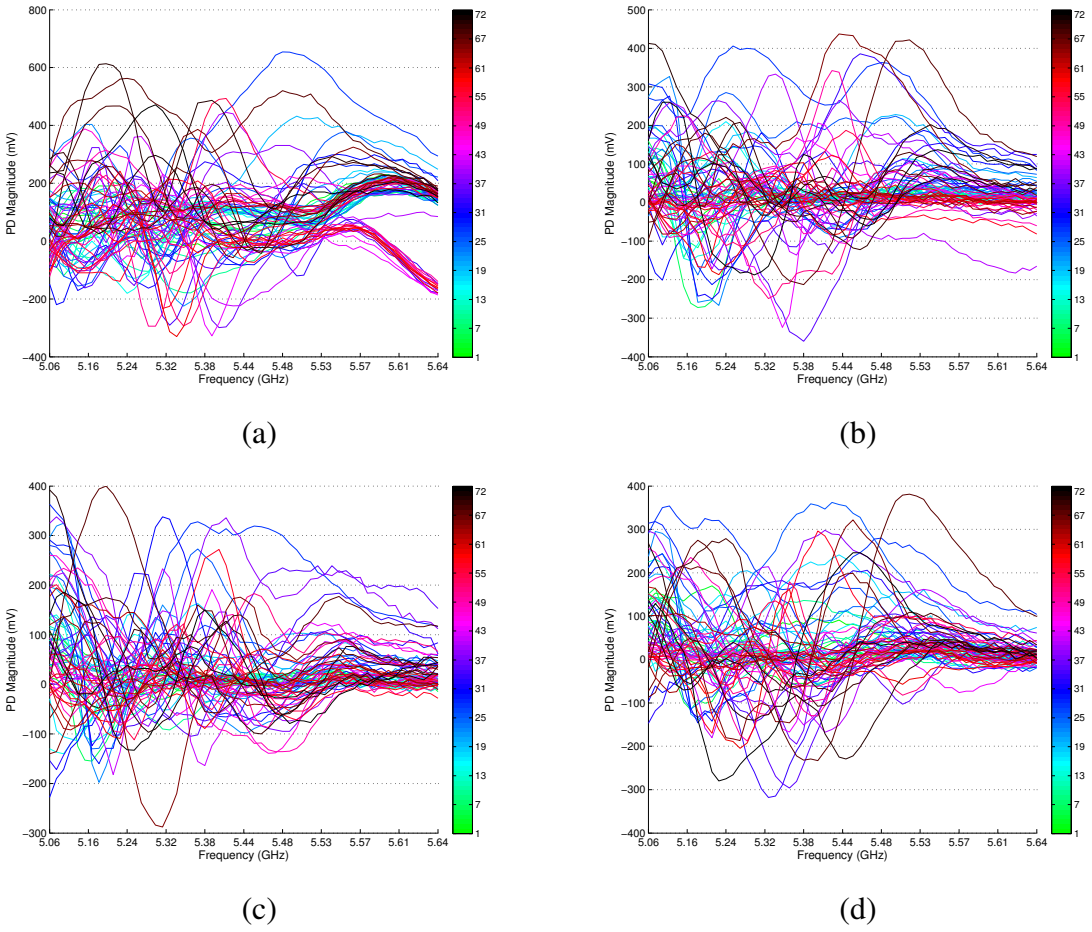


(a)



(b)

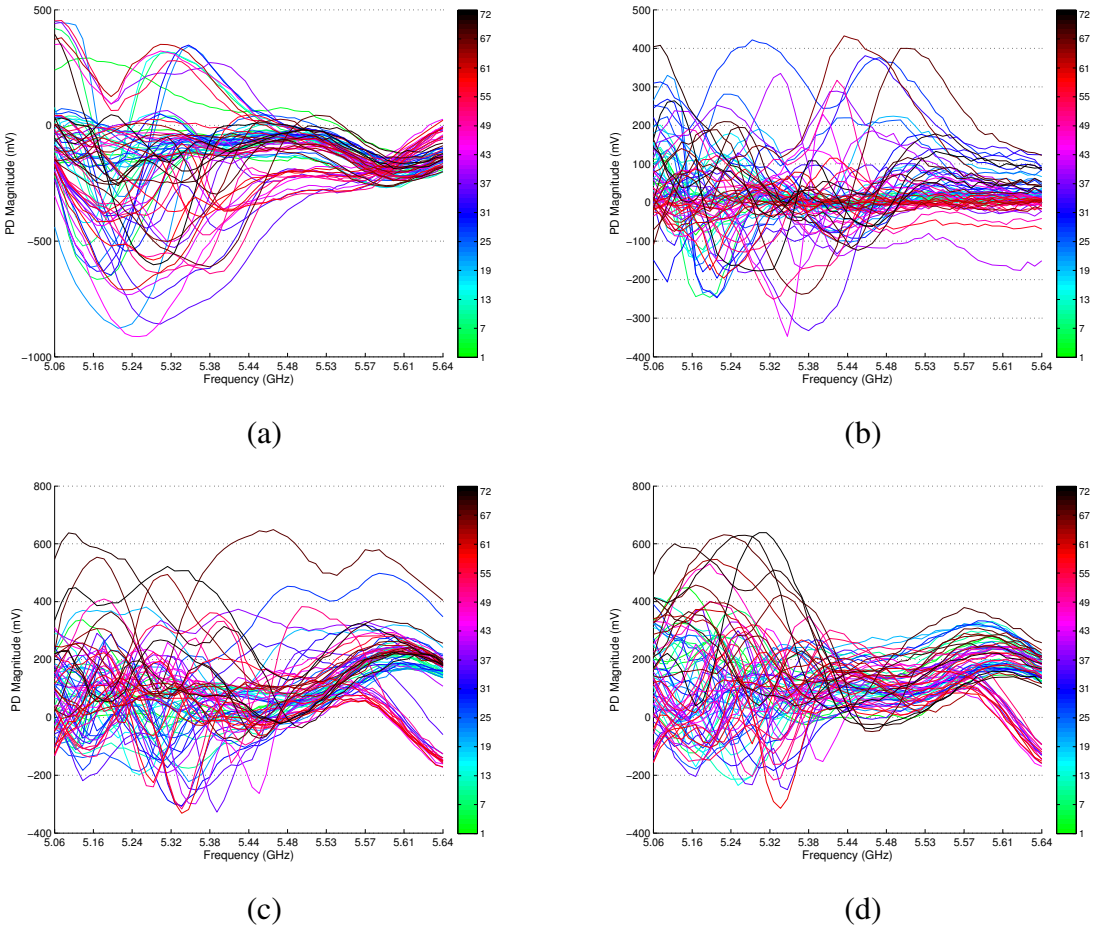
Figure 47: The *No COA* fingerprint (a) over frequency and (b) over antenna couplings.



(a) (b)

(c) (d)

Figure 48: Euclidean distance between the *No CoA* NF signature and the signatures of randomly chosen copper-based certificates (a) *2gF*, (b) *2gC*, (c) *2gJ* and (d) *3gJ*.



(a) (b)

(c) (d)

Figure 49: Euclidean distance between the *No CoA* NF signature and the signatures of randomly chosen paper-based certificates (a) *B*, (b) *C*, (c) *D* and (d) *I*.

6.2.2 NF Response as a Function of the Distance of the NF-CoA Instance From the Antenna Array

As part of the initial performance characterization that can determine particular aspects of the setup of the final application, it is essential to examine how the NF signature depends on the distance between the antenna array of the reader and the certificate instance, when the signature of the latter is being extracted.

A random NF-CoA , *3gE*, is initially inserted into the slot of the NF-CoA reader almost touching the antenna elements (as shown in Figure 44, but without the white plastic bolts). This case of shortest distance is labeled in the following figures with "just CoA". This distance is gradually increased either introducing up to two plastic bolts vertically of 2.5 mm thickness each (labeled with "bolts" and "2bolts") or by introducing on top of one bolt up to 12 plain photo paper sheets of Kodak gloss premium photo paper of 0.22 mm (8.5 mil) thickness and 5.2 cm by 5.2 cm lateral area each. These cases of different distances ranging from almost zero ("just CoA") up to approximately 6 mm are labeled as "bolt + Xε", where X is the number of intermediate layers of photo paper used with dielectric constant ϵ_r of around 3.2 [58] in the neighborhood of 5.5 GHz.

Since it would not be possible to discern the difference because of varying distance if the whole signature was provided, scattering parameter curves corresponding to four different couplings, namely B1-D1, B2-B4, D4-B4, and C3-B4, and four different frequency points, namely 5.342, 5.387, 5.410, and 5.429 GHz, with relatively high magnitude and standard deviation of NF response are shown in Figures 50 and 51, respectively.

The curves corresponding to zero distance ("just CoA") and one plastic bolt ("bolt") exhibit the most distinctive (or differentiating) behavior compared to all the rest in all eight different examples presented (either over frequency or over antenna couplings). This phenomenical abnormality, as explained in Section 3.1, should actually be attributed to the crossing of the boundary between the reactive and the radiating near-field region and. On the contrary, the trend for the rest curves is similar between them.

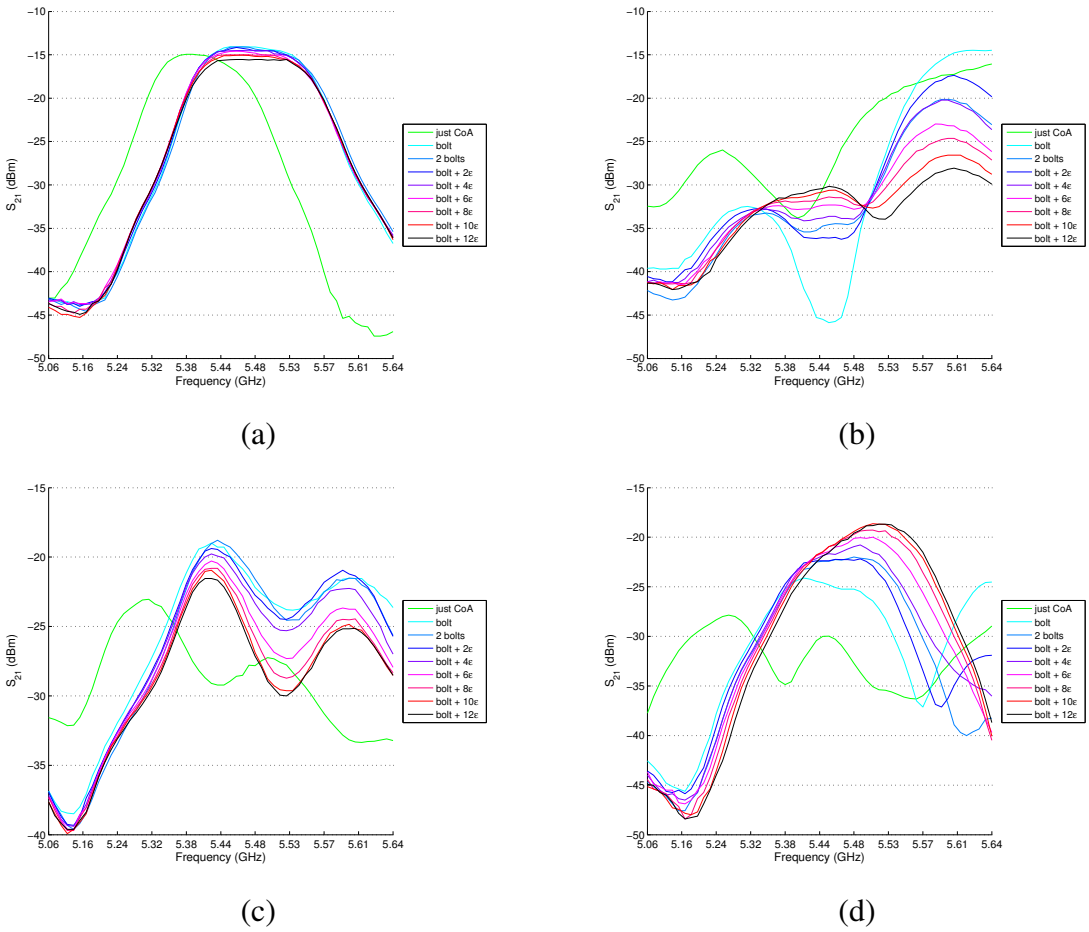


Figure 50: NF signature curves of NF-CoA *3gE* corresponding to antenna couplings (a) B1-D1, (b) B2-B4, (c) D4-B4 and (d) C3-B4 of NF-CoA *3gE* at distances ranging from almost zero ("just CoA") up to approximately 6 mm ("bolt + 12ε").

Moreover, it can be noted that as the frequency increases the dynamic range (difference between maxima and minima) increases and, thus, the difference between the responses increases and as the distance increases up to almost 4.5 mm, i.e., bolt thickness plus thickness of 12 plain photo sheets, the magnitude of the maxima of the NF responses also increases.

From the point of view of highest entropy desired, the study in this subsection leads to considering as optimum distance the one that corresponds to the thickness of one plastic bolt. This is the distance chosen for all the subsequent measurements.

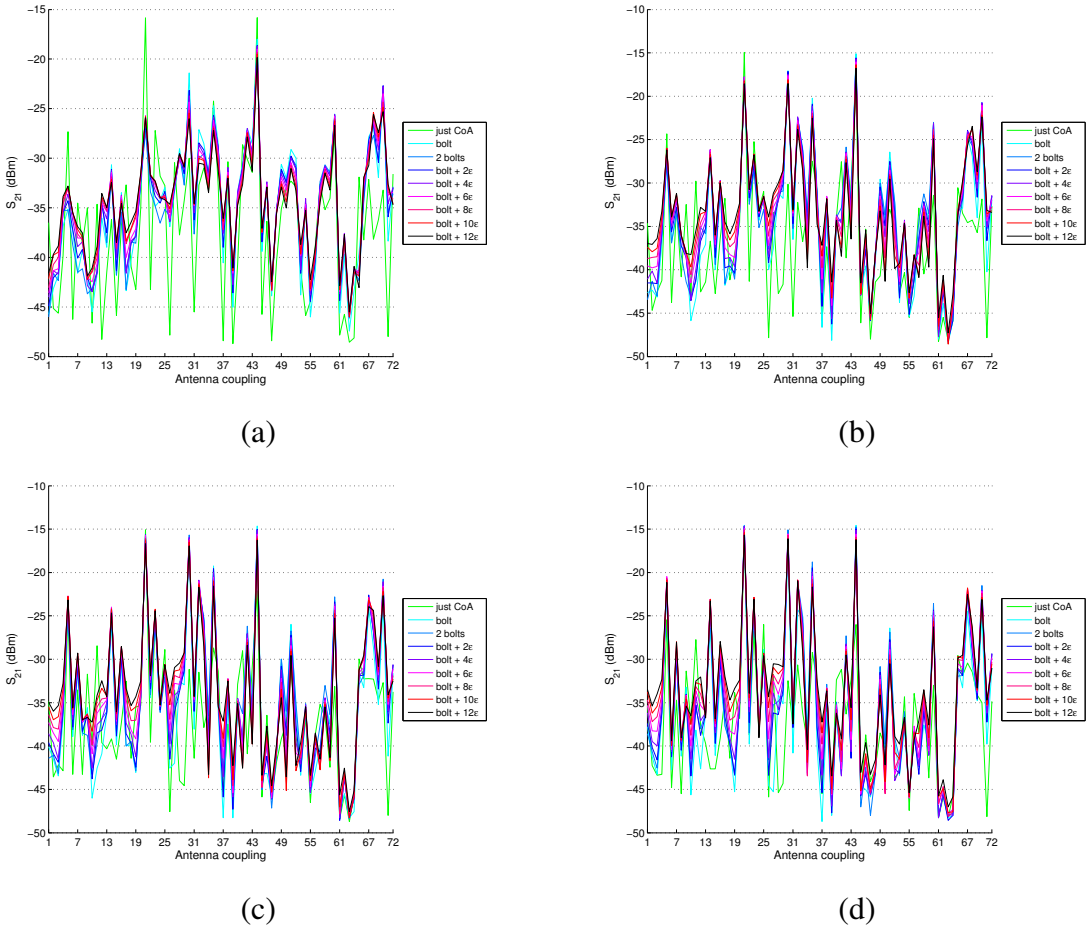


Figure 51: NF signature curves of NF-CoA *3gE* corresponding to frequency points (a) 5.3419, (b) 5.3871, (c) 5.4083 and (d) 5.4285 GHz at distances ranging from almost zero ("just CoA") up to approximately 6 mm ("bolt + 12ε").

6.2.3 NF Response as a function of the NF-CoA 2D Projection Area

As mentioned in the introduction of this section, two different sizes of copper-based NF-CoAs have been fabricated. The objective of the test of this subsection is to evaluate the difference between the NF responses of the full-sized certificates *2gI* and *2gJ* and all the rest 45 smaller-sized copper-based certificates. Additionally, it is important to verify that the entropy yielded by the smaller-sized certificates is adequate.

The fact that the small certificate instances do not cover the whole area of the antenna area and, thus, there may be particular antenna couplings not significantly disrupted creates the expectation of particular couplings to be significantly more disrupted by the full-sized instances *2gI* and *2gJ*.

To show this, all 72 couplings of the 47 different copper-based NF-CoAs available are sorted by both descending maximum magnitude and sample standard deviation. Using these two tables, couplings of the full-sized certificate *2gI* that are sorted to rank significantly higher than the same couplings of the small-sized NF-CoAs are identified and presented in Table 6. Specifically, this table shows the (for most cases single-digit) number of other copper-based small-sized CoAs, the couplings of which are not exceeded by the same couplings of full-sized *2gI* in terms of maximum magnitude and maximum sample standard deviation.

The results not only make sense, but are actually absolutely expected when the couplings of Table 6 are depicted in Figure 52 on an actual photo of the antenna array of the NF-CoA reader with an aligned semi-transparent 2D projection of an attached small-sized certificate instance; here *2gK*.

Table 6: Antenna couplings of full-sized copper-based *2gI* that significantly exceed the same couplings of all 45 small-sized CoAs, except for *X* many, in terms of maximum magnitude and maximum sample standard deviation.

Antenna Coupling	Full-sized *2gI* exceeding significantly all 45 but *X* many copper-based small-sized CoAs in terms of:	
	Maximum Magnitude of Coupling	*Maximum Sample Standard Deviation of Coupling*
B1-E2	0	0
E5-B5	2	2
E4-B5	2	2
C3-E2	3	4
A2-D1	4	2
D5-A5	4	16
C3-E1	5	1
B2-D1	5	12
A1-D2	7	7
A1-E1	7	-
E5-B4	8	4
D4-E2	10	-

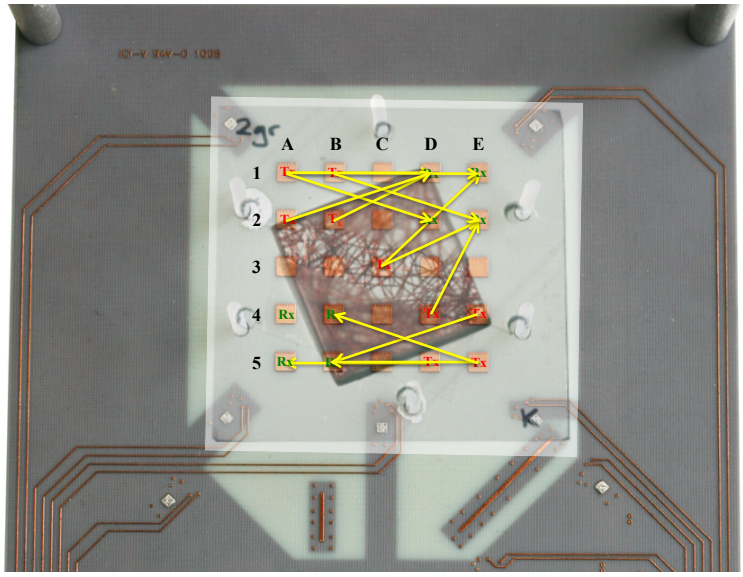


Figure 52: Antenna couplings (yellow) of full-sized copper-based *2gI* that significantly exceed the same couplings of all 45 small-sized CoAs in terms of maximum magnitude and maximum sample standard deviation.

6.2.4 Effect of the Conductive Material Density of the NF-CoAs

The next question that arises, concerning the optimal design of the NF-CoA certificates, is what is the effect of the amount of metal density in the 3D structure of the NF-CoA to the entropy of its NF frequency response. Although it would be possible to investigate this aspect with paper-based CoAs by varying the number of conductive nano-particle inkjet-printed, this option would not be very reliable as the final metal density would highly depend on how well and uniformly the instances have been cured for the percolation to be equally effective among all paper-based CoAs.

As a highly more reliable solution for this test, three different sets of copper-based CoAs of different mass per meter, namely 2, 3 and 4 grams per meter, are used. Each one of these sets includes 15 certificates of the same copper weight (excluding the two full-sized ones). No well-determined and fixed structures of different mass are used. Instead, in order to keep the test setup closer to reality and to the final application, random amount, but not considerably different, of each type of wires has been randomly mixed with dielectric fixative to create the copper-based certificate instances already presented in Section 4.1.2.

First, all Euclidean distances between all possible pairs of instances within the same group, which yields the binomial coefficient of $15!/[2! \cdot (15-2)!] = 105$ differences of NF fingerprints, are captured and presented in Figure 53 over frequency ((a), (c), and (e)) and over antenna couplings ((b), (d), and (f)). In particular, (a) and (b) correspond to the group of 2 g/m NF-CoAs, (c) and (d) correspond to the group of 3 g/m NF-CoAs, and (e) and (f) correspond to the group of 4 g/m NF-CoAs. It is noticed that the metal density does indeed affect the entropy of the frequency response and that the lighter copper-based certificates, i.e., the 2 g/m ones, yield the highest response differentiation.

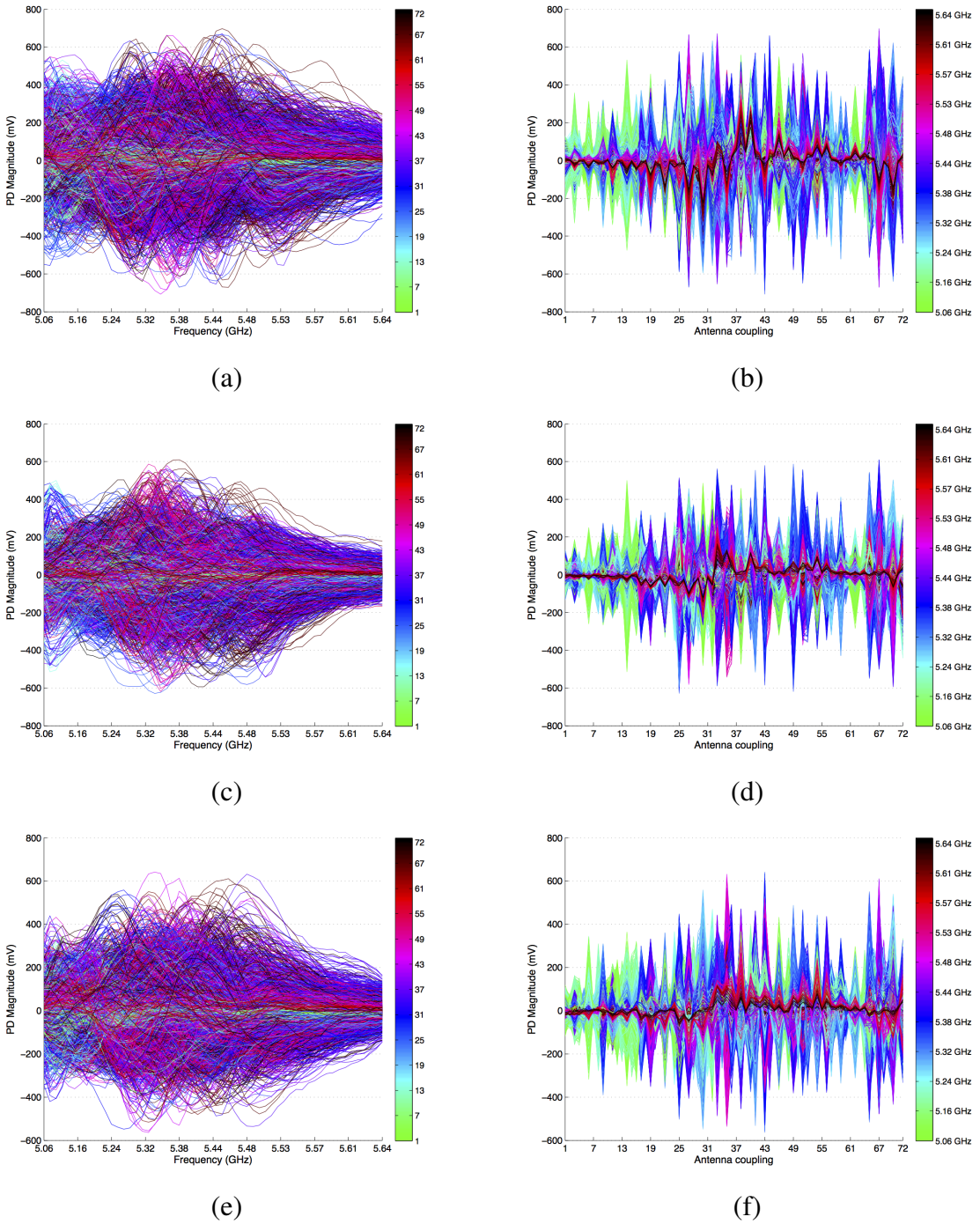
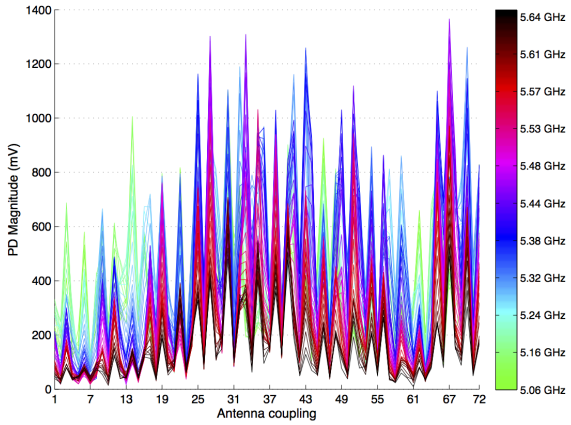
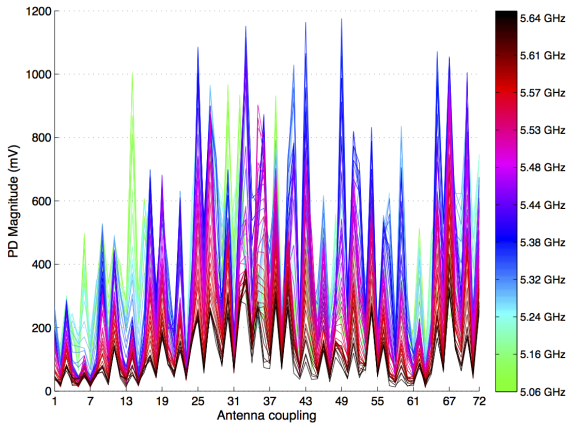


Figure 53: Euclidean distances between all possible pairs of NF-CoA signatures of (a) 2 g/m over frequency, (b) 2 g/m over antenna couplings, (c) 3 g/m over frequency, (d) 3 g/m over antenna couplings, (e) 4 g/m over frequency, and (f) 4 g/m over antenna couplings.

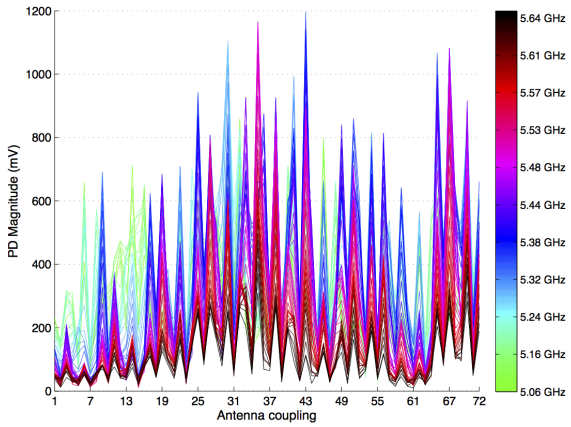
For a clearer assessment, additionally the range, i.e., difference between the maximum and the minimum of each sample, and the interquartile range (IQR) of statistical dispersion, i.e., difference between the 75^{th} and the 25^{th} percentiles of the sample are evaluated based on the data of Figure 53 and are presented in Figures 54 and 55, respectively. In both Figures, subfigure (a) corresponds to the group of 2 g/m NF-CoAs, subfigure (b) corresponds to the group of 3 g/m NF-CoAs, and subfigure (c) corresponds to the group of 4 g/m NF-CoAs. In a consistent manner across both the range and the interquartile range, it is noticed that the lighter 2 g/m instances exhibit the highest entropy and the heavier 4 g/m ones yield the lowest entropy.



(a)

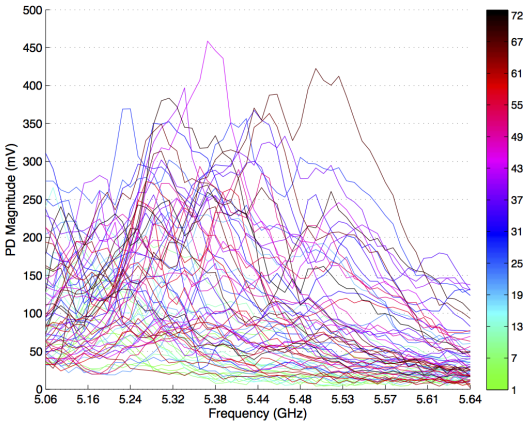


(b)

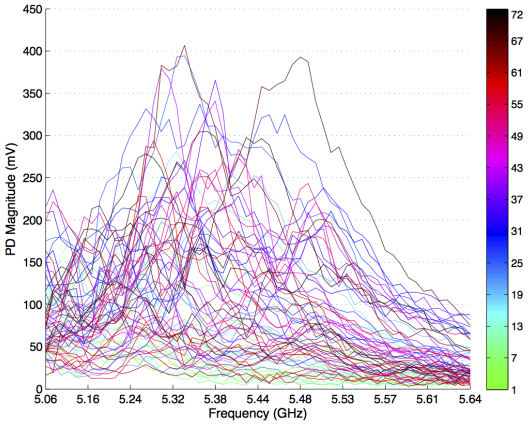


(c)

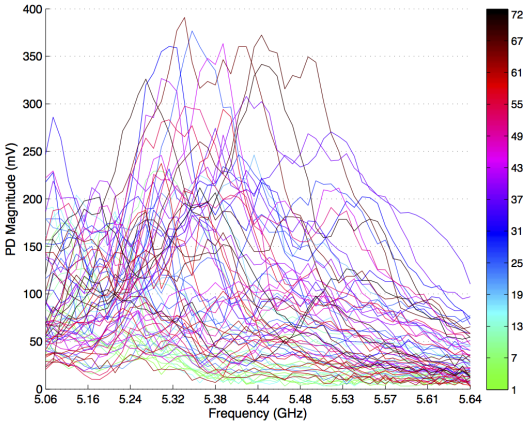
Figure 54: Range of Euclidean distances of all possible pairs of NF-CoA signatures of (a) 2 g/m, (b) 3 g/m, and (c) 4 g/m over antenna couplings.



(a)



(b)



(c)

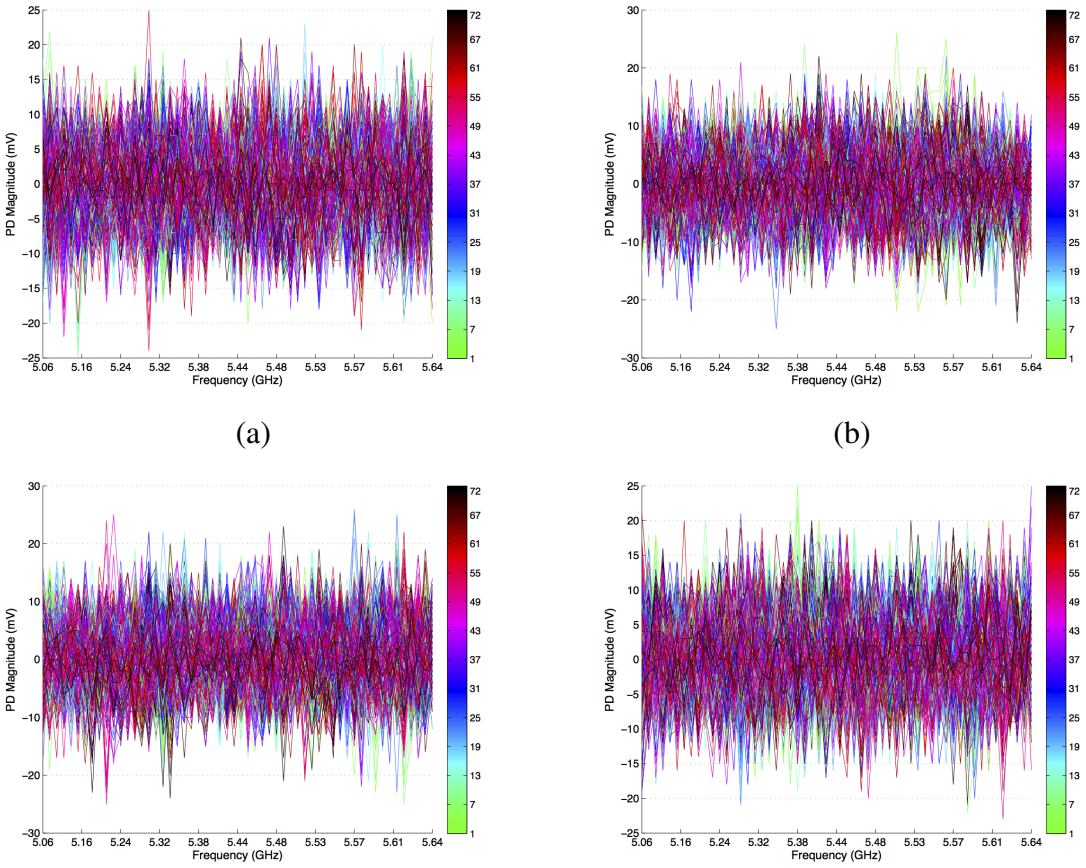
Figure 55: Interquartile range of Euclidean distances of all possible pairs of NF-CoA signatures of (a) 2 g/m, (b) 3 g/m, and (c) 4 g/m over frequency.

6.2.5 Intra-CoA Robustness

The most important and sine-qua-non property that the NF-CoA system has to possess is the intra-CoA robustness. With this property it is ensured that always nearly exact replicate signatures are extracted from the same certificate instance by the NF-CoA reader.

The test procedure here is very simple and conducted as follows: a single certificate instance is placed on the reader, its NF signature is extracted, then the instance is taken off and then placed back on the reader to extract again its signature. This is repeated a number of times to indicate any changes in measurement results. Specifically, the full-sized copper-based instance *2gI* and three random small-sized instances, *2gE*, *3gE* and *4gC*, are chosen for this test and measured five times each. The Euclidean distance between all $5!/[2! \cdot (5-2)!] = 10$ possible pairs of the five repeatedly extracted signatures of each certificate instance are shown in Figure 56 over frequency. The reason there is no apparent difference in the trends between the graphs over frequency and over antenna couplings is that in both cases the differences look like noise. Actually the differences almost are noise since the maximum difference at any combination of frequency point and antenna coupling does not exceed 30 mV.

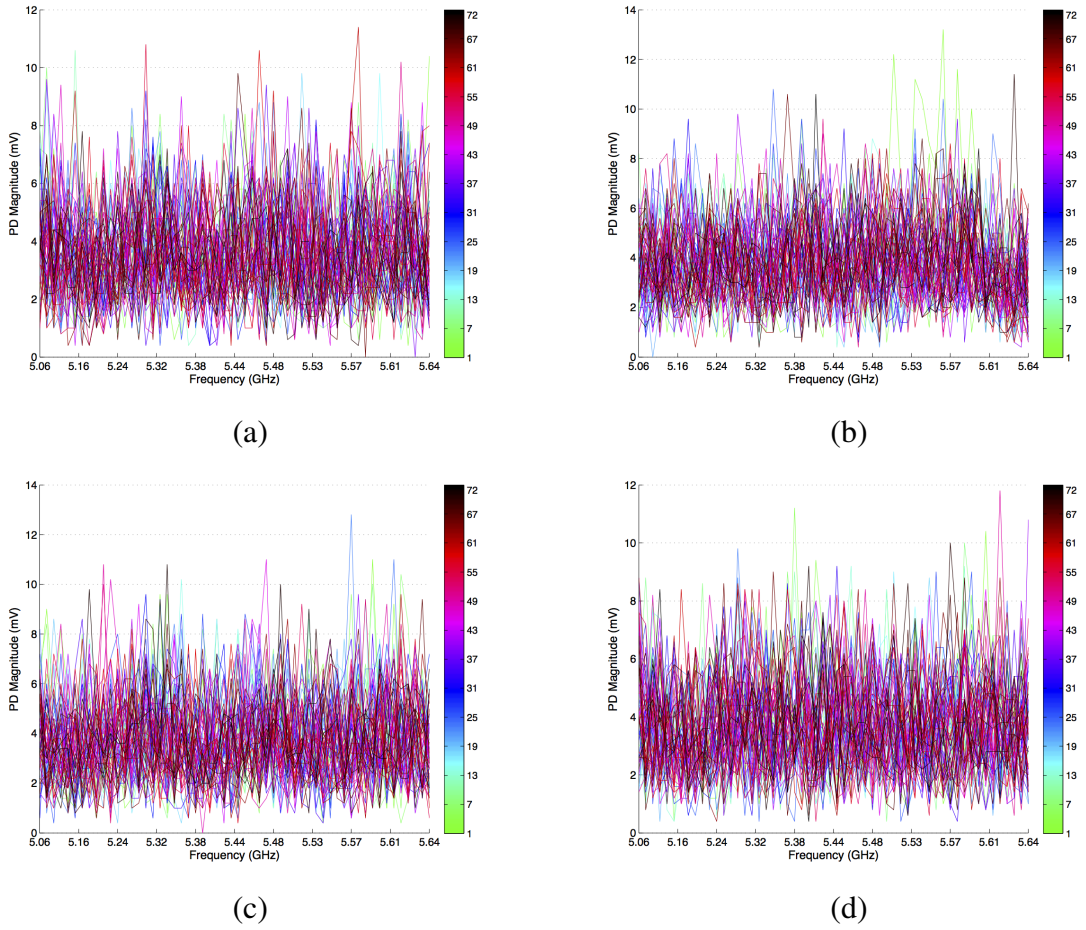
For a more complete assessment of how small the intra-CoA differences/distances are, the mean and the sample standard deviation of the differences of Figure 56 are presented in Figures 57 and 58, respectively. Regardless of at which part of the logarithmic power range of the power detector these Euclidean distances are measured, the distances for the randomly chosen four different certificate instances never exceed 13 mV of PD magnitude for any combination of frequency point and antenna coupling and the vast majority of the measurements has a value below 8 mV. If one considers that the overall dynamic range of the power detector is approximately 180 mV to 1400 mV (see Section 5.2.3 and [75]), it can be safely concluded that the differences are located in the neighborhood of the noise floor of the PD and/or the ADC of the MCU and that indeed nearly identical signatures are finally extracted.



(a) (b)

(c) (d)

Figure 56: Euclidean distance between all 10 possible pairs of the five times (repeatedly) extracted signatures of certificate instances (a) *2gE*, (b) *3gE*, (c) *4gC* and (d) full-sized *2gI*.



(a) (b)

(c) (d)

Figure 57: Mean of Euclidean distance between all 10 possible pairs of the five times (repeatedly) extracted signatures of copper-based certificate instances (a) *2gE*, (b) *3gE*, (c) *4gC* and (d) full-sized *2gI*.

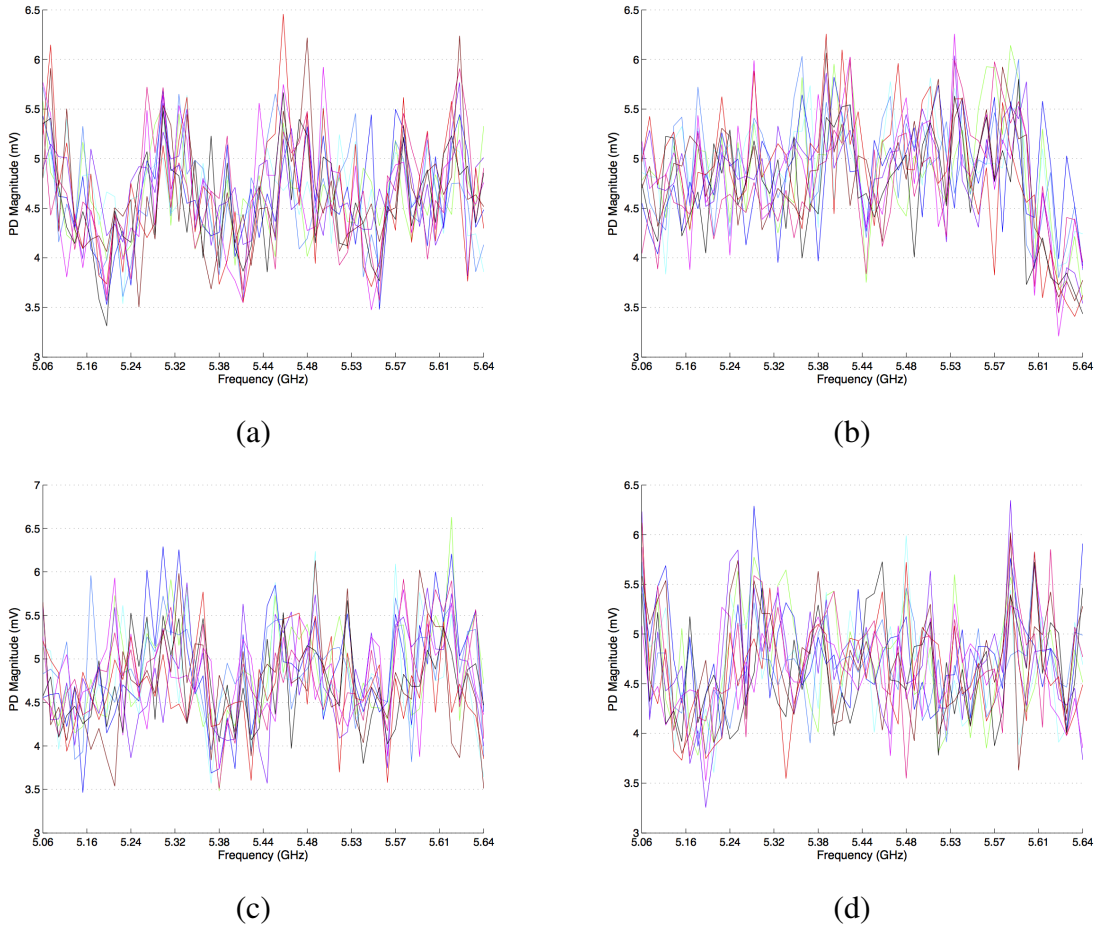


Figure 58: Standard deviation of Euclidean distance between all 10 possible pairs of the five times (repeatedly) extracted signatures of copper-based certificate instances (a) *2gE*, (b) *3gE*, (c) *4gC* and (d) full-sized *2gI*.

Visual examples of the worst case scenarios, i.e., highest magnitude and highest standard deviation of difference, of extraction of individual curves of these signatures, over frequency and over antenna couplings, are shown in Figure 59.

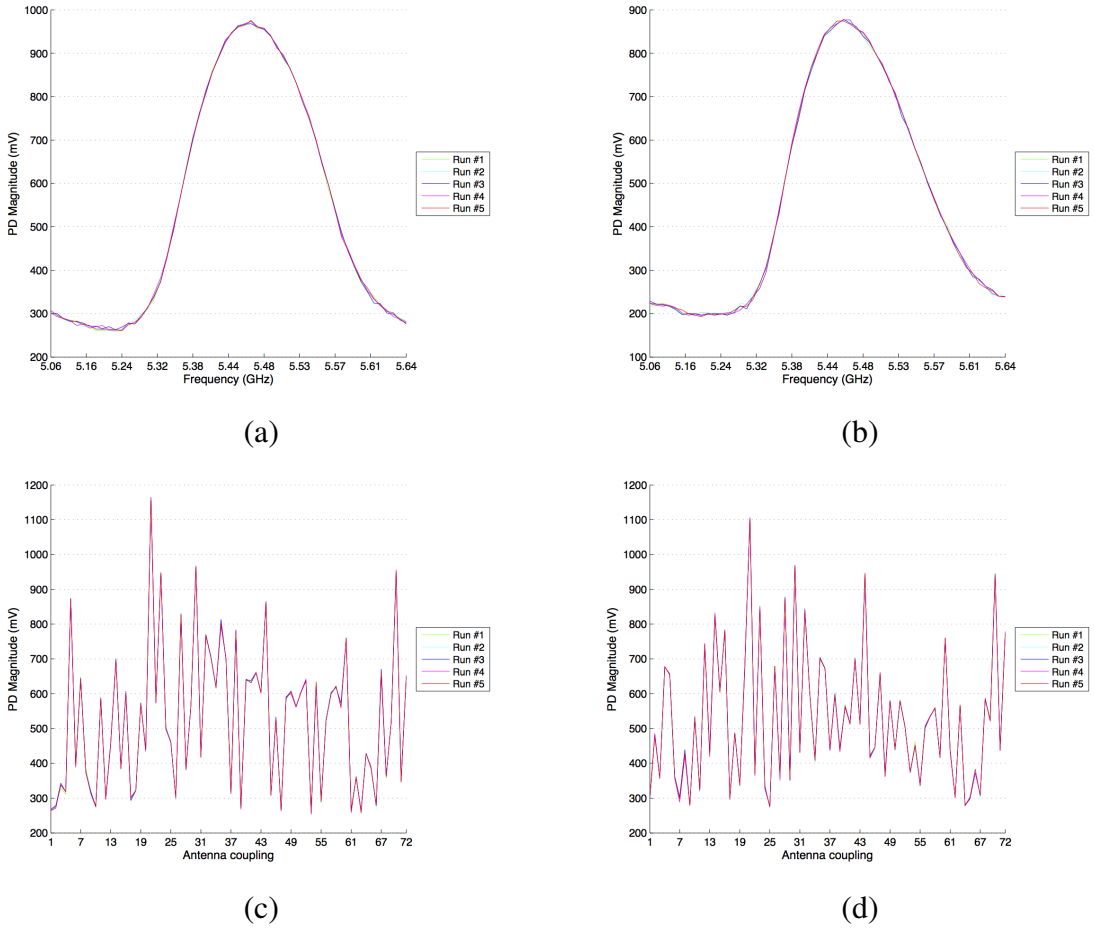


Figure 59: Visual examples of the worst case scenarios (highest magnitude and highest standard deviation of difference) of extraction of individual curves: (a) B1-E1 of *2gE* over frequency, (b) A1-D1 of *3gE* over frequency, (c) D4-D2 of *2gE* over antenna couplings, and, (d) D4-E2 of *2gI* over antenna couplings.

Similarly to the copper-based scenario, two random paper-based instances, C and H, are tested for intra-CoA robustness by extracting their instances consecutively for 10 times. The Euclidean distances between all $10!/[2! \cdot (10-2)!] = 45$ possible pairs of the five repeatedly extracted signatures of each certificate instance are shown in Figure 60. In particular, (a) and (b) correspond to the mean and standard deviation, respectively, of intra-CoA

Euclidean distances of instance *C* and (c) and (d) correspond to the mean and standard deviation, respectively, of intra-CoA Euclidean distances of instance *H*. However, as opposed to the above case of copper-based instances, in the paper-based based scenario the graphs over the antenna couplings are presented, since only with this type of graphs the major reason for the increased Euclidean distance among the paper-based instance compared to the copper-based ones can be highlighted; mean values of differences larger than 14 mV are only noticed for few particular frequencies that belong to the lower half of the spectrum. Of course, additional reasons for the increased differences are the flexibility of paper and the increased rotational displacement due to the wear-and-tear of the plastic pole holes on the paper.

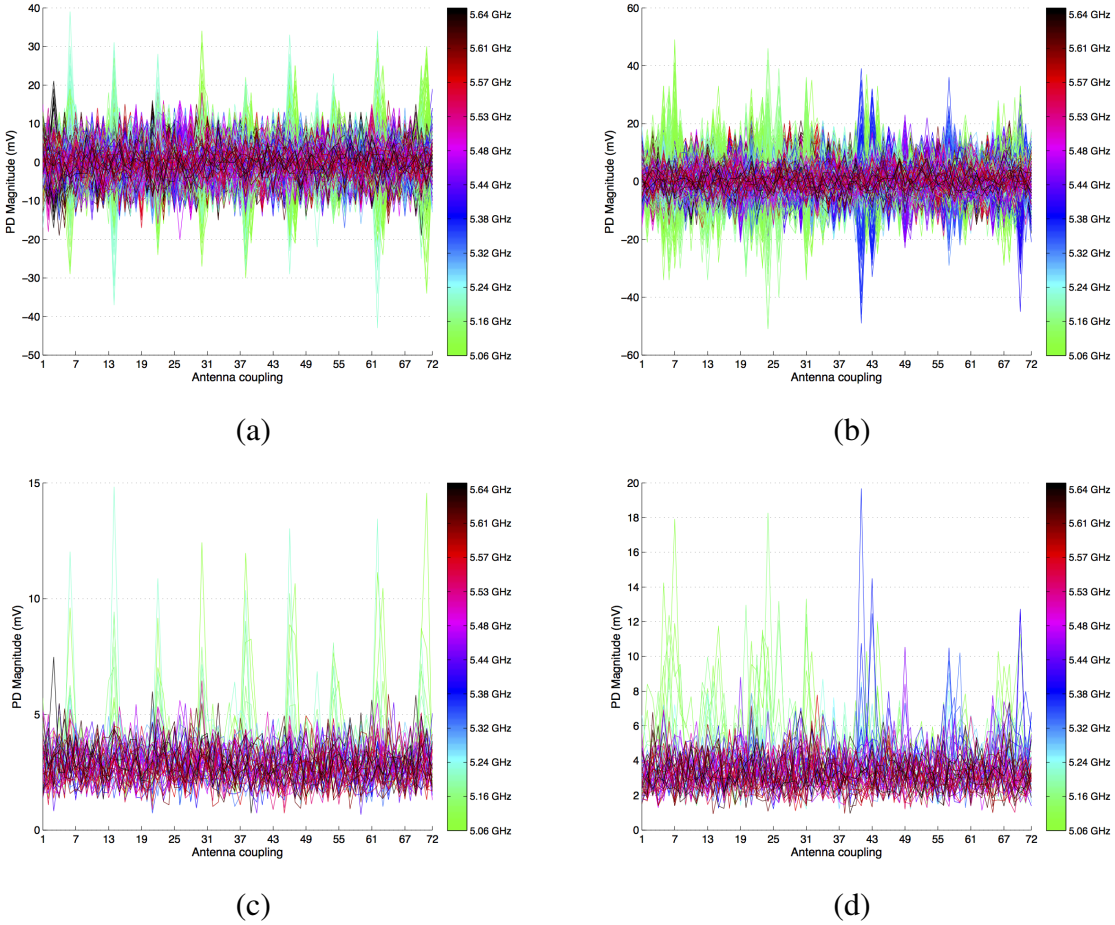


Figure 60: Euclidean distance between all 45 possible pairs of the 10 times (repeatedly) extracted signatures of paper-based certificate instances (a) *C*, (b) *H*. Mean of Euclidean distance between all 45 possible pairs of the five repeatedly extracted signatures of paper-based certificate instances (c) *C*, (d) *H*.

Visual examples of the worst case scenarios, i.e., highest magnitude and highest standard deviation of difference, of extraction of individual curves of the paper-based signatures, over frequency and over antenna couplings, are also shown in Figure 61.

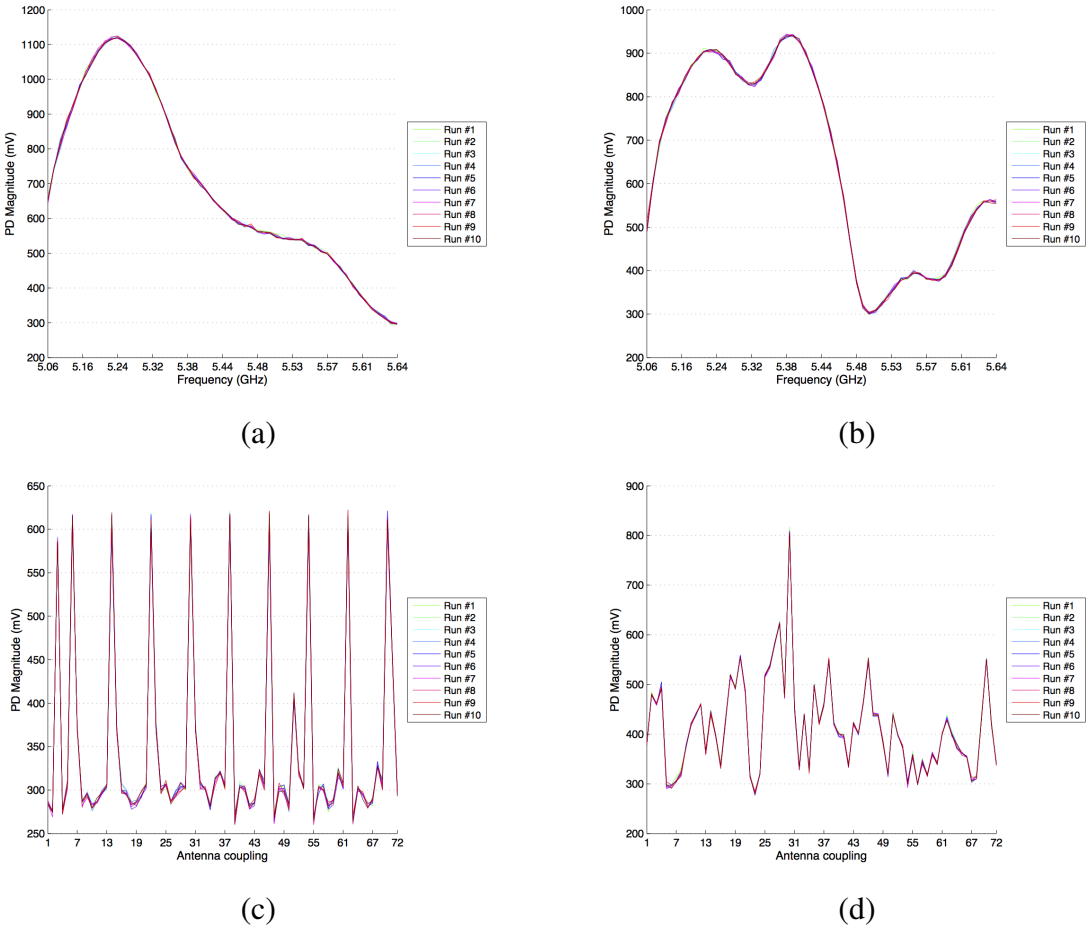


Figure 61: Visual examples of the worst case scenarios (highest magnitude and highest standard deviation of difference) of extraction of individual curves: (a) D5-B5 of H over frequency, (b) C3-B4 of H over frequency, (c) A2-E2 of C over antenna couplings, and (d) A1-E2 of H over antenna couplings.

6.2.5.1 *Determining the Similarity Detection Threshold* δ_T

Let an NF-CoA reader extract two NF signatures f and f', such that both signatures are a cardinality-N real vector of numbers $\in \mathbb{R}^N$. The reader decides that both belong to the same physical certificate instance, i.e, have been extracted by the same physical certificate instance, if $\|f_{ij} - f'_{ij}\| < \delta_T$, where the *similarity detection threshold* δ_T is a standardized distance metric $\| \cdot \|$, such as the Euclidean distance, between f and f'

The results provided in the preceding intra-CoA robustness study can lead to the reckoning of δ_T. Essential toward this goal is the knowledge that the slope of the output voltage over input RF power of the power detector [75] of the reader is 31 mV/dB, as analyzed in Section 5.2.3 and shown in Figure 35. This information combined with the sub 30 mV Euclidean difference across all antenna couplings of an NF signature for all frequencies including both copper- and paper-based certificate instance, leads to the conclusion that the maximum similarity detection threshold is bound by 1 dB or

$$|\delta_T| \leqslant 1 \text{ dB} \tag{8}$$

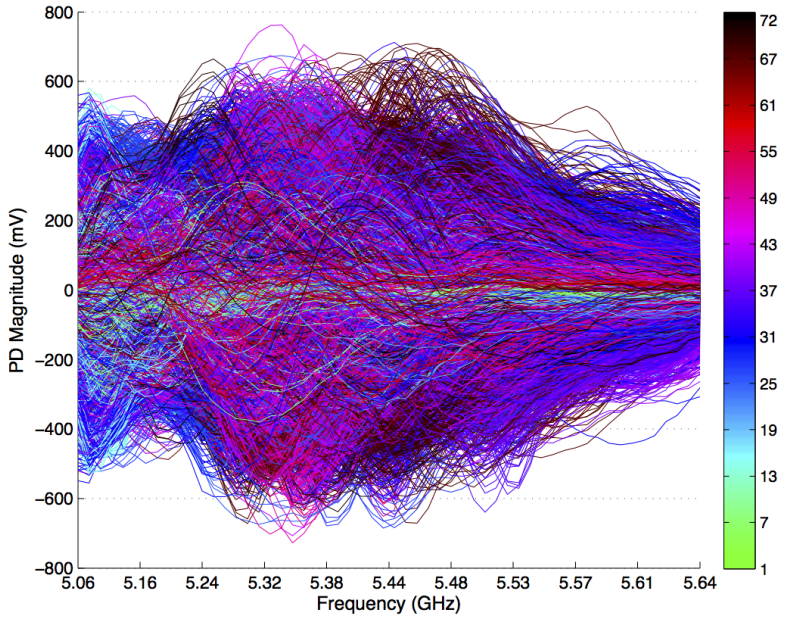
This level of accuracy takes on even higher importance if one considers that the linearity error exhibited by the power detector [75] used is ±1 dB. In other words, the maximum intra-CoA difference measured approaches the physical detection limit of the underlying hardware.

6.2.6 Inter-CoA Robustness

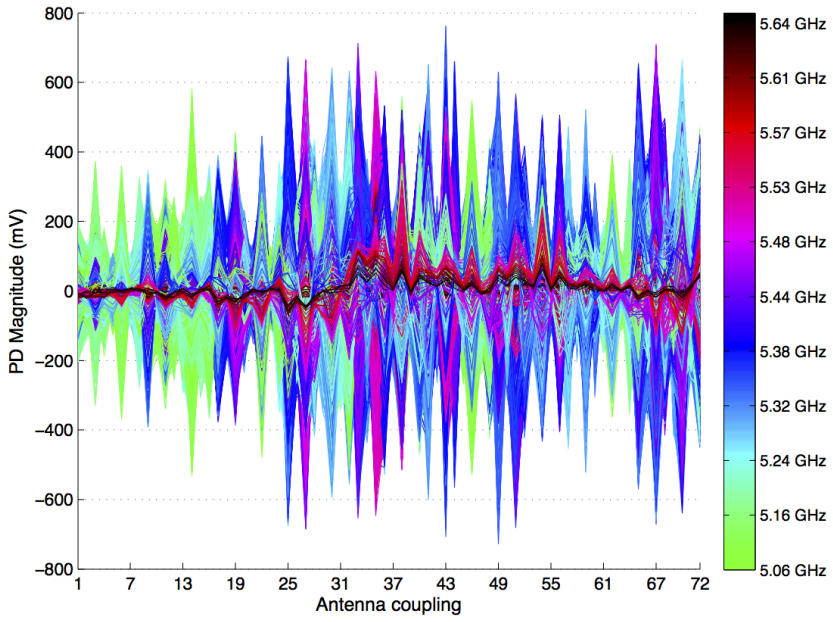
Inter-CoA robustness, i.e., the uniqueness among the signatures extracted from different NF-CoA instances, is also a sine-qua-non property that the NF-CoA system is required to have. Without this property, false-positive decisions, with which counterfeit instances are accepted as authentic, can be made by the NF-CoA reader.

For this test, the signatures of all fabricated copper-based NF-CoAs are compared to each other. As described in Section 4.1.2, this set of available fabricated copper-based instance includes 45 small-sized ones belonging to all three types of different mass per meter, namely 2 g/m, 3 g/m and 4 g/m, as well as the two full-sized, *2gI* and *2gJ*. Specifically, first the Euclidean distance between all $47!/[2! \cdot (47-2)!] = 1081$ possible pairs of extracted signatures of different certificate instance are measured and shown in Figure 62 both (a) over frequency and (b) over antenna couplings.

Because of the density of the curves of the 1081 different sets of Euclidean distances among different certificate instances, an estimation of the range of these differences is needed for a clearer assessment of how large the intra-CoA differences/distances are. The range, i.e., difference between the maximum and the minimum of each sample, and the interquartile range, i.e., difference between the 75^{th} and the 25^{th} percentiles of each sample, are evaluated based on the data of Figure 62 and are presented in Figure 63. The conclusion that can be drawn by analyzing these plots is that the differences among all the available signatures is significantly high. The range, especially around the the resonant frequency of the antenna elements and also for many antenna couplings, almost reaches the dynamic range of the power detector of the NF-CoA reader with values close to 1500 mV. As a more reliable measure of statistical dispersion, the interquartile range or *range of middle fifty* verifies the inter-CoA robustness for almost all combinations of antenna couplings and frequency points, at which the difference exceeds the intra-CoA rough threshold of 35 mV (see previous subsection).

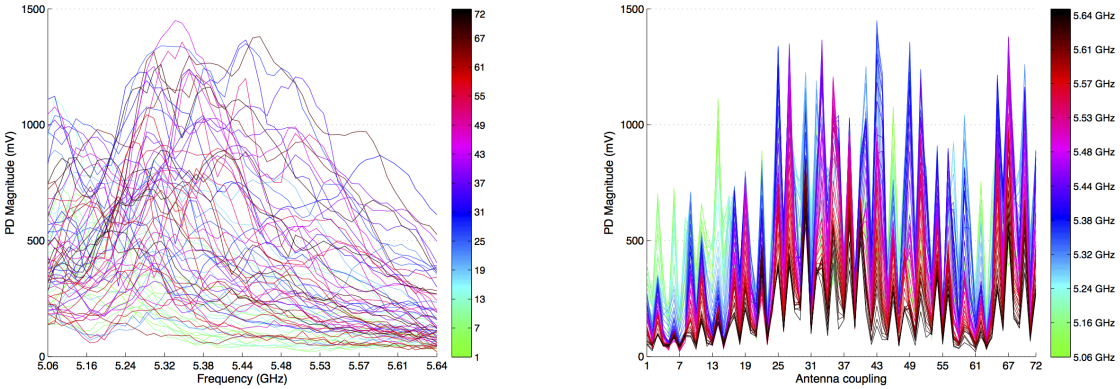


(a)



(b)

Figure 62: Euclidean distance between all 1081 possible pairs of extracted signatures of copper-based certificate instances (a) over frequency and (b) over antenna couplings.



(a) (b)

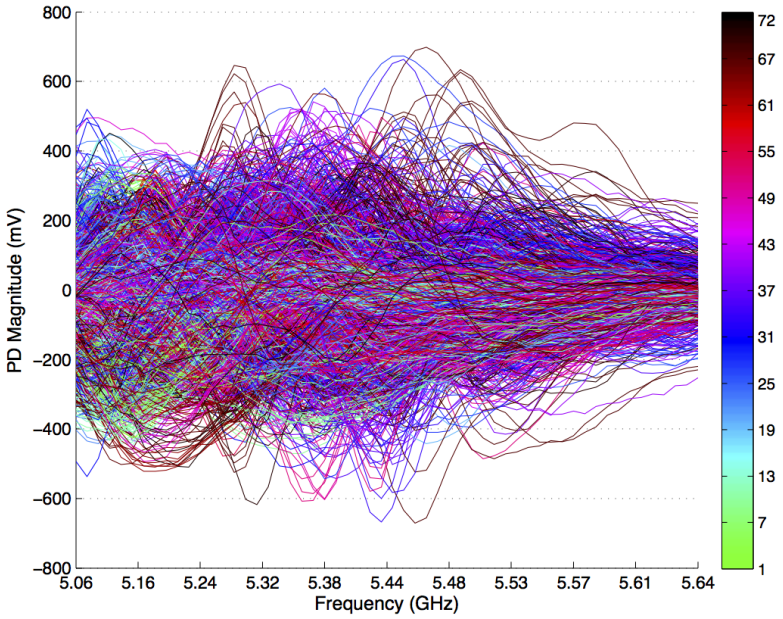
(c) (d)

Figure 63: Range of Euclidean distances between all 1081 possible pairs of extracted signatures of copper-based certificate instances (a) over frequency and (b) over antenna couplings. Interquartile range of Euclidean distances of all 1081 possible pairs of extracted signatures of copper-based certificate instances (c) over frequency and (d) over antenna couplings.

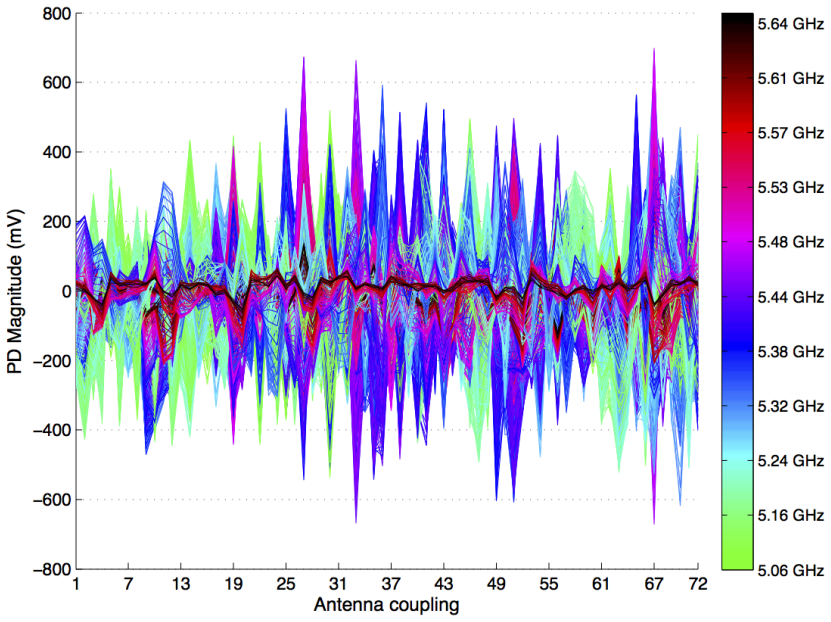
Similarly to the copper-based scenario, all 10 paper-based instances, A to J, are tested for inter-CoA robustness by comparing their instances. The Euclidean distances between all $10!/[2! \cdot (10-2)!] = 45$ possible pairs of the extracted signatures of different certificate instance are measured and shown in Figure 64 both (a) over frequency and (b) over antenna couplings. The convergence that can be noted at the very far high end of the frequency range is attributed entirely to the low resonant frequency of the antenna elements, presented in Section 5.2.1.

An estimation of the range of these differences is also provided in the paper-based case for a clearer assessment of how large the intra-CoA differences/distances are. The range, i.e., difference between the maximum and the minimum of each sample, and the interquartile range, i.e., difference between the 75^{th} and the 25^{th} percentiles of each sample, are evaluated based on the data of Figure 64 and are presented in Figure 65. The conclusion that can be drawn by analyzing these plots is that the differences among all the available signatures is, equally with the previous case of copper-based certificate instances, remarkably high. The range, especially around the resonant frequency of the antenna elements and also for many antenna couplings, almost comes close to the dynamic range of the power detector of the NF-CoA reader with values close to 1400 mV. As a more reliable measure of statistical dispersion, the interquartile range verifies the inter-CoA robustness for almost all combinations of antenna couplings and frequency points.

Of course, it comes as no surprise that the results of Chapter 7 corroborate the strong belief that, for a single scan, 72 couplings provide enough data to ensure uniqueness between CoAs.



(a)



(b)

Figure 64: Euclidean distance between all 1081 possible pairs of extracted signatures of paper-based certificate instances (a) over frequency and (b) over antenna couplings.

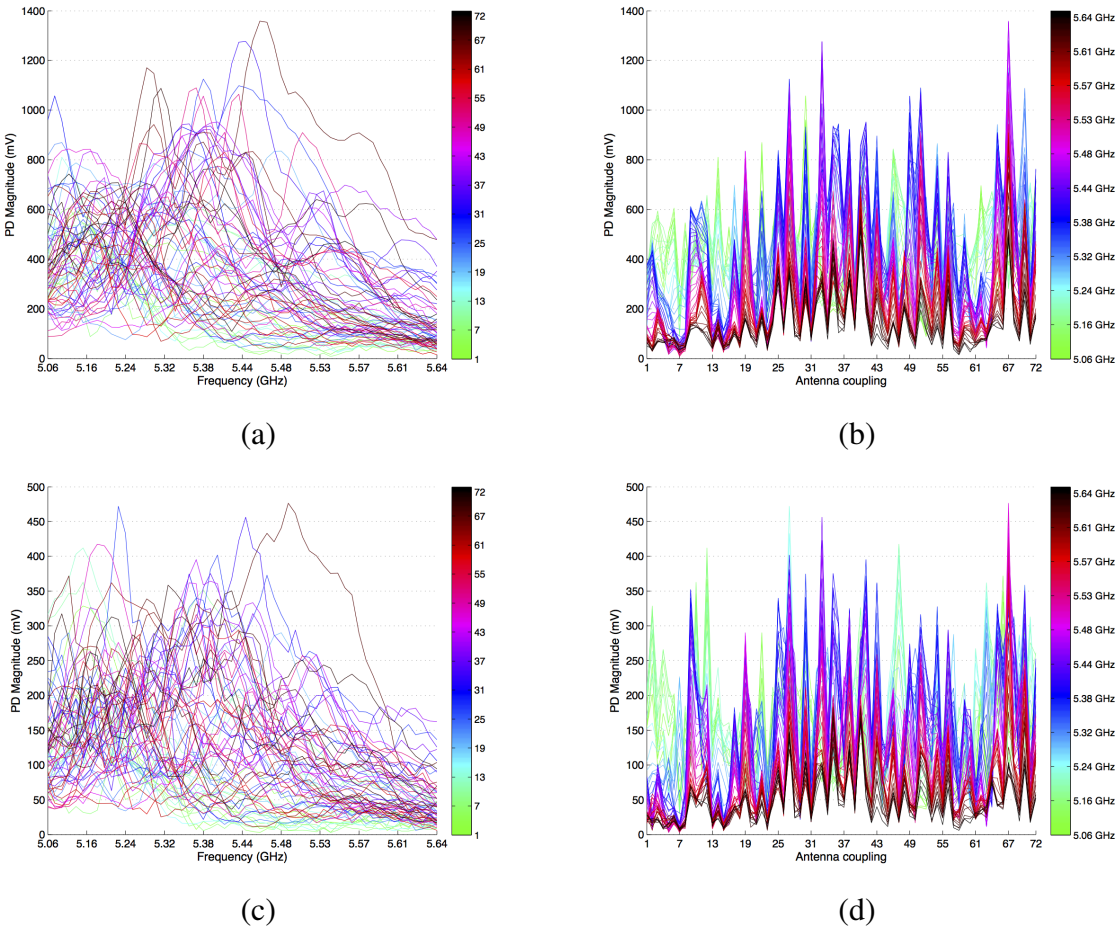


Figure 65: Range of Euclidean distances between all 45 possible pairs of extracted signatures of paper-based certificate instances (a) over frequency and (b) over antenna couplings. Interquartile range of Euclidean distances of all 45 possible pairs of extracted signatures of copper-based certificate instances (c) over frequency and (d) over antenna couplings.

6.2.7 Shielding Against Interference

As far as the applicability of the proposed anti-counterfeiting solution is concerned, it is highly desired that the NF-CoA system can operate without any problems and still yield high entropy of extracted signatures even when large conductive objects and surfaces exist in close proximity to the actual certificate instances. Actually, these kinds of environments, where shielding of the NF-CoA operation against interference from nearby conductive and dielectric material is required, are expected; for instance, when NF-CoAs are attached on computer laptops, aircraft spare parts, pharmaceutical liquids, etc.

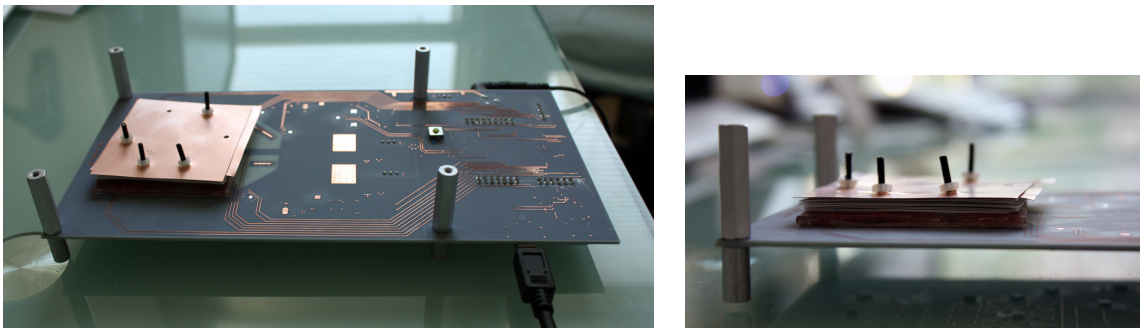
Toward assessing the shielding capability of the NF-CoA system against interference, three different tests are conducted that involve the proximity of three different types or sizes of metallic surfaces brought close enough to the certificate instances. The test procedure is the same for all three tests: the full-sized copper-based CoA *2gI* and a random small-sized one, *2gB*, are initially inserted into the slot of the NF-CoA reader. This case is labeled in the following figures with "just CoA." Afterward, two 5.2 cm by 5.2 cm plain photo paper sheets of Kodak gloss premium photo paper of 0.216 mm (8.5 mil) thickness each and the metallic surface under test are stacked on top of the NF-CoA. The distance of the metallic surface from the NF-CoA is finally being varied by introducing up to 12 photo paper sheets in-between (labeled with numbers ranging from "2ε" to "12ε").

The trend of the NF signatures extracted when the NF-CoA is in close proximity to metallic objects does not necessarily have to be very similar to the "just CoA" case. Nevertheless, the former signatures need to exhibit high enough entropy and consistency (i.e. not being averaged out). The couplings presented in the following tests are not randomly chosen; rather, they represent the cases of highest magnitude and standard deviation of NF fingerprints.

6.2.7.1 NF-CoA-sized Copper Surface

Three 5.5 cm by 6 cm laminated sheets of copper, liquid crystal polymer (LCP) and copper again, serve in this test as the copper surface that is stacked on top of a full- and small-sized

NF-CoA at different distances. The laminated sheets are attached as shown in Figure 66. As can be discerned in the cross-section view of Figure 66b, there is almost no distance between the NF-CoA and the antenna array. The rationale behind this decision has been to be able to compare this shielding behavior with the case of a distance equal to the thickness of a plastic bolt (as in Section), which is examined in the next subsection.



(a) (b)

Figure 66: (a) Top side view and (b) cross-sectional view of a laminated copper sheets with a size similar to that of NF-CoAs when stacked (at different distances) on top of a certificate instance attached to the NF-CoA reader.

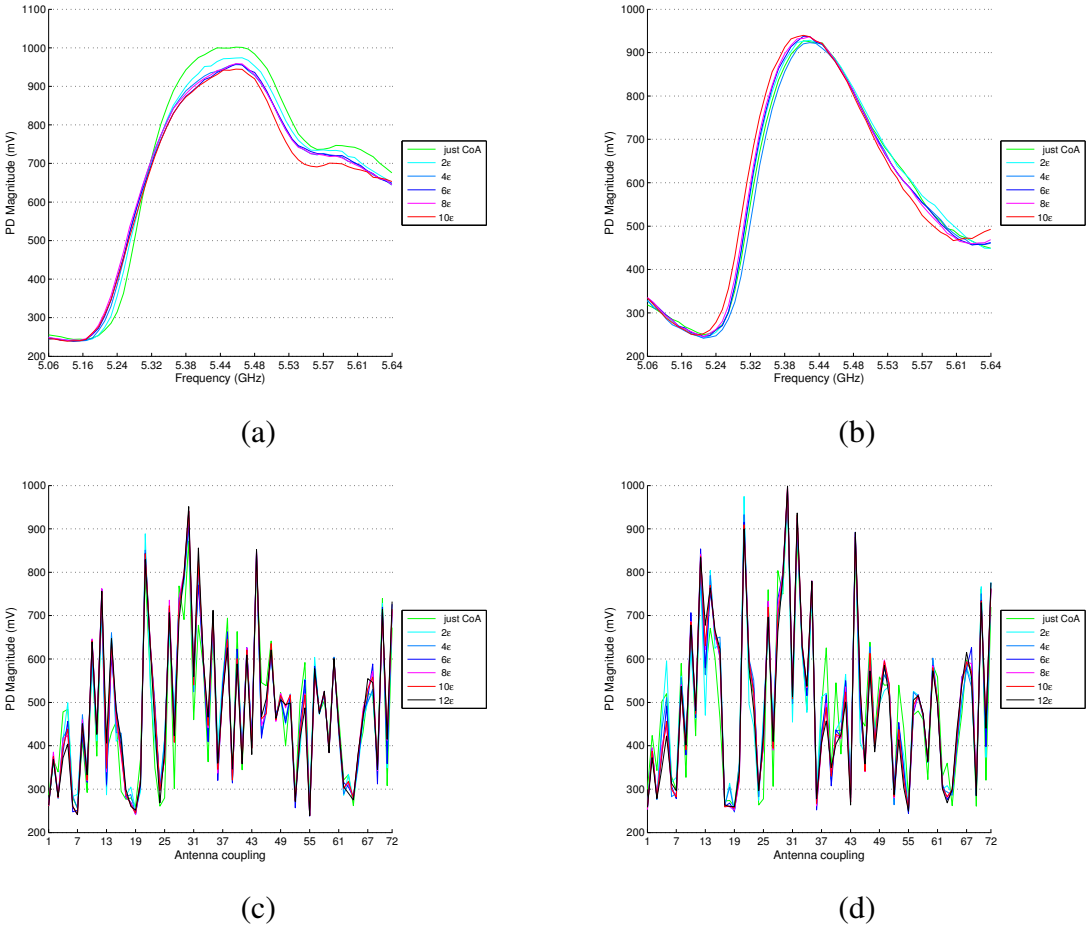


Figure 67: NF signature curves of full-sized copper-based NF-CoA *2gI* corresponding to: (a) antenna coupling B1-D1, (b) antenna coupling B2-E2, (c) frequency point 5.305 GHz, and (d) frequency point 5.349 GHz without ("just CoA") and with laminated copper sheets stacked on top of the NF-CoA at distances up to 3.5 mm ("12ε").

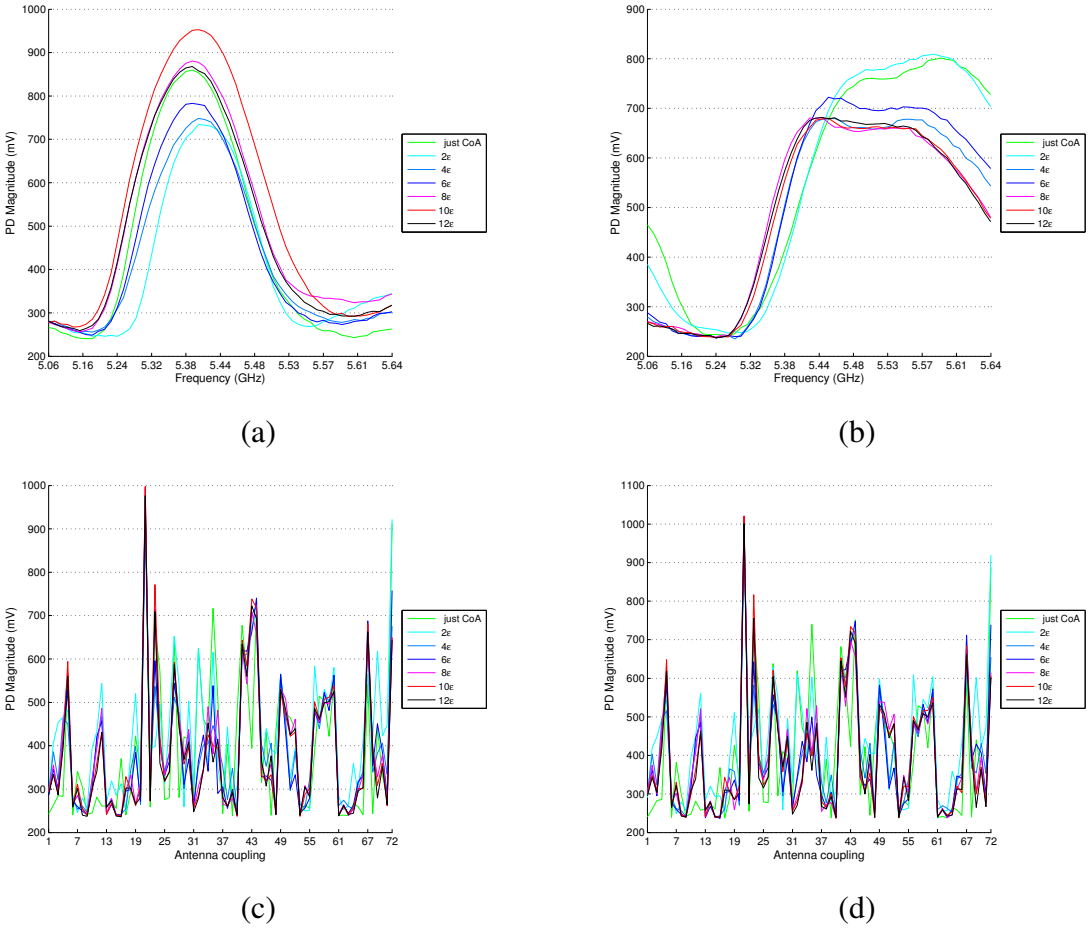


Figure 68: NF signature curves of small-sized copper-based NF-CoA *2gB* corresponding to: (a) antenna coupling B1-E1, (b) antenna coupling E4-D2, (c) frequency point 5.256 GHz, and (d) frequency point 5.269 GHz without ("just CoA") and with laminated copper sheets stacked on top of the NF-CoA at distances up to 3.5 mm ("12ε").

Within the framework of the same test, a good opportunity arises to verify the interference blocking capability of the NF-CoA system against the proximity of third conductive material, such as in this example two different keys as shown in Figure 69. Very simply the NF signatures extracted before and after placing the keys on the copper surface are compared. Of course, the copper surface serves as a shield against any third object and this is reflected in Figures 70 and 71 for the two different keys. The lack of differentiation is effectively represented by the numerical difference between the signatures being even slightly lower than the difference noticed in the intra-CoA tests of Section 6.2.5.

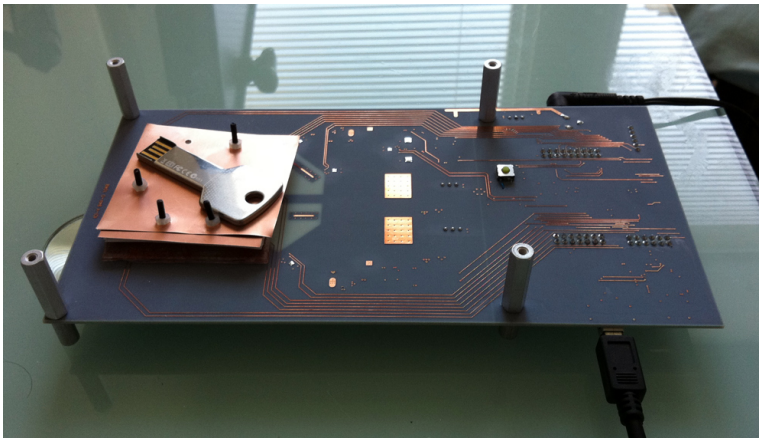
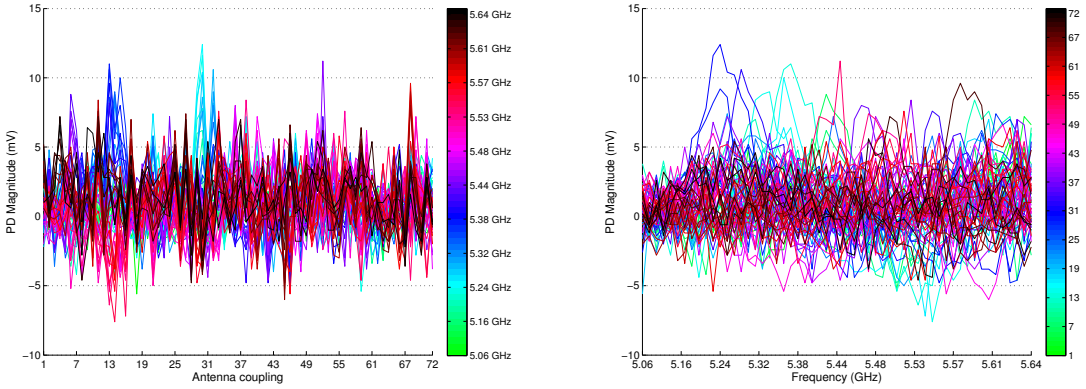
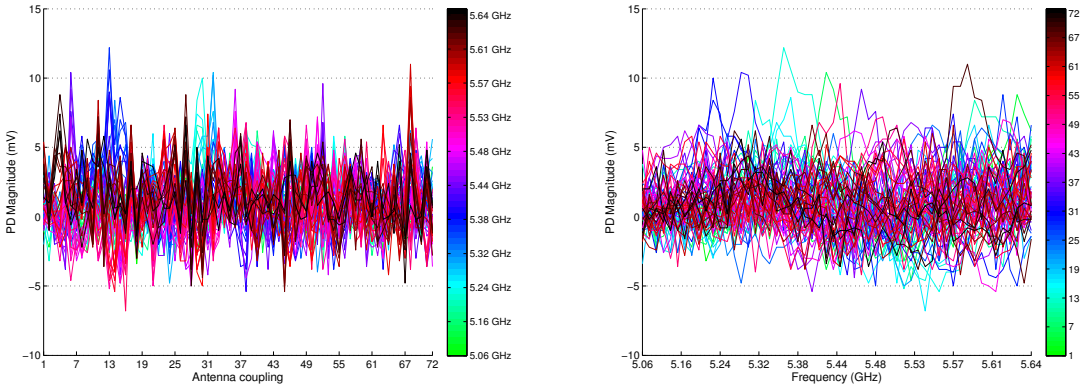


Figure 69: Test setup to verify the interference blocking capability of the NF-CoA system against the proximity of third conductive material, such as, in this example, a metallic key.



(a) (b)

Figure 70: Euclidean distance of NF signatures of the same certificate instance (a) over antenna couplings and (b) over frequency before and after placing an interfering metallic object, i.e., "key1," on top of the shielding copper surface, as shown in Figure 69.

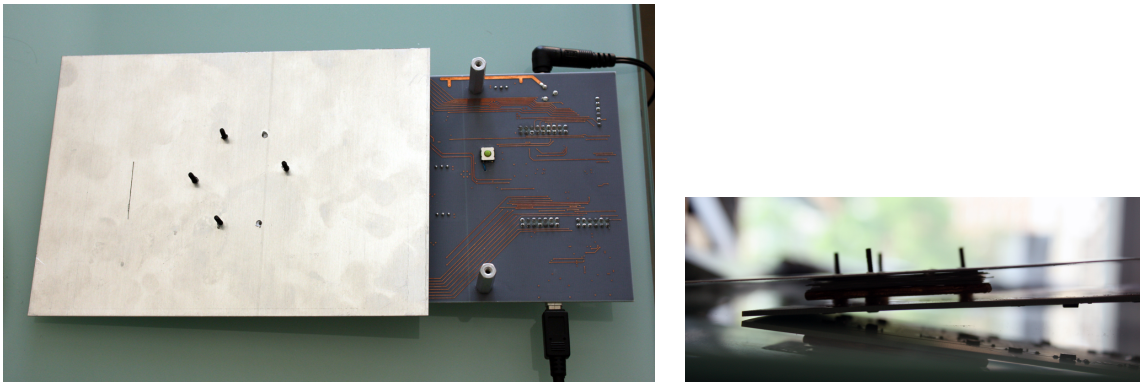


(a) (b)

Figure 71: Euclidean distance of NF signatures of the same certificate instance (a) over antenna couplings and (b) over frequency before and after placing an interfering metallic object, i.e., "key2," on top of the shielding copper surface, as shown in Figure 69.

6.2.7.2 *Large Aluminum Surface*

A 12.5 cm by 17.5 cm aluminum surface serves in this test as the conductive surface that is stacked on top of a full- and small-sized NF-CoA at different distances. The aluminum surface is attached as shown in Figure 72. The antenna array is aligned around the center of the metallic surface. As can be discerned in the cross-section view of Figure 66b, the distance between the NF-CoA and the antenna array is equal to the 1 mm thickness of a plastic bolt.



(a) (b)

Figure 72: (a) Top view and (b) cross-sectional view of a large aluminum surface when stacked (at different distances) on top of a certificate instance attached to the NF-CoA reader.

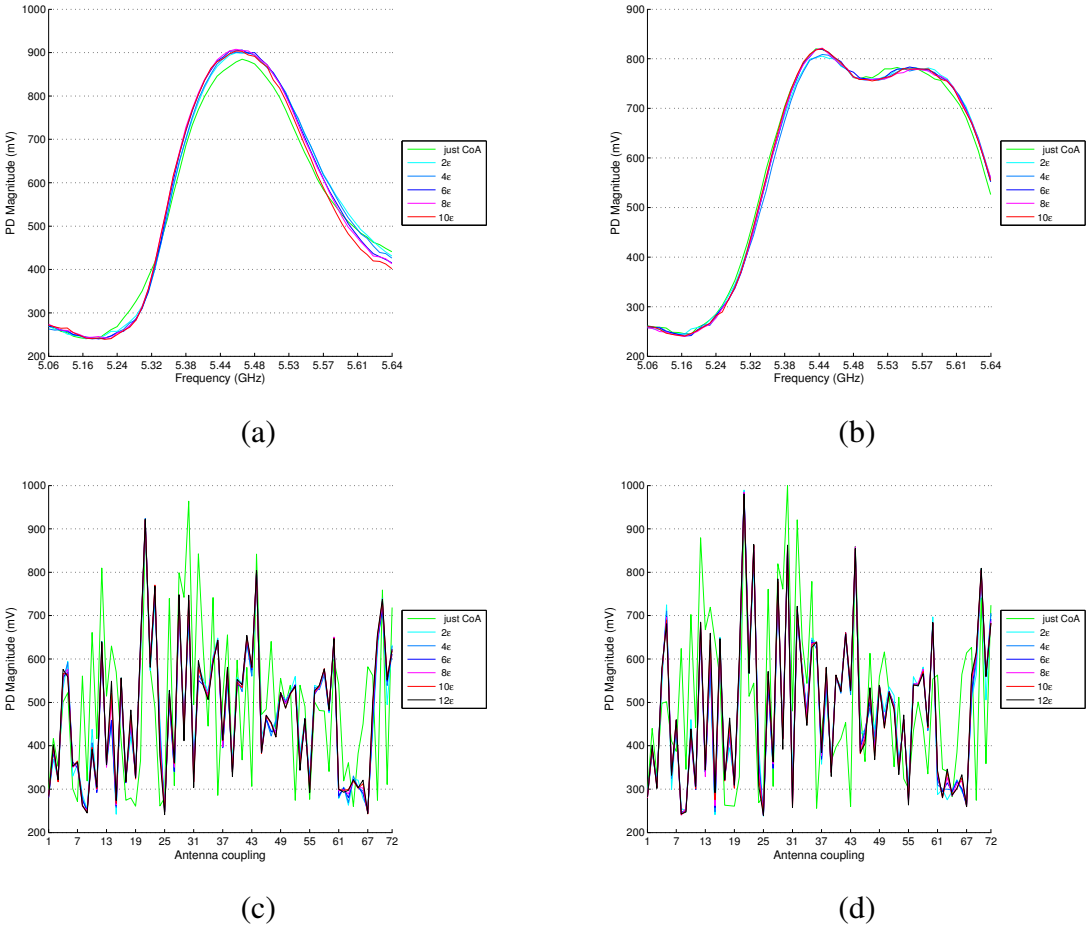


Figure 73: NF signature curves of full-sized copper-based NF-CoA *2gI* corresponding to: (a) antenna coupling B1-E1, (b) antenna coupling C3-D2, (c) frequency point 5.338 GHz, and (d) frequency point 5.370 GHz without ("just CoA") and with a large aluminum surface stacked on top of the NF-CoA at distances up to 3.5 mm ("12ε").

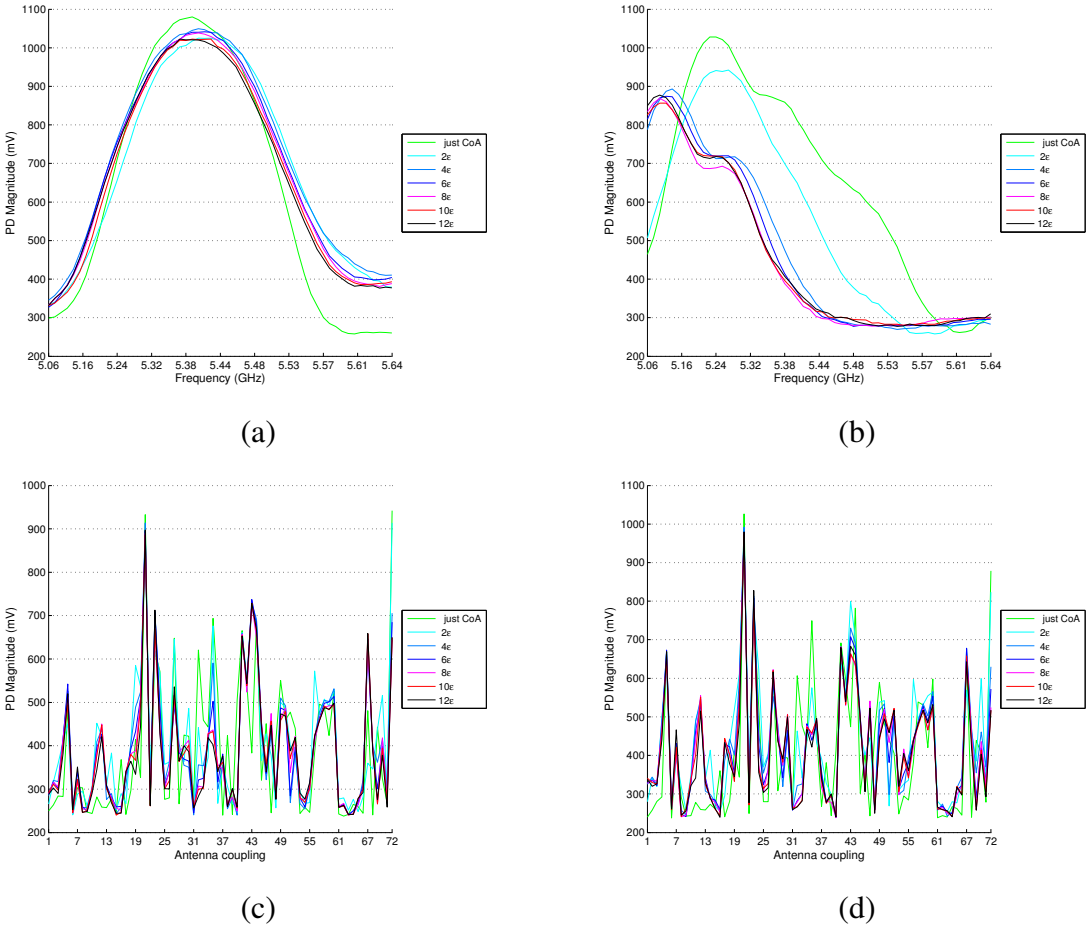
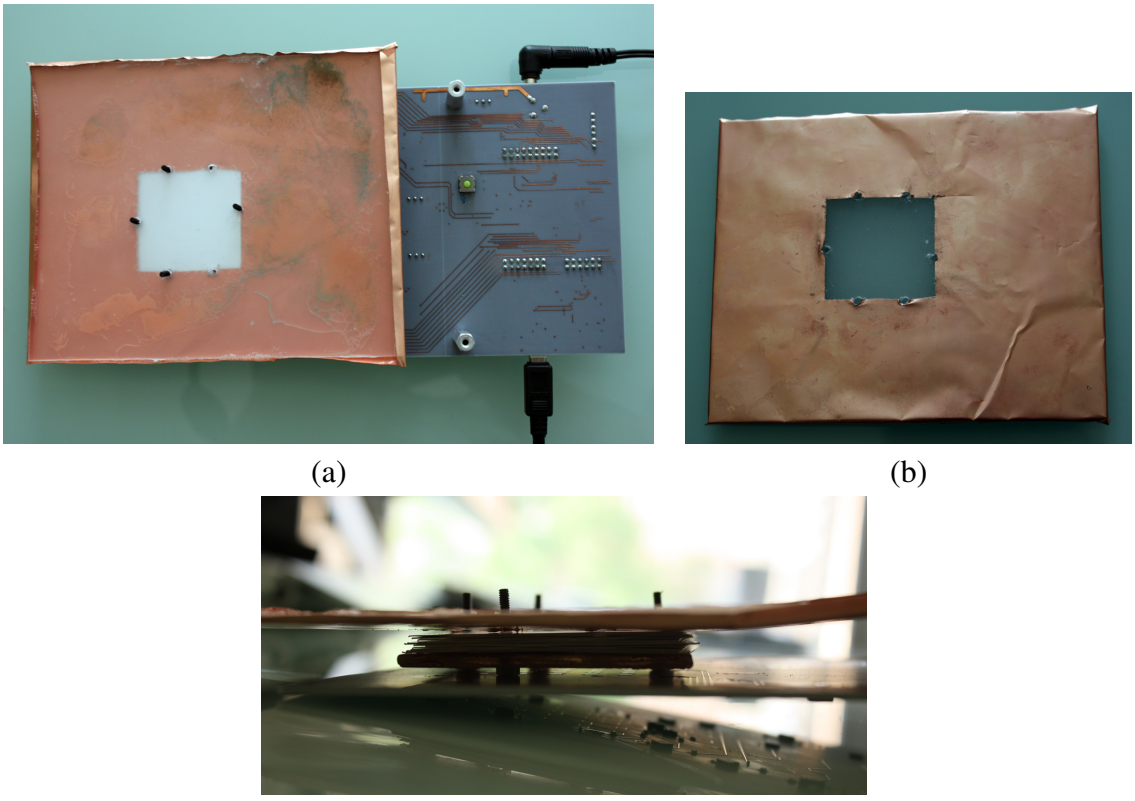


Figure 74: NF signature curves of small-sized copper-based NF-CoA *2gB* corresponding to: (a) antenna coupling B1-D1, (b) antenna coupling C3-E2, (c) frequency point 5.244 GHz, and (d) frequency point 5.281 GHz without ("just CoA") and with a large aluminum surface stacked on top of the NF-CoA at distances up to 3.5 mm ("12ε").

6.2.7.3 *Large Complementary Copper Surface*

A 12 cm by 15 cm complementary copper surface with an opening of 4 cm by 4.2 cm serves in this test as the interfering surface that is stacked on top of a full- and small-sized NF-CoAs at different distances. The aluminum surface is attached as shown in Figure 75. The antenna array, and thus the NF-CoA as well, is aligned around the opening of the metallic surface. As can be discerned in the cross-section view of Figure 66b, the distance between the NF-CoA and the antenna array is equal to the 1 mm thickness of a plastic bolt.



(a) (b)

(c)

Figure 75: (a) Top view and (c) cross-sectional view of a large complementary copper surface (shown in (b)) when stacked (at different distances) on top of a certificate instance attached to the NF-CoA reader.

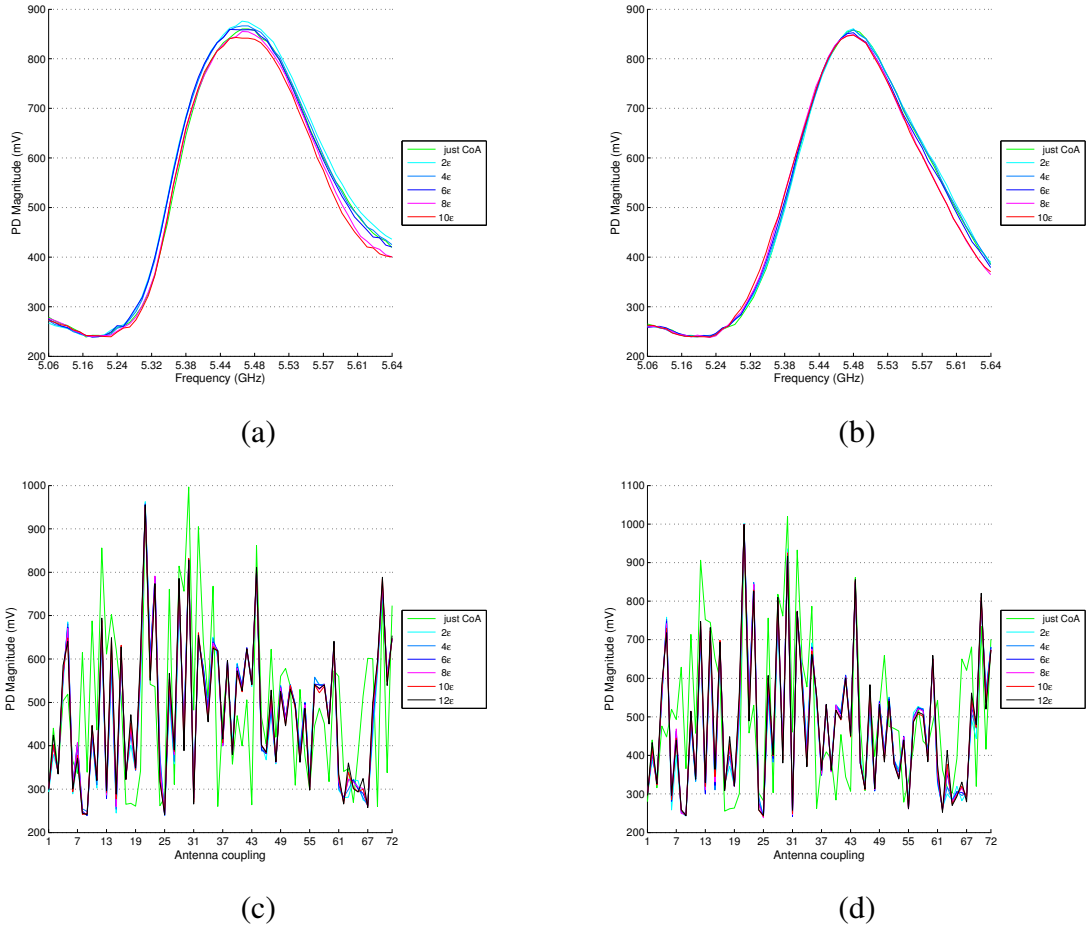


Figure 76: NF signature curves of full-sized copper-based NF-CoA *2gI* corresponding to: (a) antenna coupling B1-E1, (b) antenna coupling B2-E2, (c) frequency point 5.359 GHz, and (d) frequency point 5.389 GHz without ("just CoA") and with a large complementary copper surface stacked on top of the NF-CoA at distances up to 3.5 mm ("12ε").

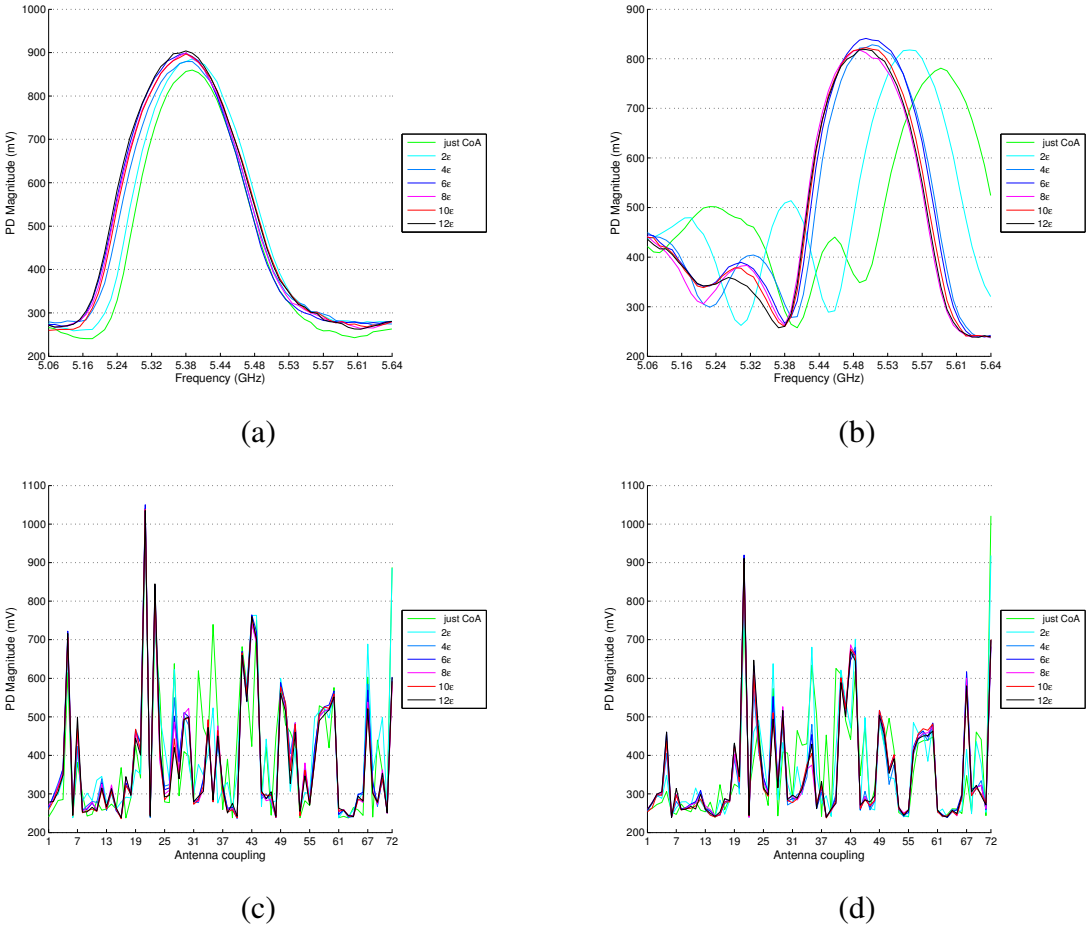


Figure 77: NF signature curves of small-sized copper-based NF-CoA *2gB* corresponding to: (a) antenna coupling B1-E1, (b) antenna coupling E4-B4, (c) frequency point 5.269 GHz, and (d) frequency point 5.204 GHz without ("just CoA") and with a large complementary copper surface stacked on top of the NF-CoA at distances up to 4.5 mm ("12ε").

CHAPTER 7

NF-COA ENTROPY EVALUATION

Before any attempt is made to quantify the entropy, or uncertainty, of the NF-CoA system, the metric of the similarity between any two fingerprints needs to be determined. An NF fingerprint f, the definition of which has been provided in Chapters 1 and 4, is a cardinality-N vector of numbers $\in \mathbb{R}^N$, where $N = N_{coupl} \times f_{MAX}$ with N_{coupl} being the number of antenna couplings, which is given by the possible permutations of the elements of the antenna array of the reader based on their functionality (see Section 5.2.1), and f_{MAX} the number of equidistant frequency points at which the scattering parameters of the NF signature are quantized and digitized (see Section 5.3.1).

In the context of this research effort, the *similarity metric* is the sum of the Euclidean distances of the magnitudes of the SHF signal power (in dB or V) of the S_{21} scattering parameters curves of different fingerprints at the same antenna coupling and frequency point over the whole aforementioned space N. Analytically, the distance $\| \cdot \|$ of two NF fingerprints, or of signatures f and f' is defined as:

$$d(f, f') = \|f - f'\| = \sum_{i=1}^{N_{coupl}} \sum_{j=1}^{f_{MAX}} \sqrt{\left(f_{ij} - f'_{ij}\right)^2} = \sum_{i=1}^{N_{coupl}} \sum_{j=1}^{f_{MAX}} \left|f_{ij} - f'_{ij}\right| \tag{9}$$

As described in Section 4.2.2, during the NF-CoA verification process the verifier first reads the signed fingerprint f^s and afterward compares the latter with a new read-out f^e of the NF-CoA that the verifier himself extracts with his own NF-CoA reader. The comparison/matching is done based on the distance metric of Equation (9). Only if the value of the distance between these two, signed and extracted, fingerprints at any (antenna coupling, frequency point) point $\|f^s_{ij} - f^e_{ij}\|$ is lower than a threshold δ_T, i.e., the difference does not exceed a certain level, does the verifier declare that the certificate and, thus, the document or product is authentic. This threshold δ_T is referred to as the *similarity detection threshold*.

The goal in this section is to use prior knowledge of the measured inter- and intra-CoA

distances/differences (presented in Chapter 6) between all the NF signatures available, so that:

- the entropy of the NF-CoA system can be reliably estimated, and
- the similarity detection threshold for any future NF-CoA system can be optimally determined with a well recognized statistical methodology.

7.1 Statistics-based Empirical Entropy Analysis

Obviously, the certificate verification/validation procedure is a *binary classification* problem, in which each certificate instance is mapped to one of two predicted classes/groups. The outcome of the comparison conducted by the NF-CoA reader between the signed and the extracted signature is labeled as

- T_+, that is, the certificate instance signature is believed to be *valid* or *authentic* (V_+), or
- T_-, that is, the certificate instance is believed to be *invalid* or *fake* (V_-).

From now, the terms *valid*, *authentic* and *positive* are used interchangeably. Accordingly, the terms *invalid*, *fake* and *negative* are used also interchangeably.

The Euclidean distance $\| \mathbf{.} \|$ between any two certificate fingerprints is represented by the data vector δ of random samples from an unknown population. Vector δ is an instance of the continuous random variable Δ.

As far as the measurement data are concerned, based on which the statistical analysis is conducted, let $\delta_p = (\delta_{p1}, \delta_{p2}, ..., \delta_{pk}) \in \mathbb{R}^{N_{\delta p}}$ with $N_{\delta p} = N_{coupl} \times f_{MAX} \times \binom{k}{2}$ be a vector of continuous independent and identically distributed (*iid*) random positive or valid (V_+) samples drawn from the distribution of S_{21} scattering parameter values (in *dBm* or simply V) of $\binom{k}{2} = k \cdot (k-1)/2$ distances between any two of the k intra-CoA (of the same CoA) signatures across all antenna permutations and frequency points. Accordingly, let

$\delta_n = (\delta_{n1}, \delta_{n2}, ..., \delta_{nl}) \in \mathbb{R}^{N_{\delta n}}$ with $N_{\delta n} = N_{coupl} \times f_{MAX} \times \binom{l}{2}$ be a vector of continuous independent and identically distributed random negative or invalid (V_-) samples drawn from the distribution of S_{21} scattering parameter values (in *dBm* or simply V) of $\binom{l}{2} = l \cdot (l-1)/2$ distances between any two of the l inter-CoA signatures (of different CoAs) across all antenna permutations and frequency points. The assumption about independence of the responses over neighboring transmitter-receiver couplings is not totally realistic, but the difficulty involved with inverting Maxwell's equations is overly high, as discussed in Section 8.2. Nevertheless, to strengthen the iid assumption, later in the "score computation" step, frequency points are skipped so that NF responses of only every other fourth frequency sample are considered. It should also be noted that misalignment noise is present in the above measurements as the placement of each certificate instance in the slot of the reader involved rotational inaccuracies around an axis perpendicular to the board and passing through the middle element (C3). This rotational displacement potentially was up to 3 degrees, which corresponds to around 1 mm of displacement on the circumference of the rotation. The reason for this was that the plastic poles were not firm enough as they were just fixed on the board with plastic screws (see Figure 44). This misalignment, is significantly higher than the mechanical alignment that can be achieved in an industrial environment and within the practicality tolerance needed for high-volume fabrication.

Following the principles of basic detection theory [91, 92, 93], the analysis needs to rely on the concepts of hypothesis testing, *probability density functions* (*PDFs*) and *receiver operating characteristic* (*ROC*) curves [48]. The formulated hypothesis under test here is that the extracted signature of a certificate instance is valid. The procedure of hypothesis testing involves the collection of data, i.e. aforementioned δ_p and δ_n, and estimating how likely the particular set of data is, assuming the hypothesis is true. If the data set is very unlikely, defined as being part of a class of data sets that are only rarely observed, the hypothesis is rejected concluding that the extracted signature is (probably) invalid. This class of data sets is specified via a test statistic, which reflects the extent of departure from

the hypothesis.

Toward that goal, let iid sample vectors δ_p and δ_n each be drawn from some distribution with an unknown density. The respective PDFs describe the relative likelihood for the random variable δ to take on a certain value of distance/difference between the extracted and signed signatures. Denote the positive PDF of a continuous signature test in variable δ as $f(\delta_p)$ in the case of a valid certificate instance and the negative PDF as $f(\delta_n)$ in the case of an invalid instance. To illustrate this approach, the graph of Figure 78 depicts examples of these PDF curves that model the four possible outcomes from the binary classifier as a function of the NF signature distance. Essentially, a continuous signature test is converted to a binary test by determining the classifier boundary between classes with value δ_T and interpreting results within those ranges as valid and results outside those ranges as invalid. As will be seen from the results of this analysis, a low probability of an incorrect classification decision is achieved when the two density distributions are largely separated with low variances.

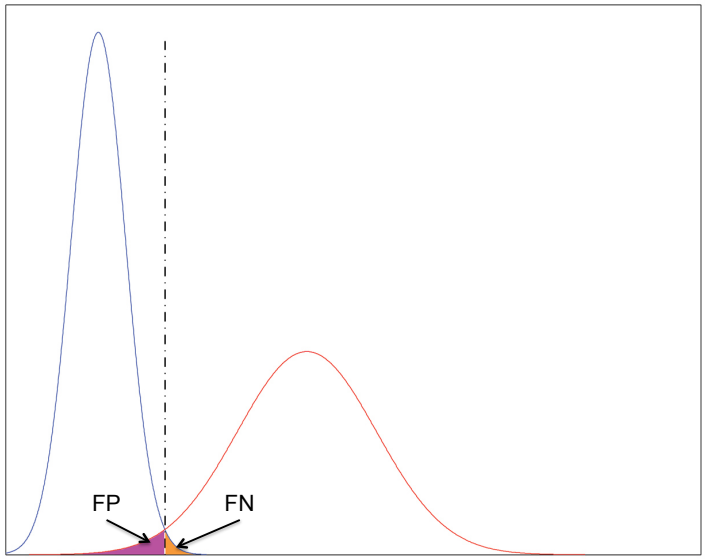


Figure 78: Example probability density curves depicting the four possible outcomes of a binary classification given a detection threshold represented by the black vertical line.

Out of the four possible classification outcomes from a binary classifier, namely *true positive* (*TP*), *true negative* (*TN*), *false positive* (*FP*) and *false negative* (*FN*), that are shown in Figure 78, the emphasis is placed on estimating the latter two ones:

- *FP* or *false alarm* ($= \int_{-\infty}^{\delta_T} f(\delta_n)\, dx$), where the outcome from a prediction is *P* and the actual value is *N*, i.e., the CoA is fake and predicted as authentic
- *FN* or *miss* ($= \int_{\delta_T}^{\infty} f\left(\delta_p\right) dx$), where, conversely, the prediction outcome is *N* while the actual value is *P*, i.e., the CoA is authentic and predicted as fake.

By defining *sensitivity* or *true positive rate* as $\text{Se} \triangleq TPR = P(T_+|V_+) = TP/(TP + FN)$ (probability of a successful verification when the certificate is authentic), and *specificity* or *true negative rate* as $\text{Sp} \triangleq TNR = P(T_-|V_-) = TN/(FP + TN)$ (probability of a failed verification when the certificate is fake), one can get the two-by-two contingency table or confusion matrix of outcome probabilities, shown in Table 7. Here, $P(D_+)$ is the pre-test probability of validity prevalence in the general population.

Table 7: Contingency table (or confusion matrix) of outcome probabilities of a binary classification problem.

		True Class	
		$\mathbf{V}_+$	$\mathbf{V}_-$
Predicted Class	$\mathbf{T}_+$	$P(D_+) \cdot \text{Se}$	$[1 - P(D_+)] \cdot (1 - \text{Sp})$
	$\mathbf{T}_-$	$P(D_+) \cdot (1 - \text{Se})$	$[1 - P(D_+)] \cdot \text{Sp}$
Total		$P(D_+)$	$1 - P(D_+)$

For the intra-CoA measurements, a single NF-CoA instance is placed on the reader, then taken off and then placed back on the reader to indicate any changes in measurement results and the whole process is repeated nine times. As for the inter-CoA scenario, this involves the measurement of all 47 different available certificate instances. Given that the absolute value of the distances between NF-CoA signatures is considered, the positive PDF curve that includes probabilities *TP* and *FN* is expected to have a large magnitude and be

located close to 0+ (the y axis) and the negative PDF bell is expected to be located on the positive x semi-axis. The decision or discrimination threshold value or similarity level δ_T is the distance value (on the x axis) shown with the dotted line in Figure 78 where the two PDF curves intersect [91].

The corresponding classification ranges can be identified with the use of the likelihood-ratio criterion [94, 95, 96, 97].

$$\lambda(\delta) = \frac{f(\delta|V_+)}{f(\delta|V_-)}$$

describes the ratio of the likelihood of observing a sample distance vector δ in the population of valid signatures over that of the population of invalid ones. Regions with $\lambda < \delta_T$ are denoted as T_- and those with $\lambda \geq \delta_T$ as T_+, where the threshold δ_T can vary between zero and infinity. Additionally,

$$\text{Se} = P(T_+|V_+) = \int_{\delta_T}^{\infty} f(\delta|V_+)\, dx$$

$$1 - \text{Sp} = P(T_+|V_-) = \int_{\delta_T}^{\infty} f(\delta|V_-)\, dx$$

Adjusting the threshold δ_T will in turn change Se and (1-Sp), which together determine all four decision fractions (Table 7). Explicitly changing the decision threshold several times, will yield several different pairs of Se and (1-Sp), which if plotted on a two-dimensional graph will give the ROC curve (see Figure 79).

First, the distance/difference vectors δ_p and δ_n are calculated after extracting with the NF-CoA reader all available positive $f_p \in \mathbb{R}^{N_p}$ and negative $f_n \in \mathbb{R}^{N_n}$ signatures with $N_p = N_{coupl} \times f_{MAX} \times k$ and $N_n = N_{coupl} \times f_{MAX} \times l$, respectively. For each single antenna permutation and frequency combination, the logarithm base 10 (log) of the PDF of the intra-CoA random variable δ_p (for distance values that positive samples take) and in a small frequency neighborhood (total of nine frequency points) is estimated. Since accurate PDFs are difficult to acquire with relatively few measurements (binomial coefficients), the most popular non-parametric way is applied, namely the *kernel density estimation* (*KDE*). KDE

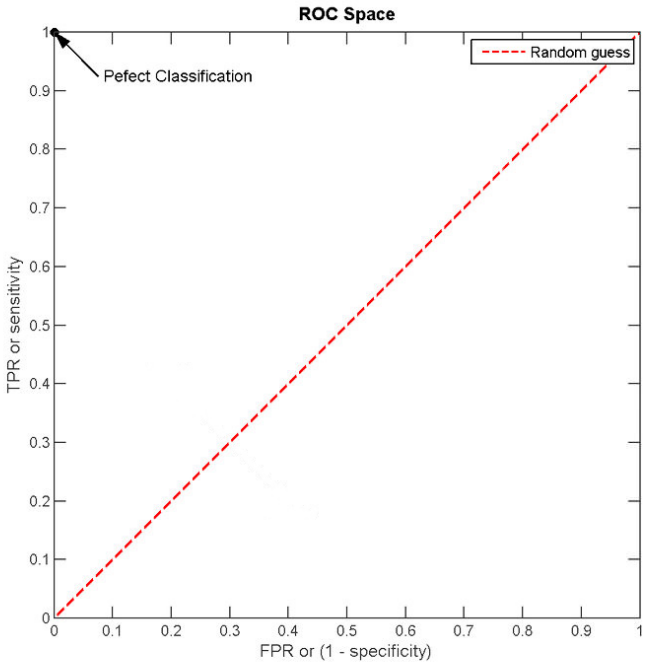


Figure 79: The receiver operating characteristic space. The red dashed line represents a random guess, whereas point (0,1) indicates perfect classification.

takes a finite sample of data and make inferences about the underlying PDF everywhere by smoothing out the contribution of each data point (with the weighting function of the kernel) into a region of space surrounding it and aggregating (iid property already assumed) the individually smoothed contributions (see [98, 99, 100]). The kernel density estimator is represented with Equation 10, where $K(\cdot)$ is the kernel and $h > 0$ is the smoothing parameter (bandwidth).

$$\hat{f}_h(\delta) = \frac{1}{n}\sum_{i=1}^{n} K_h(\delta - \delta_i) = \frac{1}{nh}\sum_{i=1}^{n} K\left(\frac{\delta - \delta_i}{h}\right) \tag{10}$$

In the framework of this analysis, the KDE implementation of Botev et al. [101] is used, since it is considered a bona fide PDF; it is conservative enough (fits each point with a thick Gaussian of automatically chosen bandwidth) and substantially reduces the asymptotic bias and the mean square error, unlike other proposals.

Since the PDF of positive distances/differences is now available, it is possible to derive the maximum likelihood estimate, the so-called "probability of the data" rather than the parameter, of a signature distance measurement (sample vector δ). In other words, the maximum likelihood estimate that the certificate instance is positive or negative is derived. Each binomial-coefficient possible distance measurement is "scored" with an aggregate maximum log likelihood (averaged across the frequency spectrum and the antenna couplings) corresponding to the aforementioned hypothesis that the extracted signature of a certificate instance is valid. A histogram of these scores is shown in Figure 80. As expected, small log values (leftward on the x axis) correspond to the negative, that is, invalid, samples. For the sake of completeness, Figure 81 illustrates the maximum log likelihood of the negative and positive signature distances/differences averaged across all the binomial coefficient available measurements for each pair of frequency point and antenna coupling. Especially regarding the negative scenario, only every other fourth frequency point is considered to strengthen the aforementioned iid property assumption.

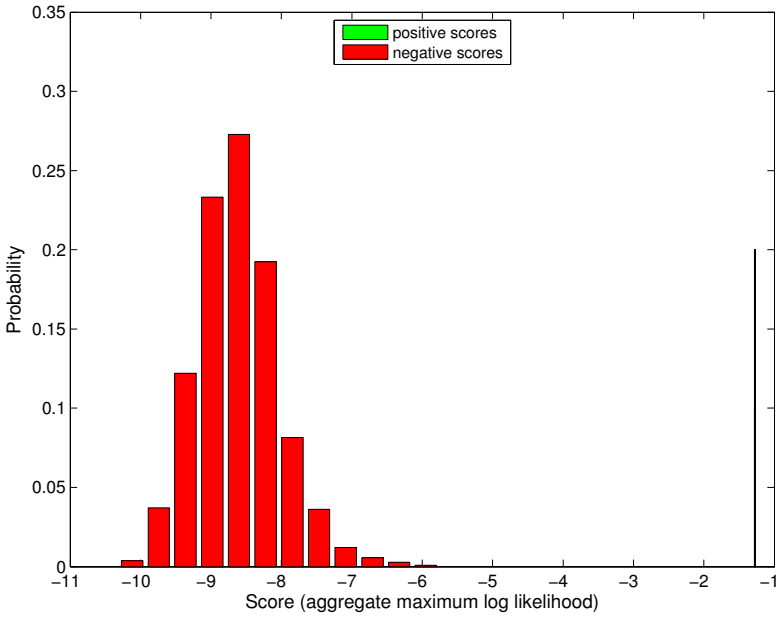
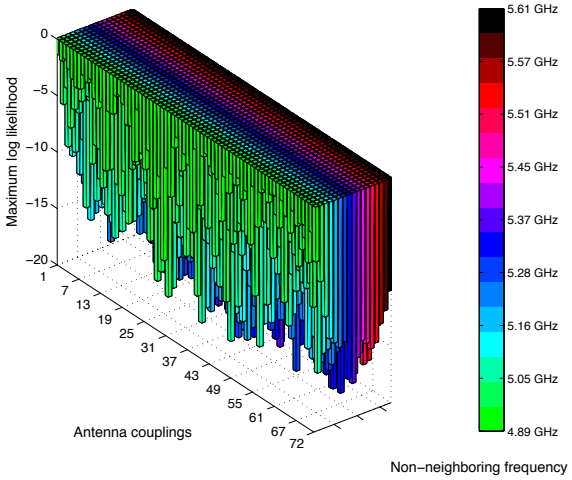
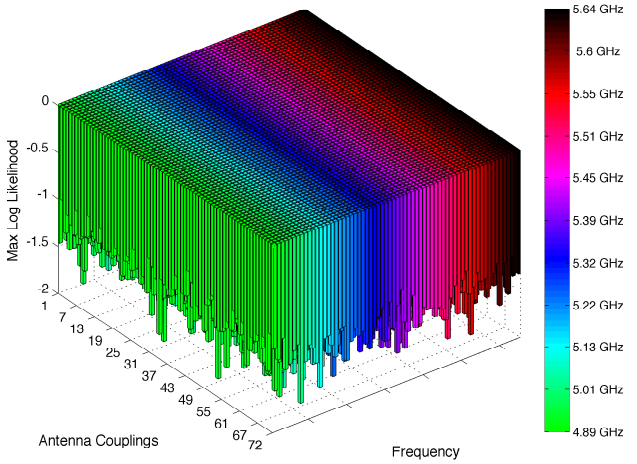


Figure 80: Histogram of the negative (red) and positive (green) scores (aggregate maximum log likelihood values) of each binomial-coefficient possible distance measurement.



(a)



(b)

Figure 81: Three-dimensional bars of the maximum log likelihood of the (a) negative and (b) positive signature distance measurements. To strengthen the iid property assumption, every other fourth frequency point is considered in the negative (inter-CoA) scenario.

The overall resulting positive and negative scores can be modeled as PDFs, using the pure Gaussian-based KDE (*ksdensity* function of Matlab [87]), to get the two final densities that model the *FP* and *FN* error probabilities. These negative and positive probability densities over the scores defined above are shown in Figure 82. The result of this empirical analysis is that the probability of intersection of the density curves is lower than 10^{-200}. In other words, the probability that the NF-CoA system predicts a fake CoA as authentic or predicts an authentic CoA as fake is inconceivably small.

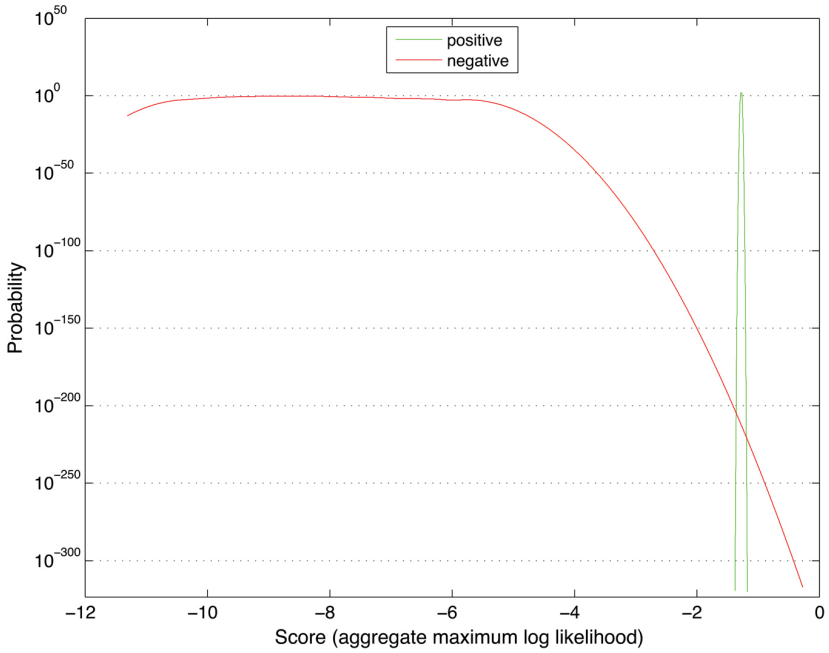


Figure 82: The positive and negative probability densities over the aggregate maximum log likelihood values of the signature difference measurements.

The near-deterministic and highly entropical performance of the NF-CoA system is also verified by the calculated ROC curve, shown in Figure 83. The *sensitivity* (Se) or *true positive rate* (*TPR*), that is, the proportion of instances that tested authentic (*TP*) to all the instances that actually are authentic (*TP*+*FN*), is by many decimal points almost 1 (0.99999...) and the *1-specificity* (1-Sp) or *false positive rate* (*FPR*), that is, the proportion of instances that tested authentic (*FP*) to all the instances that actually are fake (*FP*+*TN*), is

by many decimal points almost 0 (extremely small number in the ROC space: 0.00000...). This means that the chosen point on the ROC space, shown in Figure 83, for a certain detection threshold δ_T is almost identical to that of $(0, 1)$, which is termed *perfect classification*. Equivalent to this, is that the value of the area under the ROC curve, abbreviated *AUC*, is close to 1.0.

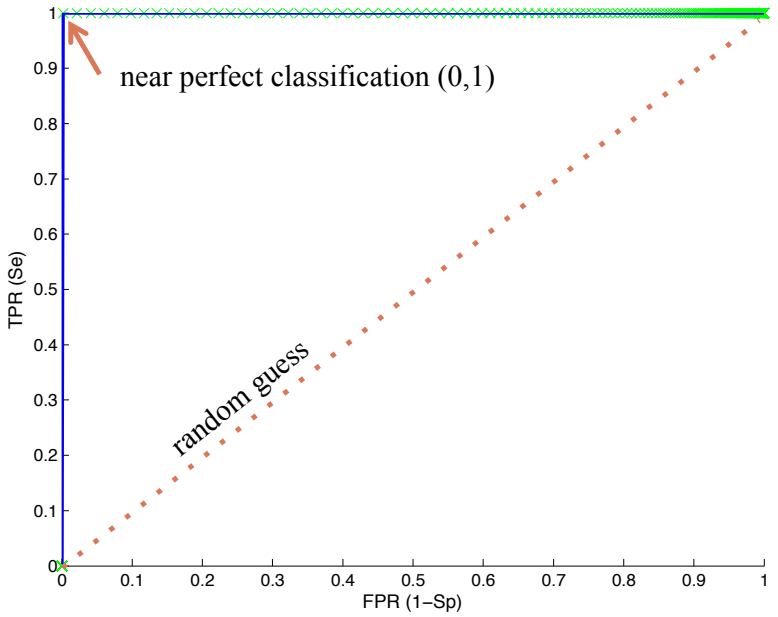


Figure 83: The receiver operating characteristic curve of the NF-CoA binary classification problem. The green points represent different (TPR, FPR) points for different similarity detection threshold δ_T values. A δ_T option that corresponds to almost perfection classification, i.e., $(0, 1)$, exists.

By following a conservative statistical methodology at modeling each PDF, an upper bound on performance is expected to exist. A parametric analysis on the two sole parameters, namely frequency neighborhood for the Botev KDE and density of non-neighboring frequency points for the iid property, has been conducted, of course, yielding a similar or even greater performance. In particular, for any of the two parameters being assigned a value in the $[2, 10]$ range, the probability of intersection of the negative and positive density curves is always lower than 10^{-150} and in many cases close to 10^{-300}.

7.2 Randomness Evaluation With the NIST Statistical Test Suite

Based on the analysis provided in the previous section, it is believed that the signatures extracted by the NF-CoA system are indeed random and, thus, the entropy is high. Nevertheless, in order to strengthen the above claim, empirical evidence is also provided in this section by conducting randomness testing based on one of the most stringent and highly regarded test suites, the NIST Statistical Test Suite (NIST STS) [102]. This battery of independent and computationally intensive statistical tests is the same test suite that was used for the randomness testing of the five finalist encryption algorithms for the Advanced Encryption Standard (AES), namely Mars, RC6, Rijndael, Serpent and Twofish [103].

7.2.1 The *Null* Hypothesis

The null hypothesis typically corresponds to a general or default position and can never be proven. A statistical test, based on a set of data, can only reject a null hypothesis or fail to reject it. The null hypothesis in the context of this research work is that *a tested bit sequence that represents an NF signature/fingerprint is random and could have been generated by running a truly random number generator*. A test applies particular mathematical methods on the input data, i.e., the NF signature, to derive a relevant randomness statistic, based on which the null hypothesis is accepted or rejected. This test statistic value, the *P-value*, embodies the strength of the evidence against the null hypothesis. Basically, it is the probability that the given sequence could have been generated by running a truly random number generator once.

If P-value is larger than a critical value, the significance level α, then the sequence appears to be random and the null hypothesis is accepted. Otherwise, if P-value is smaller than α, then the null hypothesis is rejected. The level of significance, also called *Type I* error or α error, is the probability that a test indicates that a sequence is non random when it is in fact random.

7.2.2 Testing Against the NIST Statistical Test Suite

The NIST Statistical Test Suite, developed by the Computer Security Division and Statistical Engineering Division of the National Institute of Standards and Technology, is a highly regarded set of algorithmic tests, which attempt to identify binary digit sequences that do not behave in a truly random manner. They are widely preferred for analyzing cryptographic random number generators (RNGs) and pseudorandom number generators (PRNGs).

As described in the previous subsection, a P-value is calculated for each binary sequence and each statistical test. A sequence is considered to pass a test if the corresponding P-value exceeds the predetermined significance level α. A very common value of α in cryptography is 0.01. A P-value ≥ 0.01 leads to the conclusion that the sequence is random with a confidence of 99%. Conversely, a P-value < 0.01 leads to the conclusion that the sequence is non random with a confidence of 99%. Closely associated with the P-value is the proportion of success sequences; the number of sequences with a P-value greater than the significance level α, divided by the total number of bit sequences tested. NIST [102] specifies a range of acceptable proportions. This confidence interval is defined as

$$\hat{p} \pm 3\sqrt{\frac{\hat{p}\,(1-\hat{p})}{m}} \tag{11}$$

where $\hat{p} = 1 - a$ and m is the number of bit sequences tested. For the NF-CoA empirical randomness tests, 47 copper-based bit sequence signatures ($m = 47$) were available and used. Based on the formula above, the lower boundary of the range of acceptable proportion is 0.946 for copper-based NF-CoAs. If the proportion falls outside of this interval, then there is evidence that the data is non random.

The NF signatures have been fed to the NIST STS as ASCII characters consisting of zeroes and ones, which is the binary representation of the data extracted by the NF-CoA reader. It was evident from the performance analysis of Chapter 6, that the highest entropy exists around the resonant frequency of the antenna elements of the reader. So, the results presented below are for a portion of the NF signatures over the 60 MHz range around the

center frequency of 5.45 GHz, in which case the size of each of the bit sequences is equal to 17.408 Kbytes.

The NIST STS tests focus on different types of non randomness that can exist in a sequence [102]. The ones the NF signature bit sequences were tested against are the following:

- **Frequency Test** determines whether the number of ones ("1") and zeros ("0") in a tested bit sequence are approximately $1/2$.
- **Cumulative Sums Test** determines whether the maximum absolute value of the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected cumulative sum for truly random sequences. A dual test is derived by applying the test backward through the input sequence instead of forward.
- **Discrete Fourier Transform Test** detects periodic features in the tested sequence, such as repetitive patterns that are near each other, by computing the peaks of the discrete fast Fourier transform (DFFT) of the tested sequence.
- **Rank Test** checks for linear dependence among fixed-length substrings of the original sequence.
- **Non-overlapping Template Matching Tests** determine whether there are too many occurrences of predefined aperiodic patterns (148 such patterns and, thus, different tests). If a pattern is not found, the match window slides one bit position. The default block length parameter value of nine is used.
- **Linear Complexity Test** determines the length of a linear feedback shift register [104] that would produce the tested bit sequence. A short feedback register implies lack of randomness. The default block length parameter value of 500 is used.

The NIST STS results are summarized in Table 8. Obviously, the proportion of signatures that passed the tests for copper-based NF-CoAs is very high. Even in the case of the discrete Fourier transform test tagged by the NIST STS as "Failed," the proportion of passed signatures (0.915) is very close to the aforementioned pass rate of 0.946. The presence of periodicity between the binary sequences of the signatures that causes the failure of a few sequences is mostly attributed to the fact that the small-sized copper-based NF-CoAs do not cover the whole area of the antenna array and, thus, allow certain antenna couplings not to be disrupted. An increased success rate can be achieved with a smaller antenna array, the projection area of which coincides with the 2D area of the small-sized copper-based CoAs.

Table 8: NIST statistical test suite results for all 47 copper-based NF-CoAs.

Test name	*Proportion of passed signatures within interval range*	*NIST STS Conclusion*
Frequency (Monobit)	0.979 (= 46/47)	Passed
Cumulative Sums (forward)	0.957 (= 45/47)	Passed
Cumulative Sums (backward)	0.979 (= 46/47)	Passed
Rank	1.000 (= 47/47)	Passed
Discrete Fourier Transform	0.915 (= 43/47)	Failed (< 0.946)
Non-overlapping Template Matching	1.000 (= 47/47) for vast majority of 148 tests	Passed
Linear Complexity	0.957 (= 45/47)	Passed

This deduced inherent unpredictability potentially allows the NF-CoA system to take over the additional role of a reasonably good physical RNG. This statement takes on an even larger importance if one considers that:

- No pre- or post-processing of the bit sequences is applied, compared to the related work in the area. Instead, the raw data is directly fed to the suite.
- No consecutive multiple refeeds of the bit sequences is applied. The results are based on the test outputs for a single feeding of each bit sequence of each NF signature.
- No Von Neumann [105, 106] or any other corrector is applied on the bit sequences to remove any weakness in the entropy source, such as potential duplicate patterns.
- No optimization of the parameters of the NIST STS has been pursued.

7.2.3 The NF-CoA System as a Physical Random Number Generator

The ability to generate random and pseudorandom numbers is essential in many cryptographic applications. As opposed to pseudo random number generators that produce bit sequences from an initial value, a *seed*, using a known algorithm, physical/hardware RNGs require no seed. Instead, RNGs attempt to extract randomness directly from complex and unpredictable physical non-deterministic sources, such as temperature, atmospheric or electromagnetic noise, etc., to produce random bits [107, 108, 109, 110].

For a physical RNG to use its produced bit strings directly, without the application of further processing, the generated sequences need to meet strict randomness criteria to determine that the underlying physical sources appear random [102]. In this section, one candidate physical RNG, the underlying physical concept of which is based upon the near-field electromagnetic effects of an SHF signal impinging on complex 3D physical conductive and dielectric structures, has been tested against one of the most stringent and worldwide recognized test suites revealing the potential of leveraging the NF-CoA system for applications that need hardware RNGs.

CHAPTER 8

WITHSTANDING ADVERSARIAL EFFORTS/ATTACKS

The anti-counterfeiting nature of the NF-CoA system and the consequent benefits from counterfeiting NF-CoA protected objects render a discussion about potential attacks imperative.

Regarding the NF fingerprint f as a cardinality-N real vector of numbers $\in \mathbb{R}^N$, the key attack problems can be formulated as following:

Problem #1: Assuming the adversary has physical access to an original NF-CoA reader, as well as any original certificate instance X he wishes to counterfeit, is it possible to develop a manufacturing process that can massively and exactly or nearly-exactly reproduce/replicate X at a low price?

Problem #2: Assuming the adversary has in his possession the electromagnetic fingerprint f of an authentic certificate instance, which he himself extracted using an original or successfully replicated NF-CoA reader, is it possible to find a three-dimensional object of the same dimensions as the original certificate, that produces an electromagnetic near-field response f' such that $\|f_{ij} - f'_{ij}\| < \delta_T$, where the detection threshold δ_T is a standardized distance metric $\| \cdot \|$, such as the Euclidean distance, between f and f' and, as such, is a proportionally small scalar?

Problem #3: Is it possible for an adversary to directly compute the issuer's private key and, as a result, be able to ultimately create his own physical NF-CoA object, extract its near-field signature with an NF-CoA reader and sign and store the fixed-length bit string of the signature (as in Figure 12)?

Problem #4: Assuming that the certificate instance is not embedded into the surface of the protected item, i.e., the certificate is in the form of a tag, and assuming that the embedded storage chip is physically co-located with the 3D structure of the NF-CoA, is it possible for an adversary to misappropriate original NF-CoA tags?

The NF-CoA instances are intended to protect a physical object in scenarios where any of the above challenges may be applied. As a result, all the above problems are considered separately below. Considering them, nevertheless, first as a whole, these key problems involve two layers of difficulty and complexity, namely manufacturing (the first two problems) and computational (the last three problems). As argued below, it is these two layers that inherently enforce the security of the CoA instances.

For completeness sake, the practical aspects of all the above attacks, visited in recent studies [111, 48, 53], are reported. Nevertheless, this chapter focuses on the most interesting, from a complexity point of view, problem; Problem #2. Complementary to the theoretical study is an example of inverse design attack that has been launched against the NF-CoA system in Section 8.2.3.

8.1 3D CoA Physical Replication/Reproduction

Let us assume that an adversary has in his possession an original, physical NF-CoA instance. By using a, somehow acquired, NF-CoA reader, the adversary extracts the exact NF fingerprint f. An attack against the NF-CoA system is considered successful when the adversary is able to construct a nearly-exact replica that can produce a near-field response f' such that $\|f - f'\| < \delta_T$, where δ_T is the detection threshold analyzed and quantified in Chapters 6 and 7.

Formulating a manufacturing process that can exactly or nearly exactly replicate the 3D structure of an already signed CoA instance consists of two major steps, namely (i) capturing the physical 3D structure and (ii) realizing this structure into the physical world. There

is a number of potential state-of-the-art 3D scanning and imaging processes, such as stereoscopy [112], confocal microscopy [113], conoscopic holography [114], structured-light method [115], and computed tomography, including magnetic resonance imaging (MRI) [116], X-ray microtomography [117], and optical coherence tomography [118, 119], that can help accurately scan arbitrary complex 3D structures. Nevertheless, the major challenges arise during the attempt to fabricate this three-dimensional physical structure with very high precision in terms of mechanical tolerances and, finally, to embed the structure in an encapsulating sealant by making using of materials that have dielectric properties as close as possible to those of the original certificate instance.

Although this type of attack is not unfeasible, it requires certain expenses by the malicious party. The cost of a massive successful adversarial manufacturing process, including not only the development but also the necessary research, has to be lower than the earnings that can be fetched on the market by selling the counterfeit product. From this perspective, it is obvious that a certificate instance can be used to protect an object, the value of which does not exceed the cost of forging a single CoA instance. Finally, it should be highlighted that a successful such attack results in the forging of only a single certificate instance, that is, the same effort has to be invested for every single NF-CoA physical instance.

8.2 Inverse Design Attack

The objective of the malicious party under this type of attack is to be able to create any 3D object of the same dimensions as an original NF-CoA that produces a near-field signature f' that is nearly-exact same to that of the original one f. In addition to any final manufacturing process involved, here an adversary needs to be able to numerically compute the NF signature of any own-designed physical certificate instance with very high precision and almost no assumptions (*forward design* problem) and also be able to launch and complete in reasonable amount of time a space search of all candidate designs, the superposition or other combination of which yields the desired fingerprint f' (*inverse design* problem). As

a result, solving the forward problem is only a step toward solving the associated inverse problem. This dependence also reveals that the higher numerical accuracy and efficiency of the forward solution is, the less arduous the search for the inverse solution/s is.

8.2.1 Step 1: Forward Design Complexity

The first challenge that an adversary is confronted with under this type of attack is the forward design complexity, the fundamental problem of directly computing NF responses/signatures.

The adversary will typically attempt to launch a *super-positioning attack*, that is, try to obtain a desired final near-field response by combining a number of physical objects with known fingerprints at different highly accurate 3D positions relative to the plane of the antenna array. To acquire these "known fingerprints," the adversary needs to be capable of numerically computing with high precision any complex physical structure constrained by the fixed dimensions of an original NF-CoA instance. A small change in the physical position incurs a large set of different responses for each one of the individual physical objects combined, as shown later in Section 8.2.3. This parameter, in addition to the number of physical objects used, are only a couple of the many parameters that the malicious party has to deal with in an optimal way so that the search space visited in the next step of inverse design problem does not end up being tremendously large.

Moreover, it is argued that, for a dense population of scatterers in the CoA instance, the system is *non-linear* in terms of near-field responses produced. One can understand this by simply assuming only two scattering physical objects S_1 and S_2 that, when individually placed in front of an antenna array, yield $f(S_1)$ and $f(S_2)$, respectively. Nevertheless, when both are in each other's proximity and in front of the antenna array, their joint response is $f(S_1 + S_2) \neq f(S_1) + f(S_2)$ because of their mutual interdependence, which is expressed, for example, by coupling between S_1 and S_2 or by additional reflection or refraction on S_1 by the reradiated energy from S_2 (which energy did not exist when S_2 was not in the proximity of S_1, finally yielding $f(S_1)$).

The precision and reliability of the electromagnetic field solvers has been thoroughly studied and assessed in a large body of literature. The benchmark studies, referred to below, employ the majority of the available state-of-the-art full Maxwell three-dimensional electromagnetic field solvers. Categorized by their solution method, the integral equations solvers are IE3D of Zeland Software, FEKO of EM Software & Systems, ADS Momentum of Agilent and MAGMAS 3D of K.U. Leuven, the finite element method (FEM) solvers are Ansoft HFSS and Comsol Multiphysics, the finite-difference time-domain (FDTD) solver is CST Microwave Studio and the method of moments (MoM) solvers are AWR Microwave Office Sonnet and Software EM. With the exception of a few studies, these popular EM solvers are not only compared to each other, but their results are compared against real measurements performed on prototype antennas and/or microwave devices manufactured with high mechanical precision just for this purpose.

The structures benchmarked include a line-fed planar patch with local dielectric inhomogeneity, an ultra-wide-band (UWB) planar antenna (3.1 GHz to 10.6 GHz) and a planar folded monopole antenna for GSM application (up to 2 GHz) in [120], a simple line-fed patch antenna (45 mm by 15 mm) on an extended Rogers R04003 substrate in [121], a cavity-backed aperture antenna (covering, among others, the 3 GHz to 6 GHz range) in [122], a slot rhombic antenna (covering the 2 GHz to 3 GHz range) in [123], a very compact planar antenna in [124], a conventional $\lambda/2$ microstrip resonator and a 2D Hilbert resonator (covering the 5 GHz to 6 GHz range) in [125], dielectric objects in free space and a cavity with a perfectly metallic boundary in [126], a resonant left-handed (LH) microstrip line, composed of complementary split ring resonators and capacitive gaps in the microstrip in [127], and a complete industry-standard SOIC8 (single-outline integrated circuit with eight leads) circuit, packaging, and an interconnection topology combined with a completely passive electrical circuit inside represented by a well-defined geometrical and material model (covering the 1 GHz to 14 GHz range) in [128]. Specifically in the near-field region domain, Karamehmedović et al. [129] investigated the problem of scattering

by a spheroidal silver nano particle immersed in glass and illuminated in the wavelength range 250 nm to 900 nm. After ruling out purely analytic methods such as the Mie theory [130], which is restricted to simple shapes like spheres, the FDTD, which relies on the staircase approximation and not on an unstructured mesh to accurately represent curved surfaces, and time domain methods, which usually require an approximation of the permittivity with analytic models, the authors compared the FEM-based Comsol Multiphysics, a multiple multipole (MMP) implementation (MMP 3D), a discrete dipole approximation (DDA) implementation (DDSCAT) and the null field method with discrete sources (NFM-DS) implementation of T-Matrix type.

The authors of these benchmark testing articles notice considerable deviations in the real and imaginary parts of the scattering parameters, the resonant frequency and its power magnitude, the -10 dB bandwidth and quality factor Q or even the electric field magnitude in V/m in the time domain. Vasylchenko et al. [121] in their study conclude that forcing HFSS to double the amount tetrahedra for antenna model discretization or number of mesh cells per wavelength in Momentum and CST Microwave Studio does not affect the solution significantly, if a convergence criterion of the method is met. Furthermore, Karamehmedović et al. [129] drew the conclusion that the quality of the computed near field can deteriorate significantly as the observation point approaches the scatterer surface. To summarize, the conclusions of all the above studies prove that the analysis of even planar antennas is not always straightforward; simple antennas with regular geometries, may involve intensive computational tasks of arguable accuracy [131].

The deviations in the results can be attributed to a plethora of reasons. Two of the most crucial design goals are the correct feeding modeling and the proper mesh generation [120]. Since a slight difference between the simulated feed topology and the actual setup may result in completely different performance, the model selected has to match as closely as possible the real physical feed topology [132]. Very fine/dense meshing near the ports and at critical regions is also a necessity. According to Massaro [133], the singular

behavior of the electromagnetic field close to sharp dielectric edges is poorly represented and the frequency domain characteristics of the structure will typically be shifted, unless a very fine mesh is used. The researcher recommends, specifically for these points, the analytical treatment of the EM field configuration in proximity of 3D corners. Impedance mismatch of the feed lines, different excitation models and de-embedding schemes should also be considered. Nevertheless, Vandenbosch et al. [120] indicate that the PCB manufacturing process, although it does not yield loss and substrate dielectric constant uniformity, is not the cause of the discrepancy between the solvers; this may only explain some of the variation between the solvers.

Important, though, the difference between the simulation results and the measurements may be, what is even more critical is that the aforementioned investigations of the simulation results reveal lack of mutual correspondence between the different software solvers themselves. This discrepancy is further corroborated by the existence of a relatively new IEEE standard [134], which attempts to validate computational EM simulation results, even if the software code used is established.

Finally, the computational complexity exists even despite the fact that for the current generation of NF-CoAs instances only isotropic materials have been considered. Finding approximations that can accelerate an electromagnetic field solver can be a difficult task if non-linear building materials are used for the fabrication of the certificate instances. Candidate such materials are *ferrites* (ceramic compounds with ferromagnetic properties that show various kinds of anomalies in their power absorption at high microwave signal levels [55]) and *metamaterials* (artificial materials, the permittivity and permeability of which are both negative resulting in a negative index of refraction and, thus, in a phase velocity that is anti-parallel to the direction of the Poynting vector [135, 56]).

8.2.2 Step 2: Inverse Design Complexity

The inverse design problem, that is, the problem of inverting time-domain electromagnetic data to recover three-dimensional distributions of electrical conductivity, is of major interest in the fields of geophysics and medical imaging.

There are many practical challenges that render the task of fully interpreting three-dimensional datasets an arduous one [136]. A fast, accurate and reliable algorithm for 3D forward modeling is required, but the reliability and accuracy of this solution are open to question [137], as discussed in the previous section. On top of that, the accumulated errors while performing the super-positioning of the discrete simulated physical structures to-be-combined has a direct negative effect on the inverse design problem. Additionally, from the real observation point of view, ambient signal noise, spatial-configuration errors, instrument malfunction, ill-determined and poorly understood recording parameters all contribute to data inaccuracy [138]. This inaccuracy, when combined with the aforementioned resolution issues of the EM solver methods, can lead to many models that can equally fit the data within a given tolerance threshold, i.e., the problem is inherently *ill-posed* [139]. In some occasions, the trial-and-error forward modeling may be the only available tool [137].

8.2.3 An Inverse Design Attack Example: 2D to 3D Projection

Experiments that aim to test the invincibility of the NF-CoA system against the super-positioning attack have been carried out. This type of attack can be realized by using three-dimensional structures, each created as a different-ordered stack of multiple inkjet-printed 2D CoAs. The separate layers of a 3D stacked certificate are shown in Figure 84. The key point here is that all the resulting 3D structures have the same 2D projection when viewed from above, or, in other words, from the perspective of the antenna array.

The first experiment is essentially an ADS simulation, the goal of which is to compare the near-field responses extracted by a 3D metallic object to that extracted by the object's 2D projection when viewed from the top (from the perspective of the reader antenna array). This "random" 3D object that possesses the properties of copper material is shown in Figure

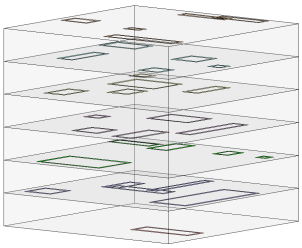


Figure 84: Separate 2D photo-paper-based layers with inkjet-printed rhombic loops that, when stacked, form a 3D NF-CoA instance.

85. The subset of S_{21} antenna couplings that are simulated are A1-D1 and C3-D1 and the results are shown in Figure 86. In the same figure, the different colors correspond to the two different couplings, the continuous lines correspond to the 3D structure and, last, the dashed lines correspond to the "squeezed" 2D projection of the same copper-based metallic object. Despite the relatively same trend, the differences in magnitude between the scattering parameter curves reaches up to 7 dBs. Of course, since the A1-D1 coupling is on the periphery of the antenna array and is "obstructed" in a significantly lesser degree compared to the centrally-originating C3-D1, the differences between the responses of A1-D1 are smaller.

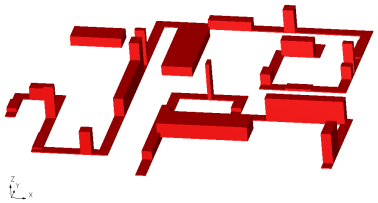
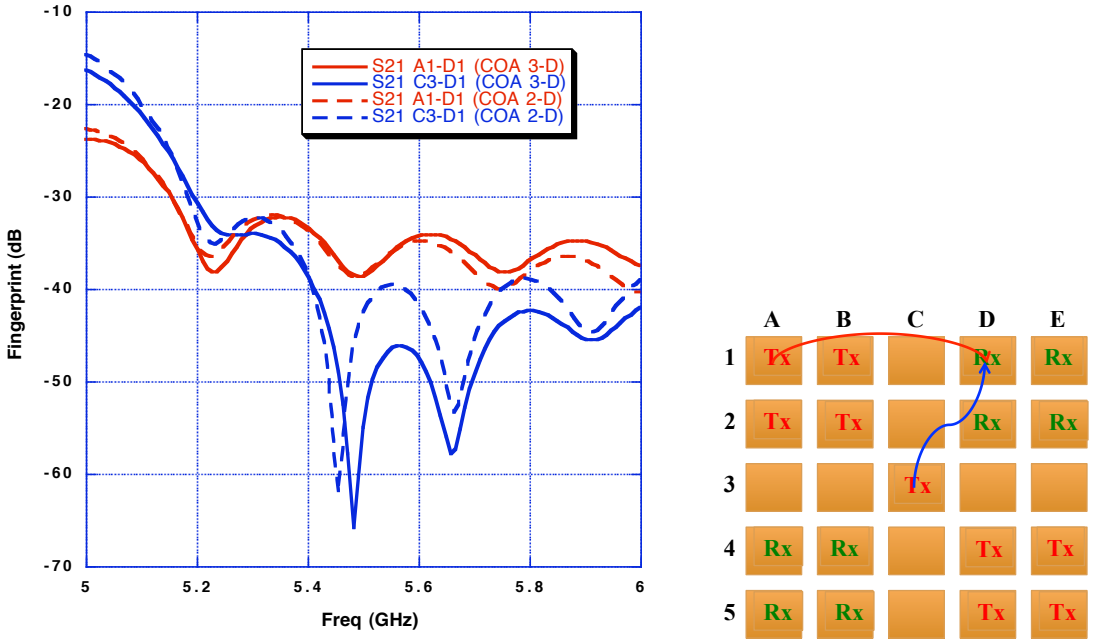


Figure 85: 3D "random" metallic structure designed and used for the simulated inverse design attack.



(a) (b)

Figure 86: Comparison between the near-field responses extracted by the 3D metallic object of Figure 85 to that extracted by the object's 2D projection over antenna couplings A1-D1 and C3-D1.

The second experiment involves the comparison between the measured NF signatures of fabricated physical certificate instances [60]. Specifically, two different sets of four 2D photo-paper-based NF-CoA designs each that consist of random constellations of silver inkjet-printed 1 mm by 1 mm pixels are used. These two sets, D1 and D2, are shown in Figure 87. The four 2D CoAs of each set can be stacked on top of each other in 24 (4!) different orders, but they always produce the same visual 2D projection when viewed from above, or equivalently from the antenna array. Given that the thickness of each photo paper sheet is 0.22 mm (8.5 mil), the resulting 3D CoA has an approximate total thickness of 0.9 mm. This meets the "three-dimensionality" design requirement of Section 4.1 and is comparable to the thickness of a regular credit card (0.762 mm or 30 mil).

First, for each set, the near-field responses of 24 different-ordered stacks of 2D CoAs are captured and the Euclidean distance between all $24!/[2!\cdot(24-2)!] = 276$ possible pairs

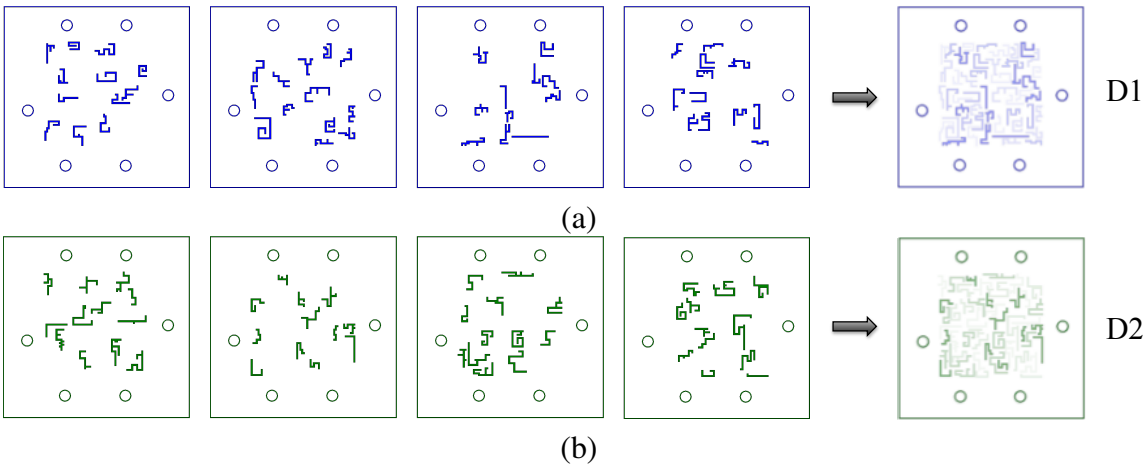
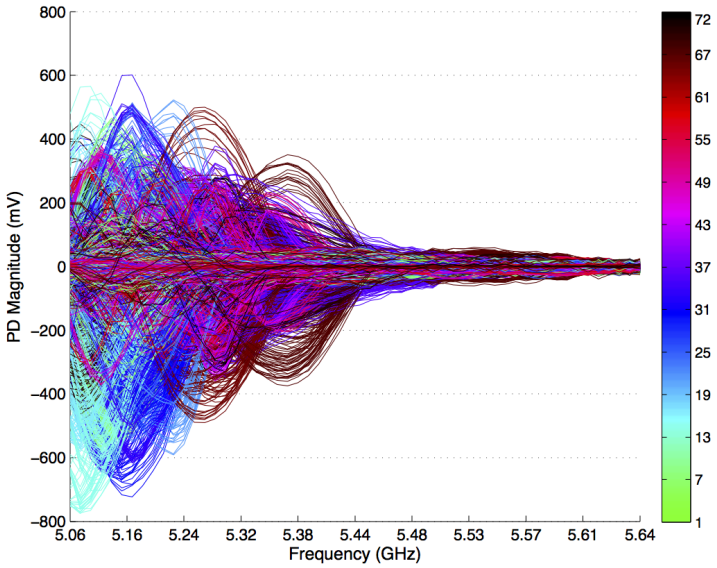


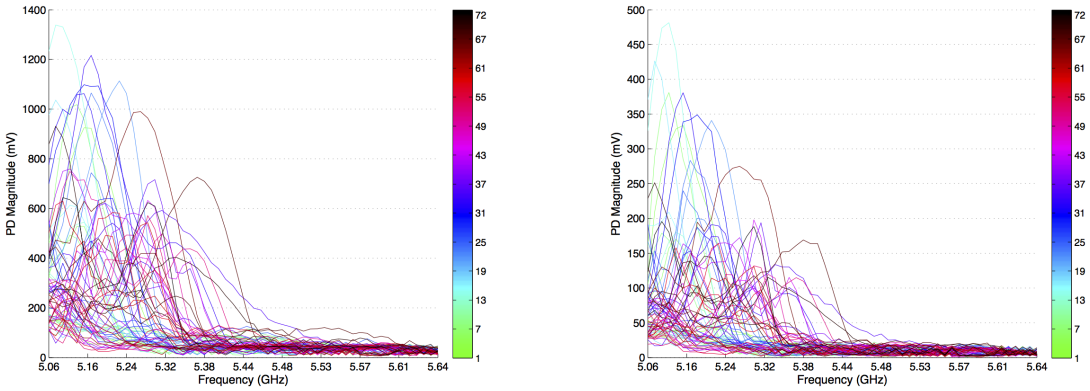
Figure 87: (a) Set D1 and (b) Set D2 of four fabricated two-dimensional photo-paper-based NF-CoA designs. Each design consists of random constellations of silver inkjet-printed 1 mm by 1 mm pixels. The resulting 2D projections are shown on the right.

of signatures are measured and shown over frequency in Figures 88a and 89a for D1 and D2, respectively. Because of the density of the curves of the 276 different sets of Euclidean distances among different stacks of the 2D certificate instances, an estimation of the range of their differentiation and their standard deviation is needed for a clearer assessment of how large the differences/distances between the signatures are. The range, i.e., difference between the maximum and the minimum of each sample, and the interquartile range are evaluated and presented in Figures 88 and 89 for D1 and D2, respectively.

The conclusion that can be drawn by analyzing these plots is that the Euclidean distances among all the available signatures are significantly large. The range, especially around the the resonant frequency of the antenna elements and also for many antenna couplings, almost reaches the dynamic range of the power detector of the NF-CoA reader with values close to 1200 mV. This result supports that even slight variations in manufacturing across the z axis, that is, the thickness of the certificate objects, which in the above two tests is on the order of less than 1 mm, will produce distinct enough NF fingerprints.

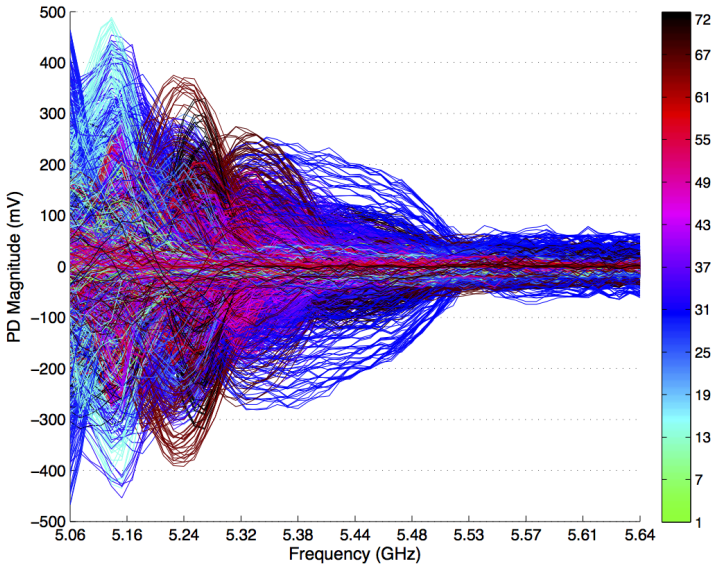


(a)

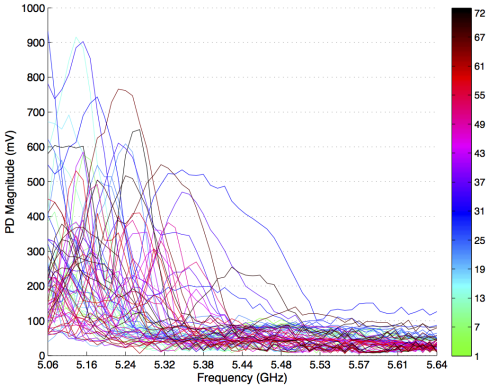


(b) (c)

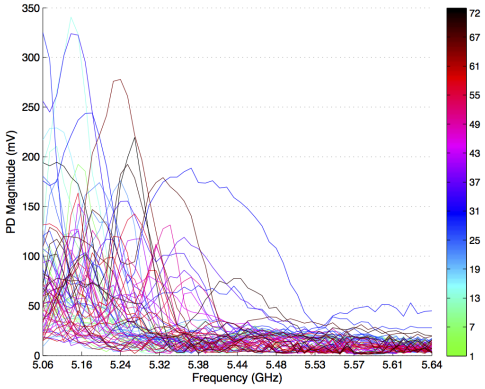
Figure 88: (a) Euclidean distances, (b) range of Euclidean distances, and (c) interquartile range of Euclidean distances between NF signatures extracted from all 24 possible different stacked orderings of the four 2D paper-based NF-CoAs yielding projection *D1*.



(a)



(b)



(c)

Figure 89: (a) Euclidean distances, (b) range of Euclidean distances, and (c) interquartile range of Euclidean distances between NF signatures extracted from all 24 possible different stacked orderings of the four 2D paper-based NF-CoAs yielding projection *D2*.

8.3 Private Key Computation

As described in Section 4.2.1, the NF-CoA issuing process relies on the use of asymmetric key algorithms that involve the use of a *public key* known to everyone and a secret *private key*. The keys are related mathematically [54], but it is virtually impossible to deduce the private key from the public key, as long as factorization of large numbers remains practically intractable [140]. This is the same kind of technology (Hypertext Transfer Protocol Secure (HTTPS) with SSL or TLS encryption) used nowadays to secure communications between a user's Internet browser and a web server of a financial institution, e-shop or government agency during e-commerce, e-banking and other transactions when the two parties need to authenticate one another [141, 142, 143].

So with public key cryptography, only the issuer can digitally sign the NF-CoA with the secret private key. Nevertheless, one potential attack could be to directly compute the issuer's private key [144]. A successful such attack would allow an adversary to ultimately create his own NF-CoA object, extract its near-field signature with a, possibly, original reader, rather than exact replica, and store and sign the fixed-length bit string f into the embedded storage chip accompanying the certificate instance (see Figure 12).

The solution to this potential attack is to make the private key computation arbitrarily difficult and time consuming by adjusting the length of the key of the public key cryptosystem deployed [140, 145, 54] at the expense of a larger amount of information stored in the embedded storage chip accompanying the certificate instance. As it is obvious from the description of Section 4.2.1, adjusting the length of the private key is totally possible. Moreover, each potential successful attack is constrained in the context of a single certifier, or in other words, of a single manufacturer. This means that only the objects of that particular manufacturer can be counterfeited. The reason for this is that the verifier's NF-CoA reader will make use of the public key of the scanned objects manufacturer. The time and effort of breaking a new private key has to be reinvested for an attack against a different certifier.

8.4 Original Signed CoA Instances Re-use

This type of attack does not apply to the cases in which the certificate instance is embedded in the protected object, such as for instance passports, cars, etc., which typically represent the upper bound of value of protected objects. Instead, it only applies to the case where the CoA is in the form of a detachable tag.

Under the later scenario, it is possible that one collects CoA instances from already sold products, attaches or embeds them on counterfeit objects that, necessarily, have the same properties, e.g. product model, color and, more importantly, serial number, with the original products, and sells the fake products as authentic merchandise.

This type of attack is eliminated in the case of the on-line authentication process, where the CoA of an already sold item has been invalidated in the central database. Regarding the offline authentication case, one way to address this problem is by destroying/devaluing the certificate object after its validation.

CHAPTER 9

CONCLUSIONS

The research work presented in this dissertation has involved the design and realization of a novel standalone wireless robust system that inherently exhibits enhanced authentication and anti-counterfeiting capabilities. The system consists of two major components, namely the near-field certificates of authenticity (NF-CoAs), which serve as authenticity vouchers for the products to which they are attached, and a microcontroller-enabled, low-power, and low-cost reader.

This work embarked on describing the many-fold rationale behind focusing on the near-field observation of the electromagnetic phenomena of reflection, refraction, diffraction and, most importantly, scattering. The boundary values of the electromagnetic regions of the space surrounding the miniature antenna elements deployed have been determined following the two most popular theoretical approaches. Leveraging the unique near-field scattering properties and the complexity of the incurred electromagnetic effects, especially when the latter are viewed under the prism of a thorough literature survey, highlights the important qualitative features not exhibited by related anti-counterfeiting techniques.

Two different types of NF-CoA instances that yield unique and highly-divergent NF fingerprints have been studied and realized following a design and fabrication strategy that has allowed for control over their properties, as well as randomness. The first category includes three different sets of two-dimensional geometries inkjet-printed with conductive silver nano-particle-based ink on regular photo paper layers that are stacked one on top of each other. The second type includes three different sets of copper-based CoAs of varying mass per meter, namely 2, 3 and 4 grams per meter. Very simply, these copper-based instances are created by immersing and fixating randomly entangled and squished metallic hair into a dielectric substrate, the thinnest dimension of which should be substantial (e.g. 0.75 mm). Regardless of the type, the entire life cycle of a certificate instance, spanning

from the fabrication process (issuing) to the point where it is used for identity validation or genuineness authentication (verification process), has been outlined.

The design and fabrication of the NF-CoA reader that is used to expose the subtle variances of the near-field electromagnetic effects, which result from the impingement of electromagnetic energy on a certificate instance, has evolved over three different generations of mixed-signal boards. The full characterization of all hardware components comprising the reader, with an emphasis on accuracy and insertion loss introduced, as well as the operating details of the three generations have been described. During the design of the first generation of the NF-CoA board reader, the attention was almost exclusively concentrated on the super-high-frequency plane. The operation of this first prototype implementation was assisted by an external data acquisition board. The most important advancements brought by the second-generation board was the computationally more powerful MCU-controlled operation of this board for the first time with an external board, the optimal coverage of the contiguous 5.0 to 6.1 GHz frequency spectrum by using two distinct VCOs, and the decrease by 16% in the overall dimensions. This has provided not only a very fast means of capturing each fingerprint, but also the accuracy required toward an effort to maximize the resulting entropy. The third and last generation did not make use of an external data acquisition board. Instead, a big leap toward unifying the super-high-frequency plane and the digital control plane and integrating them on a single board has been achieved. This is the first standalone reader. This design has necessitated special care to maintain isolation of EM interference between digital and analog circuitry, so as to preserve the signal integrity of the NF fingerprint and to produce a firmware code that complies to the timing characteristics of all the components across the signal path. The operational state diagram of the algorithm implemented by the NF-CoA reader has also been discussed and illustrated.

A wide array of tests have been conducted to assess the feasibility and performance of the proposed authenticity certification technology. Physical objects that belong to both

aforementioned categories and that are conceptually very close to the final envisioned certificate instance have been tested. As a very first step, it was verified that the close proximity of an NF-CoA to the antenna array of the reader does significantly disrupt the NF response by almost $2/3$ of the overall dynamic range of the power detector of the reader. Next, the dependence on the distance between the antenna array and the certificate instance was examined. The dependence on the size of the lateral two-dimensional area was also studied by evaluating the difference between the responses of different-sized copper-based certificates. In the context of this same test, it was important to verify that the entropy produced by the smaller-sized certificates was more than adequate. Additionally, the effect of the amount of conductive material density in the three-dimensional structure of the NF-CoA to the entropy of its frequency response was investigated by comparing copper-based CoAs belonging to families with different mass per meter. The first most crucial test was the intra-CoA robustness test, which ensures that the same certificate instance always yields nearly exact replicate signatures. The results have led to the conclusion that the differences are located in the neighborhood of the noise floor of the power detector and/or the analog-to-digital converter of the micro-controller unit and that indeed nearly identical signatures are finally extracted. Based on this same test, the similarity detection threshold has been established to be equal to the low power level of 1 dB. This level of accuracy takes on even higher importance if one considers that the linearity error exhibited by the power detector used was ± 1 dB. In other words, the maximum intra-CoA difference measured is equal to the physical detection limit of the underlying hardware. The second most crucial test to conduct was the inter-CoA robustness test, which demonstrates the uniqueness among signatures extracted from different NF-CoA instances. The range of the signature differences almost reached the dynamic range of the power detector of the reader. Finally, the shielding capability of the NF-CoA system against interference by nearby conductive and dielectric material, for instance when NF-CoAs are attached onto computer laptops, aircraft spare parts, pharmaceutical liquids, etc., has been assessed. Specifically, three different tests

were conducted that involved the proximity of three different types or sizes of metallic surfaces brought close enough to the certificate instances. The results clearly indicated no detrimental effects on the entropy of the produced signatures.

Attempts to empirically quantify the entropy, or uncertainty, of the signatures generated by the NF-CoA system have been made. The term "empirically" here accentuates the fact that real measurements, i.e., bit sequences representing the digitized extracted EM signatures from all the available certificate instances, comprised the entirety of the data worked upon. The certificate verification procedure is a *binary classification* problem. As such, the analysis in the first attempt, following the principles of basic detection theory, employed the concepts of hypothesis testing, probability density functions and receiver operating characteristic curves. The probability that the NF-CoA system predicts a fake CoA as authentic or predicts an authentic CoA as fake is inconceivably small; on the order of 10^{-200}. The near deterministic and highly entropical performance of the NF-CoA system is also verified by the existence of a point on the receiver operating characteristic curve that almost corresponds to the $(0, 1)$ "perfect classification" point for a certain detection threshold δ_T. As an independent corroboration for the above finding, empirical evidence has also been provided by conducting randomness testing based on one of the most stringent and highly regarded, by industry and research community alike, test suites, the National Institute of Standards and Technology Statistical Test Suite (NIST STS). This battery of independent and computationally intensive statistical tests attempts to algorithmically identify binary digit sequences that do not behave in a truly random manner and, as expected, are widely preferred for analyzing cryptographic random number generators. The deduced inherent unpredictability of the NF-CoA system, scoring "success" for the majority of the tests, takes on an even higher importance if one considers that no pre- or post-processing of the bit sequences, no consecutive or interleaved multiple refeeds of the bit sequences and no Von Neumann or any other corrector has been applied and no optimization departing from the default NIST STS parameters has been pursued.

Finally, the security nature of the NF-CoA system and the consequent benefits from forging an identity or counterfeiting NF-CoA protected objects have rendered it imperative to identify and formulate the key potential attack problems. An example of a real attack that was launched and how the NF-CoA system could withstand it is included. Of course, the investigation of these attacks has been complemented by an analysis of how these are effectively blocked.

On top of the main functionality of the NF-CoA instances, a localization service has been provided for location estimation of the NF-CoA instances. This service is presented in the Appendix and is based on the multi-lateration received signal strength indicator (RSSI) based localization technique when the certificate instances are coupled with a battery-less solar-powered wireless connectivity module. Two different real-world WSN-enabled localization testbeds have been set up and the experiments conducted have yielded very satisfactory results.

In conclusion, the robustness of the NF-CoA system with virtually not a single false alarm in one's lifetime, the fast and versatile certificate signature extraction, the small profile of the certificate instances, and the reader's very low cost, low-power operation and wireless data relay provisioning are among the characteristics that make it applicable to a vast array of physical objects that needs protection against counterfeiters.

9.1 Summary of Contributions

Within the context of the inter-disciplinary research work presented in this dissertation, significant aspects of the near-field certificate of authenticity anti-counterfeiting system have been brought from paper to reality. A novel standalone wireless robust system with exceptional hardware-enabled authentication and anticounterfeiting capabilities has been realized following a bottom-up approach (tag/instance $\Rightarrow$ reader $\Rightarrow$ algorithm $\Rightarrow$ networking $\Rightarrow$ system).

- Designed and realized two different types of novel ultra-low-cost certificate instances

of enhanced randomness following a design and fabrication strategy that has allowed for better discrimination/performance control (stacked 2D inkjet-printed paper-based), as well as higher randomness (random copper-based).

- Designed, fabricated and fully characterized the first three generations of low-power and low-cost readers of the NF-CoA system utilizing "mix-and-play" antenna array coupling configurations. The latest generation represents the first standalone micro-controller-enabled reader.

- Developed a power-efficient algorithm for the fast and accurate NF fingerprint extraction that complies with the timing characteristics of all the components across the signal path.

- Conducted a wide array of tests to assess the feasibility and performance robustness of the system.

- Evaluated and determined the similarity detection threshold to be in the vicinity of the boundaries of the physical limitations of the reader hardware.

- Quantified empirically the entropy, or uncertainty, of the signatures generated by the NF-CoA system and verified the near deterministic and highly-entropical performance of the NF-CoA system by demonstrating the existence of a point on the receiver operating characteristic curve that almost corresponds to the $(0, 1)$ "perfect classification" point for a certain detection threshold δ_T within the context of the binary classification problem of the verification procedure.

- Supported the feasibility of the "null hypothesis" of the NF signatures being potentially generated by a true random number generator by conducting and passing the majority of the tests of one of the most stringent and highly regarded, by industry and research community alike, test suites, the National Institute of Standards and Technology Statistical Test Suite (NIST STS).

- Launched a real super-positioning inverse design attack that the NF-CoA system successfully withstood.

- Built the first two real-world WSN-enabled multilateration localization testbeds to evaluate the provision of an accurate location estimate of the certificate instances.

In Fall 2011, this research work was listed among the 25 technologies in all categories featured in the 20-year anniversary issue of Microsoft Research, Redmond, WA [146].

9.2 Directions for Future Research

While the architecture of the NF-CoA has been realized and the feasibility and robustness of this research work have been demonstrated, there is a number of research topics that can originate from this work and complement it. First, a mixed-signal design and development effort to integrate all the, currently, discrete components of the reader in a single die could be invested. This could provide a thrust toward the goal of massively producing NF-CoA readers.

Moreover, the design of novel curved, but fixed, antenna arrays that could support the near-field signature extraction of CoA instances attached or embedded onto cylindrical surfaces could be sought. This would widen even more the range of the possible applications, a prominent one being the package sealing of physical objects.

Another promising topic could be the addition of a phase detector and the expansion of the list of candidate materials for fabrication of the certificate identifiers to include non-linear materials, such as *ferrites* and *metamaterials*. This would effectively render the inverse design problem even more complex.

APPENDIX

APPENDIX A

ENABLING LOCALIZATION FOR THE NF-COA SYSTEM

The parameter that eventually plays the major role in choosing a particular localization technique is the ease of deployment in a new or an existing wireless network infrastructure. This involves the existence of a real-world implementation of a technique with low hardware complexity, low or no packet transmission overhead, low cost, and minor limitations. As for the hardware complexity, for instance, solutions based on the RSSI multilateration require only minor software module additions, whereas the lighthouse solution [147] requires the installation of quite complex anchor nodes with rotating mirrors and laser diodes.

In the framework of this dissertation, the goal is to provide a very low-cost localization service to the NF-CoA system with a satisfactory accuracy. Toward that direction, a batteryless, solar-powered wireless module is coupled with any of the developed NF-CoA instances and, by simply broadcasting identical, unique identification packets in regular intervals, does rely on the multilateration localization technique. This effort is presented in Section A.2.

A.1 Wireless Sensor and Ad-Hoc Networking

The capability of gathering, storing, and processing large amounts of data collected from tiny sensors, including the NF-CoA instances, in a centralized, efficient and low-cost way without involving the human in the loop is becoming more and more critical as we move on to the ubiquitous cognition era of the *Internet of Things* [148]. The ultimate objective is to be able to extract the sensed information not only over long wireless ranges but even from the other side of the planet.

The solution to this problem can be the deployment of Wireless Sensor Network (WSN) nodes in-between prototype sensors and the Internet, replacing existing RFID readers which are not only much larger in size than typical WSN motes but also two orders of magnitude more expensive. The bridging of the world of the sensing devices and RFIDs with that of WSNs brings in the spotlight the new area of ubiquitous wireless networks, which can provide truly cognitive intelligence over extended physical distances on top of very low-cost and mature wireless infrastructures. The motes comprising a WSN are mesh interconnected with wireless links and are capable of relaying messages to a sink, as graphically depicted in Figure 90. Under this approach, the WSN motes are not anymore the lowest-level network devices in the infrastructure hierarchy; their primary task is not as *data generators*, which role is almost entirely taken over by the sensors, but as *data routers* that relay the sensed information through wireless multihop links to one or more gateways.

For the NF-CoA reader and instances presented in the previous chapters to be able to connect to a WSN infrastructure that interfaces with the Internet, both sides are required to "speak" the same protocol language. From the networking *Open Systems Interconnection* (*OSI*) reference layer design [149] perspective, this means that not only should there be *physical layer* (*PHY*) compliance in terms of the RF transmission from the reader or instance but also the transmitted packet has to implement the proper *link layer* (medium access control (MAC)) encapsulation, as described in the following subsections.

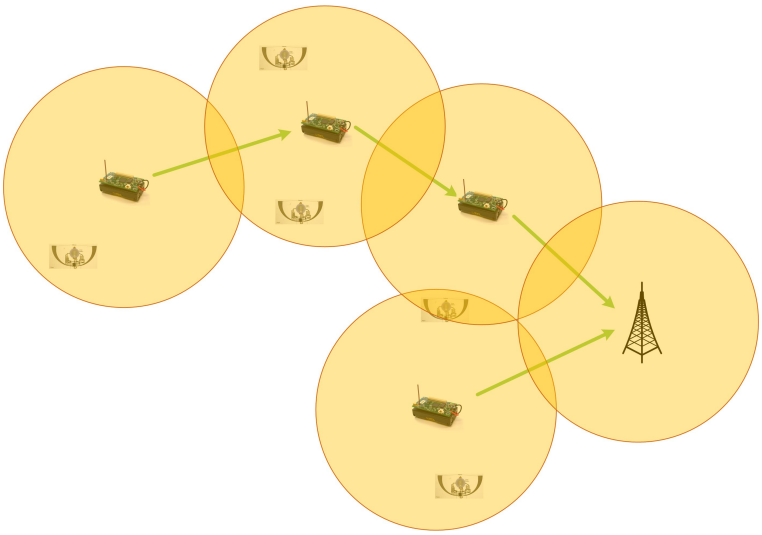


Figure 90: An example of a *wireless sensor network* (*WSN*) topology, where the WSN motes are not anymore the lowest-level network devices in the infrastructure hierarchy.

Although communication between the wireless connectivity module of the NF-CoA instances and the very popular commercial MICA2 WSN mote [150] has been successfully established as described below using a very simple but power-efficient protocol, the role of the WSN mote can also be assumed alternatively by 802.15.4/Zigbee nodes, DASH7 nodes, Oracle Sun Spot nodes and others.

Within the multihop context of a WSN, instead of transmitting high-strength signals over long single-hop wireless links, it is more power efficient to relay packets a number of times over lower-strength shorter links [151]. This decreased power consumption of the radio transmission results in increased power efficiency of both the NF-CoA wireless module the WSN node operation. At the same time, as long as the WSN nodes are located within direct radio range of others, hopping effectively extends radio communication over higher ranges overcoming non line-of-sight and path loss effects. Moreover, their multipath topology is inherently self-healing allowing the network functionalities to be sustained without any interruption because of potential WSN node failures.

A.1.1 NF-CoA Instance Wireless Connectivity

The main functionality of the MCU-enabled NF-CoA wireless connectivity module [152], shown in Figure 91, is the wireless broadcast transmission of identical, unique identification packets in regular intervals triggered and powered using energy present in ambient sunlight without a conventional battery. As expected, the parameters governing the performance of the module are the effective isotropic radiated power (EIRP), the total transmit time and the time interval between adjacent transmits.

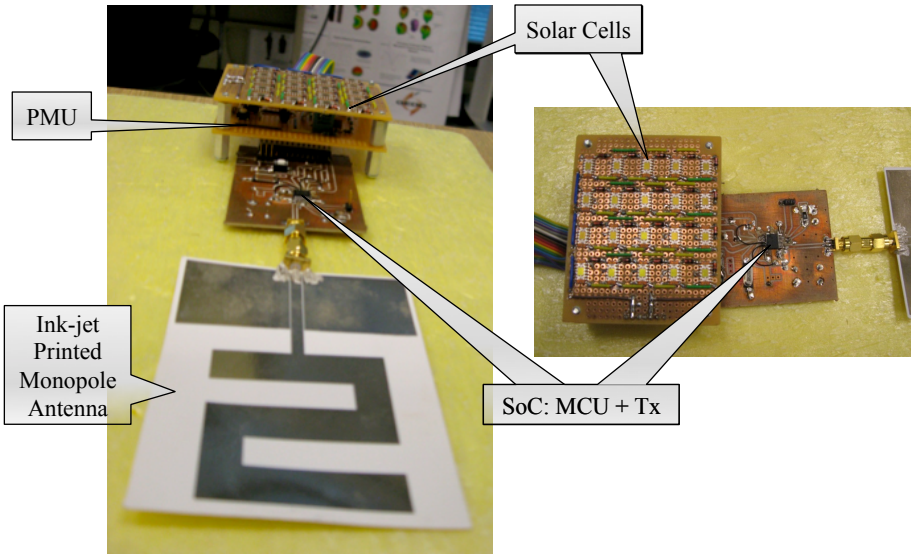


Figure 91: The NF-CoA wireless connectivity module.

This module utilizes super capacitors, which are much cleaner to dispose environmentally, have a lower voltage charge threshold and have much higher recharge lifetimes than batteries. These super capacitors are charged by the unlimited and clean solar energy harvested by a parallel configuration of GaAs solar cells interfacing to the tag through a power management circuit (PMU), which is in turn interfaced to the integrated 8-bit MCU housed in the same chip as the RF transmitter. The MCU transits from "on" to "sleep" mode and vice versa with the help of the PMU based on the amount of the solar energy collected across the charge tank capacitors. The power management unit is comprised of discrete analog circuitry. The module firmware ensures that the unique identification packet is

transmitted using the same RF power irrespective of the external light conditions, thereby ensuring that the EIRP from the tag remains the same within the area, where it is being tracked. In order to support *Frequency Shift Keying* (*FSK*) modulation, passive components are introduced to enable pulling of the phase-locked loop (PLL) crystal by a controlled amount by the MCU thereby modulating the RF output going into the antenna with respect to the frequency.

Since the packet transmissions have been observed to suffer from bit errors, the rate of which depends on the characteristics of each wireless environment, *cyclic redundancy checks* (*CRC*) are performed. As the name implies, no error correction or recovery is provided but only error detection. Additionally, the bit errors between the module and the WSN receiver are noticeably minimized by calibrating the PLL of the module so that its modulation profile around the center frequency is very closely matched to that required by the receiver Mica2 motes. This calibration also has the added advantage of requiring fewer preamble bits for the receiver to bit synchronize with the tag for Manchester bit encoding [153], which, given the limited amount of power available per energy duty cycle, can be useful.

The radiated power has to be omni-directional for the purpose of an accurate localization computation. Omni- directionality is achieved by ensuring an antenna gain close to 0 dB. The Z-shaped monopole antenna design [154] is fabricated on paper using in-house inkjet-printed technology and is shown as part of the working prototype in Figure 91. The antenna design is tweaked to ensure that its impedance is equal to $(36.95 - j71.77)\,\Omega$ [155], which is the conjugate of the optimum load impedance of the amplifier in the wireless transmitter of the module prototype. This matching ensures that almost the whole amount of the solar power harnessed is radiated out from the amplifier into the antenna as RF power.

The time to transmit one set of data packets was about $9ms$, which, given that the total transmit time available for a charge tank capacitance of 637 μ F is 43.23 ms, allows for transmission of at least four sets of data packets per energy duty cycle [152].

A.2 NF-CoA Instance Localization

Localization is the process of determining the physical position of a user or a device with a particular degree of accuracy in indoor or outdoor environments. The need for truly cognitive localization intelligence over extended physical distances on top of very low-cost and mature wireless infrastructures is ever increasing. The physical location information of a node can be a very useful or even indispensable functionality in a large number of applications, such as device tracking, involving location and bearing, geographic aware routing protocols and context- aware ubiquitous applications.

This section demonstrates the implementation of a very low-cost localization and device tracking system for the NF-CoA system on top of a *Wireless Sensor Network* (*WSN*) topology. Its major components are the NF-CoA wireless connectivity module, the fixed wireless infrastructure and the central localization server. The first component has been presented in Section A.1.1. The latter two components of the NF-CoA localization system are described below and an evaluation of the accuracy of the system is presented.

A.2.1 Lateration as the Localization Technique

The localization technique deployed is the *Received Signal Strength Indicator* (*RSSI*)-based lateration. *Lateration* is the approach according to which distances from three (*trilateration*) or more (*multilateration*) anchor nodes, whose exact absolute location coordinates are known a priori, are used to estimate the node location. The estimated position is given either relative to these anchors or to absolute coordinates, provided that the absolute coordinates of the anchor positions are known.

The RSSI returned by a register of an anchor's transceiver after the successful reception of a packet from another node can serve as an estimate of the physical distance between them. In particular, the distance from the emitter can be estimated by plugging this RSSI value along with the known *effective isotropically radiated power* (*EIRP*), which takes into account the transmission power, the antenna gain and the cables losses of the emitter, into the Friis equation [50]. For the latter equation a particular path loss coefficient and model,

which is most suitable to the actual surrounding environment, has to be chosen; in the NF-CoA localization system for an open area environment that can be the *two-ray ground reflection model* [156].

The two main characteristics that render this localization method attractive are that:

- neither additional hardware is required
- nor additional communication overhead has to be carried out.

However, there are a few factors that can degrade the accuracy of the RSSI-based approach:

- incorrect estimations are introduced when the RSSI is extracted from packets which have followed an indirect path as a result of multipath fading [157], regardless of whether or not they have been emitted from an anchor node in line of sight with the receiver
- the fast-fading effect, as well as the dynamic nature of the environment, can result in serious variations in the RSSI measurements over time
- since the widely used inexpensive radio transceivers are in most cases uncalibrated [158], the actual transmission power and returned value of RSSI for the received data can differ from the configured one and the measured RSSI value might not correspond precisely to the actual received signal strength

Nevertheless, the rather painful, and for some application environments impractical, process of calibrating every node in the network can entirely eliminate these latter problems. In the framework of this work, efforts to alleviate the above degrading effects have largely been made before the trilateration is conducted. First, rigorous mapping of the RSSI values recorded at fine grained set distances from an anchor node and for known transmit power are conducted. Additionally, in order to remove the signal noise, the RSSI data is

passed through Kalman filtering [159] with the use of appropriate procedure language *R* functions [160], as discussed in subsection A.2.2.2.

A.2.2 The Overall System/Solution

The three major components that comprise the overall system, namely the NF-CoA wireless connectivity module, the fixed wireless infrastructure and the central localization server, have been designed to inter-operate as efficiently as possible.

A.2.2.1 The fixed wireless infrastructure

The key decision that has enabled the cost of the proposed localization solution to be drastically low is the deployment of a *Wireless Sensor Network* (*WSN*) as the backbone infrastructure, instead of RFID readers which are not only much larger in size dimensions than typical WSN motes but also two orders of magnitude more expensive, and the successful establishment of an asynchronous communication link between a WSN node and the wireless connectivity module presented in the previous subsection. The motes that comprise the WSN topology are the Crossbow Mica2 [150], shown in Figure 92; one of the most popular, inexpensive and widely used WSN motes as of the time of this writing.

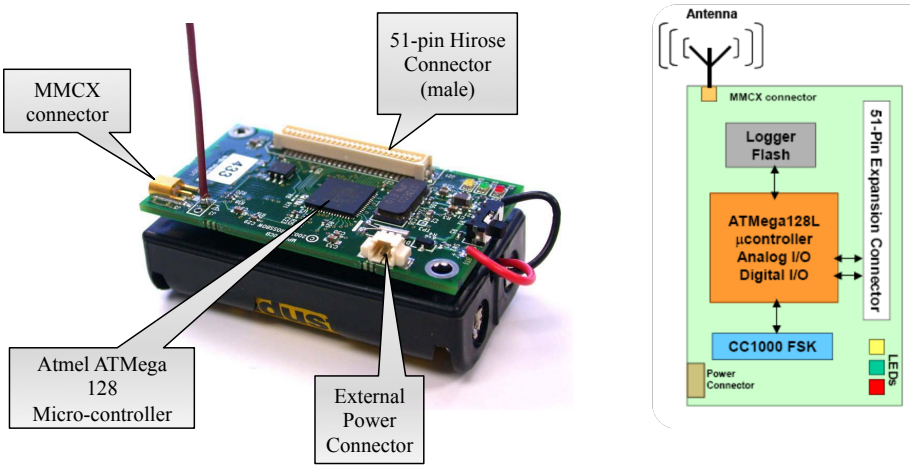
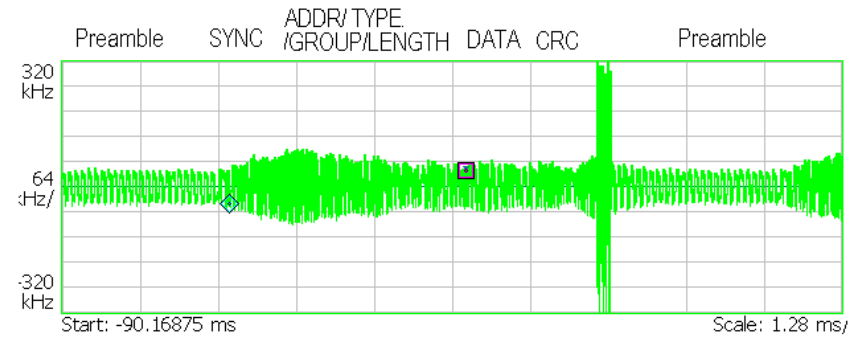


Figure 92: The Crossbow Mica2 serving as the wireless sensor network anchor node for the NF-CoA localization system.

For the WSN infrastructure to be able to capture packets transmitted by the connectivity modules and to extract the unique NF-CoA instance identity number and received signal strength indicator in dBm scale before forwarding them to a central server, both an anchor and an end node are required to "speak" the same protocol. Regarding the *physical layer*, first the transmission has to be carried out over a frequency channel supported by both sides, which in this case is 904.4 MHz and belongs to the unlicensed *ISM* (*Industrial, Scientific and Medicine*) band, and second the transmitted signal has to be modulated with FSK meeting specific frequency and modulation requirements. In regards with the *link layer*, the WSN mote is expecting the packet to be properly encapsulated before extracting the payload, which is the actual information carried. This "overhead" is not only used for communication protocol purposes but can provide topology-related knowledge and error handling functionality. More specifically, the format of the packet sent from the tag, which is received by the TI CC1000 transceiver [161] of the WSN node, consists of the following fields: *Preamble, Sync, Addr, Type, Group, Length, Payload, and cyclic redundancy check* (*CRC*). The wireless data sequence of a whole 9 ms packet broadcasted by the NF-CoA wireless module as captured with a real-time spectrum analyzer over time is shown in Figure 93. The first two fields are used for the synchronization of the receiver's clock and the latter field, namely *CRC*, helps eliminate bit errors occurring within the sent bit sequence by successfully recognizing a corrupted packet and discarding it. The *Payload*, of course, conveys the unique identifier of the NF-CoA instance.

As opposed to the plain Assembly code developed to program the NF-CoA wireless connectivity module , the Mica2 motes were programmed with NesC [162] code, a variant of *C* code that represents in this case the *middleware*.

From the wireless radio propagation perspective, the WSN setup is carried out to allow the WSN nodes to better receive the end node transmitted data, which eventually results into a better localization estimation. The requirement for the clearance of at least the 80% of the first Fresnel zone [34] is satisfied in most cases for the anchor nodes that are in line of

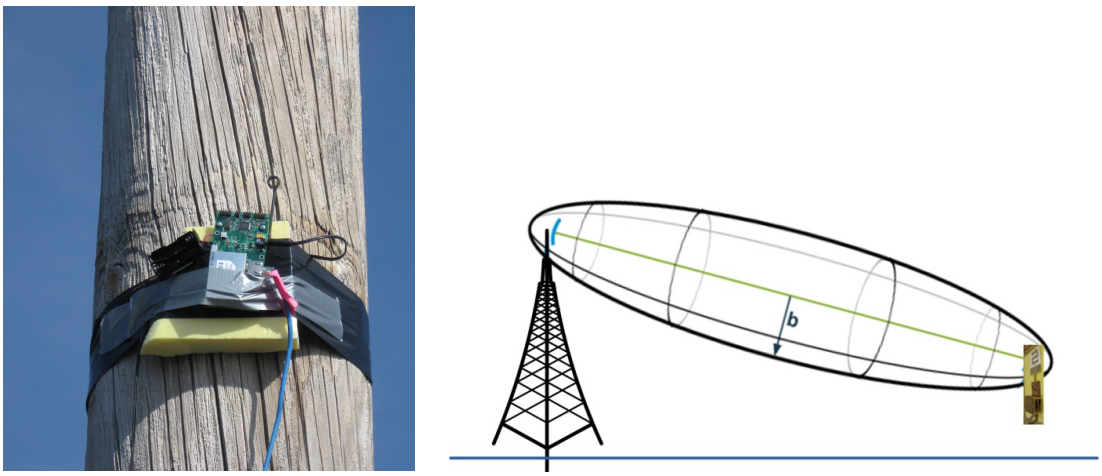


Preamble	Sync	Addr	Type	Group	Length	**Payload**	CRC

Figure 93: The wireless data sequence of a whole 9 ms packet broadcasted by the NF-CoA wireless module as captured with a real-time spectrum analyzer over time.

sight with the communication module. The Mica2 nodes that form the WSN are mounted on lamp posts; an example is shown in Figure 94a. The average height of the motes above the ground is 3.5 m and the height of the end device is around 1.5 m, the value of the radius of the cross section of the ellipsoidal of the first Fresnel zone at the middle of the distance, typically 75 m, is approximately 2.8 m and the same value just 0.5 m away from the mote side is around 0.3 m. The drawing of Figure 94b can help visualize the radius of the cross-sections of this ellipsoidal volume.

After the successful reception from a number of WSN anchor nodes of the beacon message broadcasted by the end node, essential information, namely RSSI and unique anchor identity number, is appended to the packet and forwarded to the localization central server, presented in the next subsection, through either the XMesh [163], a fully featured multihop, ad hoc, mesh routing protocol, or over an overlay 2.4 GHz IEEE 802.11 wireless local area network consisting of three Linksys WRT54GL access points; one connected to the central server and the other two connected through UTP cable to each of the eight Mica2 motes, the Ethernet interface of which was provided by an additional daughter-board. As is the case with any wireless network, the purpose of the cost metric is to minimize the total cost it takes for any mote to transmit to the base station. It is important to note that, instead



(a) (b)

Figure 94: (a) A wireless sensor network anchor node mounted on a lamp post, (b) Sketch of the ellipsoidal surface of the first Fresnel area between the transmitting NF-CoA wireless connectivity module and the wireless sensor network anchor node.

of hop count which is the traditional distance vector routing cost metric, XMesh [163] uses the minimum transmission cost metric, which minimizes the total number of transmissions in delivering a packet over multiple hops to a destination.

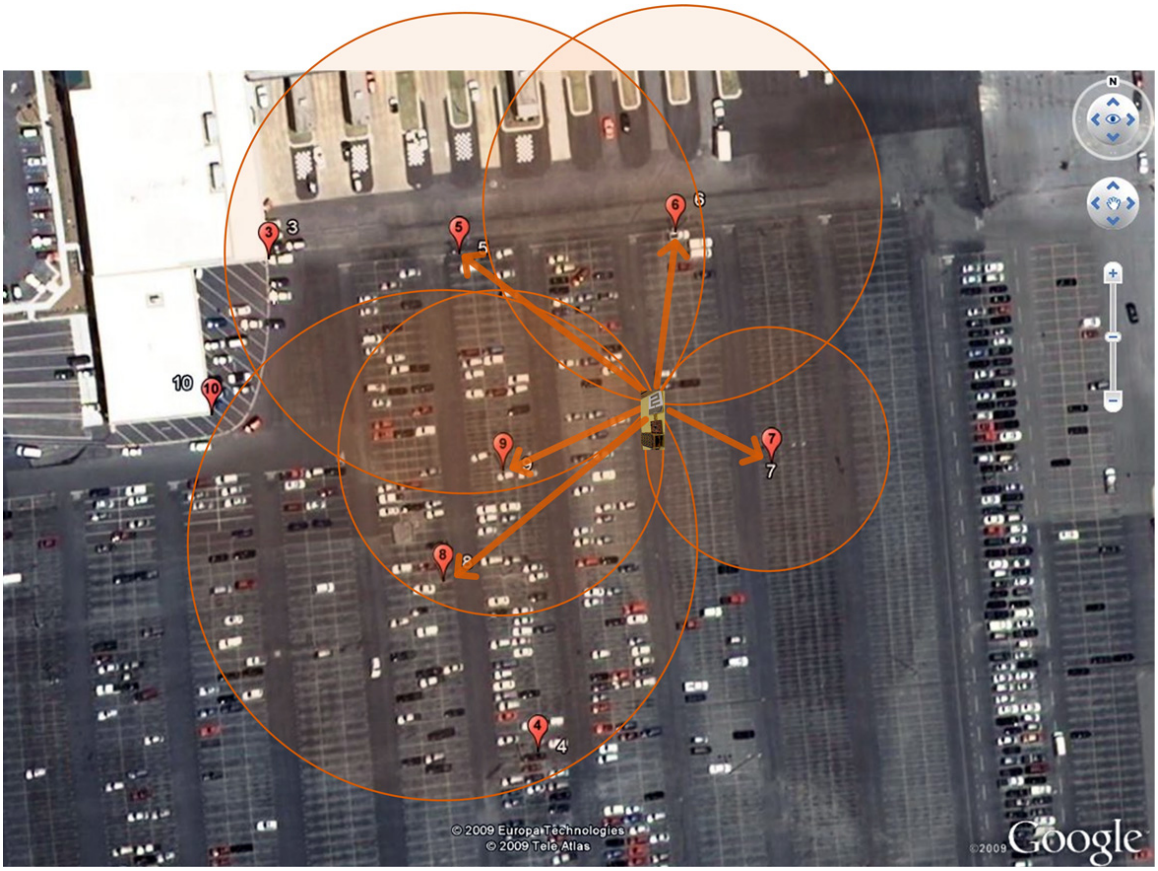


Figure 95: The multilateration localization technique as conducted in a real-world large parking lot environment that is RF covered by a wireless sensor network. Identical unique identification packets are broadcasted by the NF-CoA wireless connectivity module and captured by multiple fixed anchor nodes for multilateration purposes.

A.2.2.2 The Central Localization Server

The RSSI measurements captured by the anchor nodes from the broadcasted packets are pooled on a central computer where they were selectively parsed for computations that estimate the location of the NF-CoA instance. All the packets forwarded from the anchor nodes, as described above, are time-stamped as they arrive at the central server location and are imported as message entries into a Sqlite database of the lateration application [164].

Data validity checks are the first type of process performed to the message entries, i.e., a number of filters are applied to reject invalid entries as a result of, mainly, bit errors introduced. Then the RSSI data, after it is filtered for bit sequence inconsistencies, is extracted and passed through Kalman filtering [159] with the use of appropriate procedure language *R* functions [160, 164] in order to remove any signal noise present. Moreover, the transceiver calibration issues revealed previously are dealt with the conductance of separate test measurements right after the deployment of the anchor nodes. Specifically, RSSI values recorded at fine grained set distances from an anchor node and for known transmit power are rigorously mapped for different field wireless propagation profiles; for example, for different percentages of occupation of the parking lot by vehicles.

Since the localization solution is based on the RSSI-based lateration technique, the filtered RSSI data is used for the distance estimation between the tag and a particular WSN node with the use of a two-ray tracing radio propagation loss model. The time-stamp information availability enables the use of a timer function, which loads data from specific time periods back in the past relative to the time the location estimate is initiated. Finally, the multilateration is performed as a database procedure call [164] and in turn functions are called to display the returned *WGS 84 latitude-longitude* coordinates on the *Google Earth* [165] application.

A.2.3 Experimental Results

In order to verify the feasibility of this proposed solution for the remote localization and position tracking solution for the NF-CoA system, actual measurements of the location estimate errors are taken at different positions of the instance in two different real-world fields, covered by fixed WSN anchor nodes. This location estimate error is equivalent to the Euclidean distance between the estimated absolute coordinates returned by the program and the coordinates of the actual position of the NF-CoA instance. The first one is the rooftop of the Georgia Tech hotel's parking deck and the second one is a large car auction dealer's parking lot in Southern Atlanta, right next to the Atlanta Hartsfield Airport.

Both WSN topologies are designed to allow the WSN anchor nodes, which are mounted on lamp posts, to better RF cover and receive the transmitted data by the tag, which results in better localization estimates. The NF-CoA instance is hung from the rear mirror of a vehicle that is driven around at different positions of the fields to verify and benchmark the returned location estimations.

A.2.3.1 The Georgia Tech Hotel's parking deck rooftop

The satellite image of the 80 m × 80 m area of the rooftop of the empty of the parking deck of Georgia Tech Hotel is shown in Figure 96. Six WSN anchor nodes are mounted, as described previously, on existing lamp posts that are denoted with increasing numbers "3" through "8". Four of them are placed on the periphery of the topology and two of them around the center.

Two localization estimate examples returned in Google Earth, namely *hhr-estA* and *hh-estC*, are pinpointed in Figure 96 and can be compared to their respective real position, denoted with the car icons *A* and *C*, respectively.

A.2.3.2 A large parking lot

The WSN topology consists, in this case, of eight anchor nodes that are denoted by the red pins numbered "3" through "10" in Figure 97 and the placement of which resembles to an asterisk topology. The diameter of the area covered by the overall topology is around 190

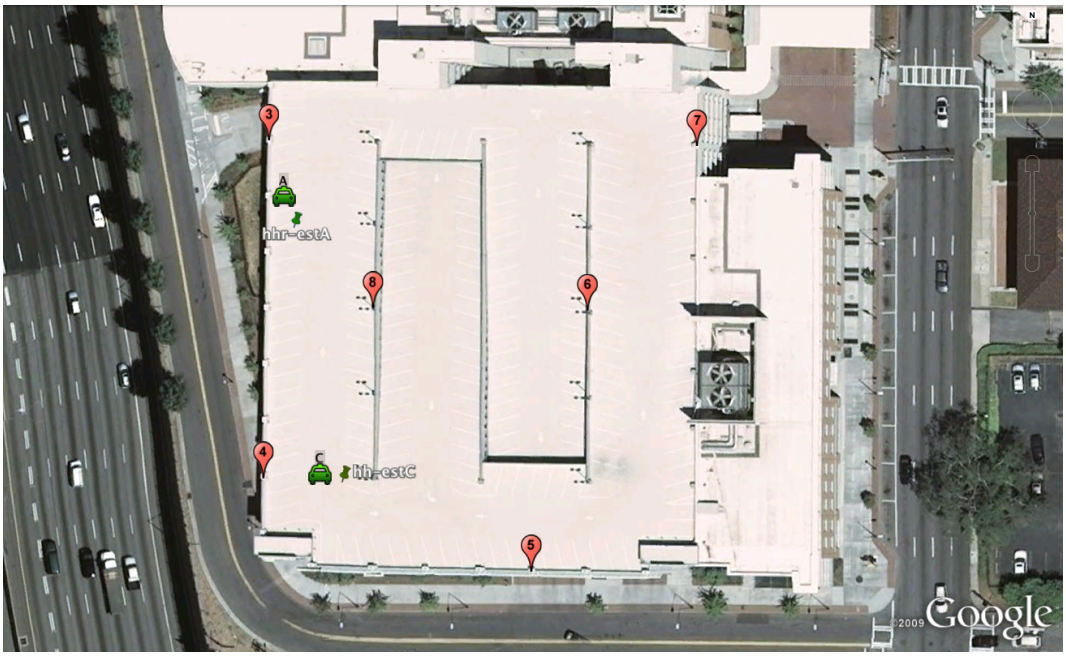


Figure 96: The WSN topology and measurement positions on Georgia Tech hotel's parking deck rooftop.

m, and the radius of the area RF covered by each anchor node is roughly 90 m. Consequently, the percentage of the overlapping areas within the overall field is high, as desired.

The green car icons correspond to 24 different predetermined positions from which an attempt to estimate their location is made so as to get an initial evaluation of the performance of the localization system.

Two examples of the localization estimates returned in Google Earth and compared to their real placement are shown in Figure 98. The mean, maximum, and minimum estimate errors are summarized in Table 9. It is worth noting that the average error is reasonable when the transmitter tag is located in an area around the center of the topology. In contrast, the location estimate error increases as the transmitter moves more toward the periphery or even outside of the topology, where optimal coverage by multiple anchor nodes is not provided. This latter value, nevertheless, needs not been taken into consideration as the NF-CoA transmitting module will always be considered to move in an area that is optimally RF covered.

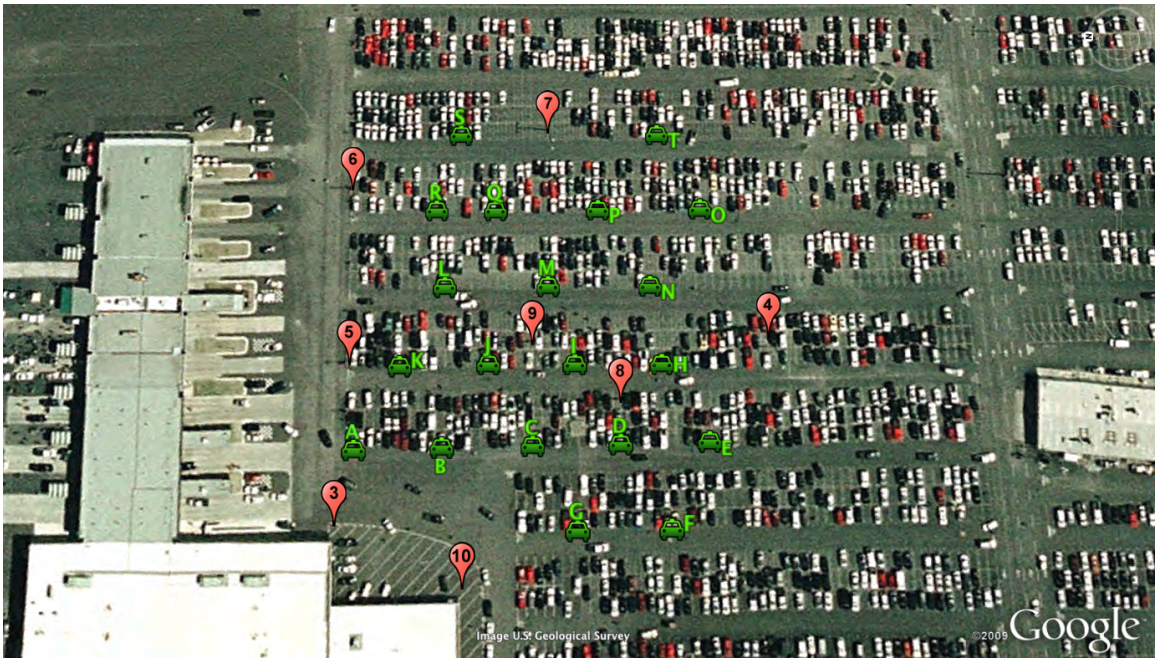
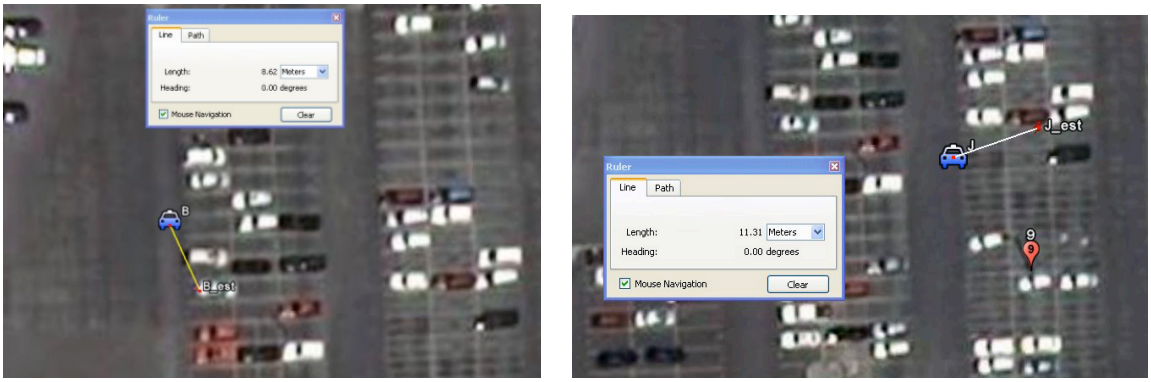


Figure 97: The WSN topology and measurement positions within a large parking lot.



(a) (b)

Figure 98: Two examples of localization estimation errors.

Table 9: Summary of the localization estimation error results.

min value	1.62 m
max value	95.9 m
mean value of 24 positions in whole topology	38.56 m
mean value in center of topology	24.52 m
mean value in periphery of topology	51.98 m

AUTHOR'S PUBLICATIONS

Book Chapters

1. V. Lakafosis, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, *Near-Field Authentication*, ch. 4, pp. 74–99. IGI Global, 2013
2. V. Lakafosis, R. Vyas, and M. M. Tentzeris, *Enabling Localization Services in Single and Multihop Wireless Networks*, ch. 15, pp. 385–412. John Wiley & Sons, Inc., 2010
3. V. Lakafosis, R. Vyas, C. Mariotti, T. Le, and M. M. Tentzeris, *Integrating Tiny RFID and NFC Based Sensors with the Internet*. Cambridge University Press, 2013 (to appear soon)

Journals

1. V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, "RF Fingerprinting Physical Objects for Anticounterfeiting Applications," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 59, pp. 504 –514, Feb. 2011
2. V. Lakafosis, A. Rida, R. Vyas, L. Yang, S. Nikolaou, and M. Tentzeris, "Progress Towards the First Wireless Sensor Networks Consisting of Inkjet-Printed, Paper-Based RFID-Enabled Sensor Tags," *Proceedings of the IEEE*, vol. 98, pp. 1601 –1609, Sept. 2010
3. V. Lakafosis and M. Tentzeris, "From single-to multihop: The status of wireless localization," *Microwave Magazine, IEEE*, vol. 10, pp. 34 –41, Dec. 2009
4. R. Vyas, V. Lakafosis, H. Lee, G. Shaker, L. Yang, G. Orecchini, A. Traille, M. Tentzeris, and L. Roselli, "Inkjet Printed, Self Powered, Wireless Sensors for Environmental, Gas, and Authentication-Based Sensing," *Sensors Journal, IEEE*, vol. 11, pp. 3139 –3152, Dec. 2011
5. R. Vyas, V. Lakafosis, A. Rida, N. Chaisilwattana, S. Travis, J. Pan, and M. Tentzeris,

"Paper-Based RFID-Enabled Wireless Platforms for Sensing Applications," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 57, pp. 1370 –1382, May 2009

Conferences

1. V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, "RFID-CoA: The RFID tags as certificates of authenticity," in *RFID (RFID), 2011 IEEE International Conference on*, pp. 207 –214, Apr. 2011
2. V. Lakafosis, A. Traille, H. Lee, G. Orecchini, E. Gebara, M. Tentzeris, J. Laskar, G. DeJean, and D. Kirovski, "An RFID system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities," in *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pp. 840 –843, May 2010
3. V. Lakafosis, X. Yi, T. Le, E. Gebara, Y. Wang, and M. Tentzeris, "Wireless Sensing With Smart Skins," in *Sensors, 2011 IEEE*, pp. 623 –626, Oct. 2011
4. C. Shi, V. Lakafosis, M. H. Ammar, and E. W. Zegura, "Serendipity: Enabling remote computing among intermittently connected mobile devices," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, (New York, NY, USA), pp. 145–154, ACM, 2012
5. V. Lakafosis, S. Addagatla, C. Belady, and S. Sinha, "Prometheus: A Wirelessly Interconnected, Pico-Datacenter Framework for the Developing World," in *10th International Conference on Wired / Wireless Internet Communications (WWIC 2012)*, (Island of Santorini, Greece), June 2012
6. D. De Donno, V. Lakafosis, L. Tarricone, and M. M. Tentzeris, "Increasing Performance of SDR-based Collision-free RFID Systems," in *Microwave Symposium Digest (MTT), 2012 IEEE MTT-S International*, pp. 1–3, June 2012
7. G. DeJean, V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, and D. Kirovski, "RFDNA: A wireless authentication system on flexible substrates," in *Electronic Components and Technology Conference (ECTC), 2011 IEEE 61st*, pp. 1332 –1337, June 2011

8. V. Lakafosis, N. Chaisilwattana, C. Kruesi, L. Yang, D. Staiculescu, and M. Tentzeris, "Low-cost low-power small-form-factor node for health monitoring wireless multi-hop personal area networks with dramatically increased range," in *Antennas and Propagation Society International Symposium, 2009. APSURSI '09. IEEE*, pp. 1 – 4, June 2009
9. D. De Donno, L. Tarricone, V. Lakafosis, and M. Tentzeris, "Multipacket Reception MAC Schemes for the RFID EPC Gen2 Protocol," in *Wireless Communication Systems (ISWCS), 2012 International Symposium on*, pp. 311–315, Aug. 2012
10. M. Marroncelli, D. Trinchero, V. Lakafosis, and M. Tentzeris, "Concealable, low-cost paper-printed antennas for WISP-based RFIDs," in *RFID (RFID), 2011 IEEE International Conference on*, pp. 6 –10, Apr. 2011
11. V. Lakafosis, R. Vyas, V. Mukala, A. Traille, and M. Tentzeris, "Wireless Sensor Network Nodes for RTLS, Biomonitoring, and Authentication Applications," in *Antennas and Propagation (EUCAP), 2012 6th European Conference on*, pp. 62–63, Mar. 2012
12. V. Lakafosis and M. Tentzeris, "Implementation of multi-hop routing protocols for the dramatic range enhancement of wireless sensor networks," in *Antennas and Propagation Society International Symposium, 2008. AP-S 2008. IEEE*, pp. 1 –4, July 2008
13. R. Vyas, V. Lakafosis, and M. Tentzeris, "Wireless remote localization system utilizing ambient RF/solar power scavenging RFID tags," in *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pp. 1764 –1767, May 2010
14. R. Vyas, V. Lakafosis, M. Tentzeris, H. Nishimoto, and Y. Kawahara, "A battery-less, wireless mote for scavenging wireless power at UHF (470-570 MHz) frequencies," in *Antennas and Propagation (APSURSI), 2011 IEEE International Symposium on*, pp. 1069 –1072, July 2011
15. R. Vyas, V. Lakafosis, and M. Tentzeris, "Enabling Localization in WSNs with Solar-Powered End Devices," in *Sensor Networks, Ubiquitous, and Trustworthy Computing*

(SUTC), 2010 IEEE International Conference on, pp. 155 –160, June 2010

16. R. Vyas, V. Lakafosis, T. Wu, Y. Kawahara, and M. Tentzeris, "Near-perpetual operated solar and RF powered autonomous sensing systems," in *Microwave Conference, 2009. APMC 2009. Asia Pacific*, pp. 2240 –2243, Dec. 2009
17. R. Vyas, V. Lakafosis, Z. Konstas, and M. Tentzeris, "Design and characterization of a novel battery-less, solar powered wireless tag for enhanced-range remote tracking applications," in *Microwave Conference, 2009. EuMC 2009. European*, pp. 169 –172, Oct. 2009
18. R. Vyas, V. Lakafosis, Z. Konstas, and M. Tentzeris, "Design of a novel, Battery-less, Solar Powered Wireless Tag for enhanced range remote tracking applications," in *Antennas and Propagation Society International Symposium, 2009. APSURSI '09. IEEE*, pp. 1 –4, June 2009
19. T. Le, V. Lakafosis, Z. Lin, C. P. Wong, and M. Tentzeris, "A Novel Graphene-Based Inkjet-Printed WISP-Enabled Wireless Gas Sensor," in *EuMC 2012*, 2012
20. T. Le, V. Lakafosis, T. Thai, Z. Lin, and M. Tentzeris, "Inkjet Printing of Graphene Thin Films for Wireless Sensing Applications," in *Electromagnetics in Advanced Applications (ICEAA), 2012 International Conference on*, pp. 954–957, Sept. 2012
21. T. Le, V. Lakafosis, Z. Lin, C. Wong, and M. Tentzeris, "Inkjet-Printed Graphene-Based Wireless Gas Sensor Modules," in *Electronic Components and Technology Conference (ECTC), 2012 IEEE 62nd*, pp. 1003–1008, June 2012
22. V. Lakafosis, R. Vyas, and M. M. Tentzeris, "A localization and position tracking solution utilizing solar-powered RFID tags," in *Antennas and Propagation (EuCAP), 2010 Proceedings of the Fourth European Conference on*, pp. 1 –4, Apr. 2010
23. Y. Kawahara, V. Lakafosis, Y. Sawakami, H. Nishimoto, and T. Asami, "Design issues for energy harvesting enabled wireless sensing systems," in *Microwave Conference, 2009. APMC 2009. Asia Pacific*, pp. 2248 –2251, Dec. 2009
24. V. Mukala, V. Lakafosis, A. Traille, and M. Tentzeris, "A novel Zigbee-based low-cost, low-power wireless EKG system," in *Microwave Symposium Digest (MTT),*

2010 IEEE MTT-S International, pp. 624 –627, May 2010

25. V. Mukala, A. Traille, V. Lakafosis, and M. Tentzeris, "Design and development of a novel wireless EKG system utilizing the low-power Zigbee standard," in *Antennas and Propagation Society International Symposium (APSURSI), 2010 IEEE*, pp. 1 –4, July 2010
26. A. Rida, V. Lakafosis, R. Vyas, M. Tentzeris, and S. Nikolaou, "Review of technologies for low-cost integrated sensors," in *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on*, pp. 513 –520, Sept. 2011
27. X. Zhang, V. Lakafosis, A. Traille, and M. M. Tentzeris, "Performance analysis of fast-moving RFID tags in state-of-the-art high-speed railway systems," in *RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on*, pp. 281 –285, June 2010

REFERENCES

[1] *Advanced Design System (ADS) Simulation Environment*. Agilent.

[2] R. Goldsborough, "Ancient Fourree Counterfeits," http://rg.ancients.info/fourees/ 2010.

[3] C. MANCINI and P. P. SERAFIN, "Identification of ancient silver-plated coins by means of neutron absorption," *Archaeometry*, vol. 18, no. 2, pp. 214–217, 1976.

[4] R. Goldsborough, "A Case for the World's First Coin: The Lydian Lion," 2010.

[5] M. Robyn, "Market-Driven Fraud: The Impact and Consequences of Counterfeit Products and Intellectual Property Violations," tech. rep., St. Louis, Missouri, 2008.

[6] "Magnitude of counterfeiting and piracy of tangible products," tech. rep., Organisation for Economic Co-operation and Development (OECD), Paris, France, 2009.

[7] R. Judson and R. Porter, "Estimating the Volume of Counterfeit U.S. Currency in Circulation Worldwide: Data and Extrapolation," tech. rep., Federal Reserve Bank of Chicago, 1 Mar. 2010.

[8] *Annual Report 2011*. European Central Bank, Mar. 2012.

[9] "Global Card Fraud - The Nilson Report," tech. rep., June 2010.

[10] Glaxo-Smith-Kline, "Counterfeiting Report," tech. rep., 2009.

[11] B. Stern, "Warning! Bogus Parts Have Turned Up in Commercial Jets. Where's the FAA?," 1996.

[12] "Anti-Counterfeiting Trade Agreement," *Wikipedia*, Apr. 2011.

[13] G. DeJean and D. Kirovski, "Radio frequency certificates of authenticity," Mar. 16 2010. US Patent 7,677,438.

[14] A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 381–394, 2006.

[15] D. Bauder, "An anti-counterfeiting concept for currency systems," tech. rep., Sandia National Labs, Albuquerque NM, 1983.

[16] G. J. Simmons, "Identification of data, devices, documents and individuals," pp. 197–218, 1-3 Oct. 1991.

[17] S. Church and D. Littman, "Machine reading of Visual Counterfeit Deterrent Features and Summary of US Research, 1980-90," tech. rep., Canada, 1991.

[18] Y. Chen, M. K. Mihcak, and D. Kirovski, "Certifying authenticity via fiber-infused paper," *SIGecom Exch.*, vol. 5, no. 3, pp. 29–37, 2005.

[19] R. Marchessault, P. Rioux, and L. Raymond, "Magnetic cellulose fibres and paper: preparation, processing and properties," *Polymer*, vol. 33, no. 19, pp. 4024 – 4028, 1992.

[20] A. C. Small and J. H. Johnston, "Novel hybrid materials of magnetic nanoparticles and cellulose fibers," *Journal of Colloid and Interface Science*, vol. 331, no. 1, pp. 122 – 126, 2009.

[21] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," *Science*, vol. 297, pp. 2026–2030, 20 Sept. 2002.

[22] B. Skoric, "The entropy of keys derived from laser speckle," *ArXiv e-prints*, Oct. 2007.

[23] P. Tuyls and L. Batina, *RFID-Tags for Anti-counterfeiting*, vol. 3860 of *Lecture Notes in Computer Science*, pp. 115–131. Springer Berlin / Heidelberg, 2006.

[24] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," pp. 58–64, 16-17 Apr. 2008.

[25] B. A. Alsaify, D. R. Thompson, and J. Di, "Identifying passive uhf rfid tags using signal features at different tari durations," in *RFID (RFID), 2012 IEEE International Conference on*, pp. 40–46, Apr. 2012.

[26] "Inkode, inc.."

[27] S. Preradovic and N. C. Karmakar, "Design of fully printable chipless RFID tag on flexible substrate for secure banknote applications," pp. 206–210, 20-22 Aug. 2009.

[28] "CrossID, Inc.."

[29] H. P. Romero, K. A. Remley, D. F. Williams, and W. Chih-Ming, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 57, no. 5, pp. 1383–1387, 2009.

[30] L. Tsang, J. A. Kong, and R. T. Shin, *Theory of microwave remote sensing*. Wiley series in remote sensing, Wiley, 1985.

[31] C. A. Balanis, *Antenna Theory - Analysis and Design (3rd Edition)*. John Wiley & Sons, 2005.

[32] E. Joy, J. Leach, W., G. Rodrigue, and D. Paris, T., "Applications of probe-compensated near-field measurements," *Antennas and Propagation, IEEE Transactions on*, vol. 26, pp. 379 – 389, May 1978.

[33] C. Capps, "Near field or far field?." EDN.com - the Internet home of Electronic News, EDN, and Electronic Business, Aug. 2001.

[34] L. Barclay and I. of Electrical Engineers, *Propagation of radiowaves*. Electromagnetic Waves, Institution of Electrical Engineers, 2003.

[35] H. Krim and M. Viberg, "Two decades of array signal processing research: the parametric approach," *Signal Processing Magazine, IEEE*, vol. 13, pp. 67 –94, jul 1996.

[36] C. A. Balanis, *Modern Antenna Handbook*. John Wiley & Sons, 2011.

[37] J. Kraus and D. Fleisch, *Electromagnetics: with applications*. McGraw-Hill series in electrical and computer engineering: Electromagnetics, WCB/McGraw-Hill, 1999.

[38] J. Violette, D. White, and M. Violette, *Electromagnetic compatibility handbook*. Van Nostrand Reinhold, 1987.

[39] D. White and M. Mardiguian, *Electromagnetic shielding*. A Handbook series on electromagnetic interference and compatability, Emf-Emi Control, 1988.

[40] A. Yaghjian, "An overview of near-field antenna measurements," *Antennas and Propagation, IEEE Transactions on*, vol. 34, pp. 30 – 45, jan 1986.

[41] Y. Rahmat-Samii, L. I. Williams, and R. G. Yaccarino, "The UCLA bi-polar planar-near-field antenna-measurement and diagnostics range," *Antennas and Propagation Magazine, IEEE*, vol. 37, no. 6, pp. 16–35, 1995.

[42] Y. Huang and K. Boyle, *Antennas: From Theory to Practice*. Wiley, 2008.

[43] "Measurement of Electromagnetic Interference Characteristics," tech. rep., Department of Defense, July 1967.

[44] K. Kaiser, *Electromagnetic Compatibility Handbook*. Electrical engineering handbook series, CRC Press, 2005.

[45] S. Laybros and P. Combes, "On radiating-zone boundaries of short, lambda;/2, and lambda; dipoles," *Antennas and Propagation Magazine, IEEE*, vol. 46, pp. 53 – 64, oct. 2004.

[46] L. Bayvel and A. Jones, *Electromagnetic scattering and its applications*. Applied Science, 1981.

[47] L. Tsang, J. A. Kong, and K.-H. Ding, *Scattering of Electromagnetic Waves: Theories and Applications*. John Wiley & Sons, Inc., 2002.

[48] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, "RFID-CoA: The RFID tags as certificates of authenticity," in *RFID (RFID), 2011 IEEE International Conference on*, pp. 207 –214, Apr. 2011.

[49] H. Schantz, "Near field propagation law a novel fundamental limit to antenna gain versus size," in *Antennas and Propagation Society International Symposium, 2005 IEEE*, vol. 3A, pp. 237 – 240 vol. 3A, July 2005.

[50] H. T. Friis, "A Note on a Simple Transmission Formula," in *Proceedings of the IRE*, vol. 34, pp. 254–256, 1946.

[51] "Electromagnetic Radiation: Field Memo." OSHA Cincinnati Laboratory, May 1990.

[52] P. V. Nikitin, K. Rao, and S. Lazar, "An overview of near field UHF RFID," in *RFID, 2007. IEEE International Conference on*, pp. 167–174, IEEE, 2007.

[53] V. Lakafosis, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, *Near-Field Authentication*, ch. 4, pp. 74–99. IGI Global, 2013.

[54] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[55] H. Suhl, "The Nonlinear Behavior of Ferrites at High Microwave Signal Levels," *Proceedings of the IRE*, vol. 44, no. 10, pp. 1270–1284, 1956.

[56] D. R. Smith, J. B. Pendry, and M. C. K. Wiltshire, "Metamaterials and Negative Refractive Index," *Science*, vol. 305, pp. 788–792, 6 Aug. 2004.

[57] Y. Li, A. Rida, R. Vyas, and M. M. Tentzeris, "RFID Tag and RF Structures on a Paper Substrate Using Inkjet-Printing Technology," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 55, no. 12, pp. 2894–2901, 2007.

[58] V. Lakafosis, A. Rida, R. Vyas, L. Yang, S. Nikolaou, and M. Tentzeris, "Progress Towards the First Wireless Sensor Networks Consisting of Inkjet-Printed, Paper-Based RFID-Enabled Sensor Tags," *Proceedings of the IEEE*, vol. 98, pp. 1601 – 1609, Sept. 2010.

[59] V. Lakafosis, A. Traille, H. Lee, G. Orecchini, E. Gebara, M. Tentzeris, J. Laskar, G. DeJean, and D. Kirovski, "An RFID system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities," in *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pp. 840 –843, May 2010.

[60] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, "RF Fingerprinting Physical Objects for Anticounterfeiting Applications," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 59, pp. 504 –514, Feb. 2011.

[61] "Aero-plastics, inc.."

[62] D. Kirovski, "Anti-counterfeiting: Mixing the physical and the digital world," in *Foundations for Forgery-Resilient Cryptographic Hardware* (J. Guajardo, B. Preneel, A.-R. Sadeghi, and P. Tuyls, eds.), no. 09282 in Dagstuhl Seminar Proceedings, (Dagstuhl, Germany), Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2010.

[63] EPCglobal Inc., "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.2.0," Oct. 2008.

[64] National Institute of Standards and Technology (U.S.), "Secure hash standard (SHS)," 2008.

[65] National Institute of Standards and Technology (U.S.), "Digital Signature Standard (DSS)," June 2009.

[66] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*. Springer Professional Computing, Springer, 2004.

[67] "National Instruments USB-6259 BNC 16-Bit, 1.25 MS/s M Series multifunction data acquisition (DAQ) module," Oct. 2011.

[68] "Hittite HMC430lp4 mmIC VCO with buffer amplifier, 5.0 - 5.5 GHz."

[69] "Hittite HMC431lp4 mmIC VCO with buffer amplifier, 5.5 - 6.1 GHz."

[70] "MSP-EXP430F5438 Experimenter Board User's Guide (Rev. E) - SLAU263E," Oct. 2010.

[71] L. RongLin, G. DeJean, M. M. Tentzeris, and J. Laskar, "Development and analysis of a folded shorted-patch antenna with reduced size," *Antennas and Propagation, IEEE Transactions on*, vol. 52, no. 2, pp. 555–562, 2004.

[72] P. Mendes, A. Polyakov, M. Bartek, J. Burghartz, and J. Correia, "An integrated folded-patch antenna for wireless microsystems," in *Sensors, 2004. Proceedings of IEEE*, pp. 485 – 488 vol.1, Oct. 2004.

[73] "Hittite HMC345lp3 GaAs mmIC SP4T Non-reflective positive control switch, DC - 8 GHz."

[74] "DC to >6000MHz RFMD 3378DS General Purpose Amplifier."

[75] "Linear 5581f 6GHz RMS Power Detector."

[76] "HP 83622B Swept Signal Generator."

[77] "MSP430F543x, MSP430F541x Mixed Signal Microcontroller (Rev. C) - SLAS612C," Mar. 2010.

[78] J. Wagner, "Filtering pwm signals," *Rev. 3*, Oct. 2009.

[79] A. Peterchev and S. Sanders, "Quantization resolution and limit cycling in digitally controlled PWM converters," *Power Electronics, IEEE Transactions on*, vol. 18, pp. 301 – 308, jan 2003.

[80] "LM6142BIM 17 MHz Rail-to-Rail Input-Output Operational Amplifier."

[81] J. Blair, "Sine-fitting software for IEEE Standards 1057 and 1241," vol. 3, pp. 1504–1506 vol.3, 1999.

[82] K. Hejn and A. Pacut, "Sine-wave parameters estimation - the second source of inaccuracy," vol. 2, pp. 1328–1333 vol.2, 20-22 May 2003.

[83] "TUSB3410 USB to Serial Port Controller (Rev. H) - SLLS519H," Jan. 2010.

[84] "CC2530 A True System-on-Chip Solution for 2.4-GHz IEEE 802.15.4 and ZigBee Applications - SWRS081B," Feb. 2011.

[85] "CC2540 2.4-GHz Bluetooth low energy System-on-Chip - SWRS084C," Nov. 2011.

[86] J. Aguilar, M. Beadle, P. Thompson, and M. Shelley, "The microwave and rf characteristics of fr4 substrates," in *Low Cost Antenna Technology (Ref. No. 1998/206), IEE Colloquium on*, pp. 2/1 –2/6, feb 1998.

[87] MATLAB, *version 7.13 (R2011b)*. Natick, Massachusetts: The MathWorks Inc., 2012.

[88] J. Gurland and R. C. Tripathi, "A Simple Approximation for Unbiased Estimation of the Standard Deviation," in *The American Statistician Journal* (A. S. Association, ed.), vol. 25, pp. 30–32, Oct. 1971.

[89] P. Charles D. Ghilani, *Adjustment Computations: Spatial Data Analysis*. John Wiley & Sons, 2010.

[90] Y. Dodge, *The Oxford Dictionary of Statistical Terms*. Oxford University Press, 2006.

[91] H. L. V. Trees, *Detection, Estimation, and Modulation Theory*. John Wiley & Sons, Inc., 1968.

[92] N. MacMillan and C. Creelman, *Detection Theory: A User's Guide*. Lawrence Erlbaum Associates, 2005.

[93] D. M. Green and J. A. Swets, *Signal detection theory and psychophysics*. New York: Wiley, 1966.

[94] J. Neyman and E. S. Pearson, "On the use and interpretation of certain test criteria for purposes of statistical inference: Part ii," *Biometrika*, vol. 20A, no. 3/4, pp. pp. 263–294, 1928.

[95] S. S. Wilks, "The large-sample distribution of the likelihood ratio for testing composite hypotheses," *The Annals of Mathematical Statistics*, vol. 9, no. 1, pp. pp. 60–62, 1938.

[96] G. E. P. Box, "A general distribution theory for a class of likelihood criteria," *Biometrika*, vol. 36, no. 3/4, pp. pp. 317–346, 1949.

[97] N. P. Johnson, "Advantages to transforming the receiver operating characteristic (roc) curve into likelihood ratio co-ordinates," *Statistics in Medicine*, vol. 23, no. 14, pp. 2257–2266, 2004.

[98] P. Wand and C. Jones, *Kernel Smoothing*. Monographs on Statistics and Applied Probability, Chapman & Hall, 1995.

[99] D. Scott, "Multivariate density estimation," *Multivariate Density Estimation, Wiley, New York, 1992*, vol. 1, 1992.

[100] J. Simonoff, *Smoothing Methods in Statistics*. Springer Series in Statistics, Springer, 1996.

[101] Z. Botev, J. Grotowski, and D. Kroese, "Kernel density estimation via diffusion," *Annals of Statistics*, vol. 38, no. 5, pp. 2916–2957, 2010.

[102] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Tech. Rep. SP800-22rev1a, NIST, April 2010.

[103] J. Soto and L. Bassham, "Randomness testing of the advanced encryption standard finalist candidates," tech. rep., DTIC Document, 2000.

[104] J. Massey, "Shift-register synthesis and bch decoding," *Information Theory, IEEE Transactions on*, vol. 15, no. 1, pp. 122–127, 1969.

[105] J. Von Neumann, R. Kent, H. Bellinson, and B. Hart, "The mean square successive difference," *The Annals of Mathematical Statistics*, pp. 153–162, 1941.

[106] B. Jun and P. Kocher, "The intel random number generator," *Cryptography Research Inc. white paper*, 1999.

[107] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *Computers, IEEE Transactions on*, vol. 56, pp. 109 –119, jan. 2007.

[108] P. Kohlbrenner and K. Gaj, "An embedded true random number generator for fpgas," in *Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays*, FPGA '04, (New York, NY, USA), pp. 71–78, ACM, 2004.

[109] C. Petrie and J. Connelly, "A noise-based ic random number generator for applications in cryptography," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 47, pp. 615 –621, may 2000.

[110] V. Fischer and M. Drutarovský, "True random number generator embedded in reconfigurable hardware," in *Cryptographic Hardware and Embedded Systems - CHES 2002* (B. Kaliski, ç. Koç, and C. Paar, eds.), vol. 2523 of *Lecture Notes in Computer Science*, pp. 415–430, Springer Berlin Heidelberg, 2003.

[111] G. DeJean and D. Kirovski, "Rf-dna: Radio-frequency certificates of authenticity," in *Cryptographic Hardware and Embedded Systems - CHES 2007* (P. Paillier and I. Verbauwhede, eds.), vol. 4727 of *Lecture Notes in Computer Science*, pp. 346–363, Springer Berlin Heidelberg, 2007.

[112] N. Valius, *Stereoscopy*. Focal Press, 1966.

[113] J. Pawley, *Handbook of biological confocal microscopy*. Springer, 2006.

[114] G. Y. Sirat, "Conoscopic holography. i. basic principles and physical basis," *JOSA A*, vol. 9, no. 1, pp. 70–83, 1992.

[115] M. Neil, R. Juskaitis, and T. Wilson, "Method of obtaining optical sectioning by using structured light in a conventional microscope," *Optics Letters*, vol. 22, no. 24, pp. 1905–1907, 1997.

[116] E. Haacke, R. Brown, M. Thompson, and R. Venkatesan, *Magnetic Resonance Imaging: Physical Principles and Sequence Design*. Wiley, 1999.

[117] J. Elliott and S. Dover, "X-ray microtomography," *Journal of microscopy*, vol. 126, no. 2, pp. 211–213, 2011.

[118] D. Huang, E. A. Swanson, C. P. Lin, J. S. Schuman, W. G. Stinson, W. Chang, M. R. Hee, T. Flotte, K. Gregory, C. A. Puliafito, *et al.*, *Optical coherence tomography*. PhD thesis, Massachusetts Institute of Technology, Whitaker College of Health Sciences and Technology, 1993.

[119] A. F. Fercher, "Optical coherence tomography," *Journal of Biomedical Optics*, vol. 1, no. 2, pp. 157–173, 1996.

[120] G. Vandenbosch and A. Vasylchenko, "A practical guide to 3d electromagnetic software tools," 2011.

[121] A. Vasylchenko, Y. Schols, W. De Raedt, and G. Vandenbosch, "A benchmarking of six software packages for full-wave analysis of microstrip antennas," in *Antennas and Propagation, 2007. EuCAP 2007. The Second European Conference on*, pp. 1–6, IET, 2007.

[122] M. Vrancken, Y. Schols, W. Aerts, and G. Vandenbosch, "Benchmark of full maxwell 3-dimensional electromagnetic field solvers on prototype cavity-backed aperture antenna," *AEU-International Journal of Electronics and Communications*, vol. 61, no. 6, pp. 363–369, 2007.

[123] O. Liske, "Comparison of computational electromagnetic tools for design and simulation of slot rhombic antenna," in *CAD Systems in Microelectronics (CADSM), 2011 11th International Conference The Experience of Designing and Application of*, pp. 114–115, IEEE, 2011.

[124] A. Vasylchenko, Y. Schols, W. De Raedt, and G. Vandenbosch, "Challenges in full wave electromagnetic simulation of very compact planar antennas," in *Antennas and Propagation, 2007. EuCAP 2007. The Second European Conference on*, pp. 1–6, IET, 2007.

[125] V. Radonic, V. Crnojevic-Bengin, and L. Zivanov, "Comparison of commercially available full-wave em simulation tools for microwave passive devices," in *Computer as a Tool, 2005. EUROCON 2005. The International Conference on*, vol. 2, pp. 1699–1702, IEEE, 2005.

[126] C. Bauer, G. Cohen, X. Ferrières, P. Monk, P. Borderies, and S. Pernet, "Comparison between a finite element method and yee's scheme to solve maxwell's equations," *Tiré à part- Office national d'études et de recherches aerospatiales*, 2004.

[127] V. Radonic, V. Crnojevic-Bengin, B. Reljic, and B. Jokanovic, "Accuracy of em simulation tools in modeling of resonant left-handed microstrip lines," in *EUROCON, 2007. The International Conference on" Computer as a Tool"*, pp. 2104–2109, IEEE, 2007.

[128] M. Vrancken, W. Aerts, and G. Vandenbosch, "Benchmark of full maxwell 3d electromagnetic field solvers on an soic8 packaged and interconnected circuit," *International Journal of RF and Microwave Computer-Aided Engineering*, vol. 16, no. 2, pp. 143–154, 2005.

[129] M. Karamehmedović, R. Schuh, V. Schmidt, T. Wriedt, C. Matyssek, W. Hergert, A. Stalmashonak, G. Seifert, and O. Stranik, "Comparison of numerical methods in near-field computation for metallic nanoparticles," *Optics Express*, vol. 19, no. 9, pp. 8939–8953, 2011.

[130] G. Mie, "Beiträge zur optik trüber medien, speziell kolloidaler metallösungen," *Annalen der Physik*, vol. 330, no. 3, pp. 377–445, 1908.

[131] Microwave Engineering Europe, "CAD benchmark," July 2001.

[132] H. ElKamchouchi and G. Abouelseoud, "Automating the electromagnetic simulation procedure and its possible," *Antennas and Propagation Magazine, IEEE*, vol. 49, no. 2, pp. 133–142, 2007.

[133] A. Massaro, L. Pierantoni, R. Cingolani, and T. Rozzi, "A new analytical model of diffraction by 3d dielectric corners," *Antennas and Propagation, IEEE Transactions on*, vol. 57, no. 8, pp. 2323–2330, 2009.

[134] "IEEE Standard for Validation of Computational Electromagnetics Computer Modeling and Simulations," *IEEE STD 1597.1-2008*, pp. c1 –41, 2008.

[135] R. A. Shelby, D. R. Smith, and S. Schultz, "Experimental verification of a negative index of refraction," *Science*, vol. 292, pp. 77–79, 6 Apr. 2001.

[136] E. Haber, D. Oldenburg, and R. Shekhtman, "Inversion of time domain three-dimensional electromagnetic data," *Geophysical Journal International*, vol. 171, no. 2, pp. 550–564, 2007.

[137] D. Avdeev, "Three-dimensional electromagnetic modelling and inversion from theory to application," *Surveys in Geophysics*, vol. 26, no. 6, pp. 767–799, 2005.

[138] E. Auken, L. Pellerin, N. Christensen, and K. Sørensen, "A survey of current trends in near-surface electrical and electromagnetic methods," *Geophysics*, vol. 71, no. 5, pp. G249–G260, 2006.

[139] V. G. Romanov and S. I. Kabanikhin, *Inverse problems for Maxwell's equations*. VSP, 1994.

[140] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," tech. rep., Cambridge, MA, USA, 1979.

[141] N. Leavitt, "Internet security under attack: The undermining of digital certificates," *Computer*, vol. 44, pp. 17 –20, dec. 2011.

[142] A. Herzberg, "Payments and banking with mobile personal devices," *Commun. ACM*, vol. 46, pp. 53–58, May 2003.

[143] W. Ford and M. S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2nd ed., 2000.

[144] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. Osvik, H. Riele, A. Timofeev, and P. Zimmermann, "Factorization of a 768-bit rsa modulus," in *Advances in Cryptology – CRYPTO 2010* (T. Rabin, ed.), vol. 6223 of *Lecture Notes in Computer Science*, pp. 333–350, Springer Berlin Heidelberg, 2010.

[145] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[146] Microsoft Research, "Technology to Combat Counterfeit Products," http://www.microsoft.com/en-us/researchconnections/science/stories/anti-counterfeit.aspx 2012.

[147] K. Römer, "The lighthouse location system for smart dust," in *Proceedings of the 1st international conference on Mobile systems, applications and services*, MobiSys '03, (New York, NY, USA), pp. 15–30, ACM, 2003.

[148] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[149] H. Zimmermann, "Osi reference model–the iso model of architecture for open systems interconnection," *Communications, IEEE Transactions on*, vol. 28, pp. 425 – 432, Apr. 1980.

[150] Crossbow Technology, "MICA2 Wireless Measurement System."

[151] H. Karl and A. Willig, *Protocols and architectures for wireless sensor networks*. Wiley, 2005.

[152] R. Vyas, V. Lakafosis, and M. Tentzeris, "Wireless remote localization system utilizing ambient RF/solar power scavenging RFID tags," in *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pp. 1764 –1767, May 2010.

[153] W. Stallings, *Data and Computer Communications*. Prentice Hall, 9th ed., 2011.

[154] Z. Konstas, A. Rida, R. Vyas, K. Katsibas, N. Uzunoglu, and M. Tentzeris, "A novel "green" inkjet-printed z-shaped monopole antenna for rfid applications," in *Antennas and Propagation, 2009. EuCAP 2009. 3rd European Conference on*, pp. 2340 –2343, march 2009.

[155] R. Vyas, V. Lakafosis, A. Rida, N. Chaisilwattana, S. Travis, J. Pan, and M. Tentzeris, "Paper-Based RFID-Enabled Wireless Platforms for Sensing Applications," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 57, pp. 1370 –1382, May 2009.

[156] T. S. Rappaport, *Wireless communications: principles and practice*. No. ISBN-10: 0130422320, Prentice Hall, 1996.

[157] N. Bulusu, D. Estrin, L. Girod, and J. Heidemann, "Scalable coordination for wireless sensor networks: Self-configuring localization systems," in *Proceedings of the Sixth International Symposium on Communication Theory and Applications*, ISCTA '01, 2001.

[158] K. Whitehouse and D. Culler, "Calibration as parameter estimation in sensor networks," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, WSNA '02, (New York, NY, USA), pp. 59–67, ACM, 2002.

[159] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal Of Basic Engineering*, vol. 82, no. Series D, pp. 35–45, 1960.

[160] "The R Project for Statistical Computing."

[161] "CC1000 Single Chip Very Low Power RF Transceiver - SWRS048A," Feb. 2007.

[162] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesc language: A holistic approach to networked embedded systems," in *Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation*, PLDI '03, (New York, NY, USA), pp. 1–11, ACM, 2003.

[163] Crossbow Technology, "XMesh Multihop Routing Protocol."

[164] K. L. Sallee, "GTAthena Localization Software," Version 1.11, Hegymagas, Hungary: Ecological Software Solutions LLC., 2008.

[165] Google Inc., "Google Earth Application."

[166] V. Lakafosis, R. Vyas, and M. M. Tentzeris, *Enabling Localization Services in Single and Multihop Wireless Networks*, ch. 15, pp. 385–412. John Wiley & Sons, Inc., 2010.

[167] V. Lakafosis, R. Vyas, C. Mariotti, T. Le, and M. M. Tentzeris, *Integrating Tiny RFID and NFC Based Sensors with the Internet*. Cambridge University Press, 2013 (to appear soon).

[168] V. Lakafosis and M. Tentzeris, "From single-to multihop: The status of wireless localization," *Microwave Magazine, IEEE*, vol. 10, pp. 34 –41, Dec. 2009.

[169] R. Vyas, V. Lakafosis, H. Lee, G. Shaker, L. Yang, G. Orecchini, A. Traille, M. Tentzeris, and L. Roselli, "Inkjet Printed, Self Powered, Wireless Sensors for Environmental, Gas, and Authentication-Based Sensing," *Sensors Journal, IEEE*, vol. 11, pp. 3139 –3152, Dec. 2011.

[170] V. Lakafosis, X. Yi, T. Le, E. Gebara, Y. Wang, and M. Tentzeris, "Wireless Sensing With Smart Skins," in *Sensors, 2011 IEEE*, pp. 623 –626, Oct. 2011.

[171] C. Shi, V. Lakafosis, M. H. Ammar, and E. W. Zegura, "Serendipity: Enabling remote computing among intermittently connected mobile devices," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, (New York, NY, USA), pp. 145–154, ACM, 2012.

[172] V. Lakafosis, S. Addagatla, C. Belady, and S. Sinha, "Prometheus: A Wirelessly Interconnected, Pico-Datacenter Framework for the Developing World," in *10th International Conference on Wired / Wireless Internet Communications (WWIC 2012)*, (Island of Santorini, Greece), June 2012.

[173] D. De Donno, V. Lakafosis, L. Tarricone, and M. M. Tentzeris, "Increasing Performance of SDR-based Collision-free RFID Systems," in *Microwave Symposium Digest (MTT), 2012 IEEE MTT-S International*, pp. 1–3, June 2012.

[174] G. DeJean, V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, and D. Kirovski, "RFDNA: A wireless authentication system on flexible substrates," in *Electronic Components and Technology Conference (ECTC), 2011 IEEE 61st*, pp. 1332 –1337, June 2011.

[175] V. Lakafosis, N. Chaisilwattana, C. Kruesi, L. Yang, D. Staiculescu, and M. Tentzeris, "Low-cost low-power small-form-factor node for health monitoring wireless multi-hop personal area networks with dramatically increased range," in *Antennas and Propagation Society International Symposium, 2009. APSURSI '09. IEEE*, pp. 1 –4, June 2009.

[176] D. De Donno, L. Tarricone, V. Lakafosis, and M. Tentzeris, "Multipacket Reception MAC Schemes for the RFID EPC Gen2 Protocol," in *Wireless Communication Systems (ISWCS), 2012 International Symposium on*, pp. 311–315, Aug. 2012.

[177] M. Marroncelli, D. Trinchero, V. Lakafosis, and M. Tentzeris, "Concealable, low-cost paper-printed antennas for WISP-based RFIDs," in *RFID (RFID), 2011 IEEE International Conference on*, pp. 6 –10, Apr. 2011.

[178] V. Lakafosis, R. Vyas, V. Mukala, A. Traille, and M. Tentzeris, "Wireless Sensor Network Nodes for RTLS, Biomonitoring, and Authentication Applications," in *Antennas and Propagation (EUCAP), 2012 6th European Conference on*, pp. 62–63, Mar. 2012.

[179] V. Lakafosis and M. Tentzeris, "Implementation of multi-hop routing protocols for the dramatic range enhancement of wireless sensor networks," in *Antennas and Propagation Society International Symposium, 2008. AP-S 2008. IEEE*, pp. 1 –4, July 2008.

[180] R. Vyas, V. Lakafosis, M. Tentzeris, H. Nishimoto, and Y. Kawahara, "A battery-less, wireless mote for scavenging wireless power at UHF (470-570 MHz) frequencies," in *Antennas and Propagation (APSURSI), 2011 IEEE International Symposium on*, pp. 1069 –1072, July 2011.

[181] R. Vyas, V. Lakafosis, and M. Tentzeris, "Enabling Localization in WSNs with Solar-Powered End Devices," in *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, pp. 155 –160, June 2010.

[182] R. Vyas, V. Lakafosis, T. Wu, Y. Kawahara, and M. Tentzeris, "Near-perpetual operated solar and RF powered autonomous sensing systems," in *Microwave Conference, 2009. APMC 2009. Asia Pacific*, pp. 2240 –2243, Dec. 2009.

[183] R. Vyas, V. Lakafosis, Z. Konstas, and M. Tentzeris, "Design and characterization of a novel battery-less, solar powered wireless tag for enhanced-range remote tracking applications," in *Microwave Conference, 2009. EuMC 2009. European*, pp. 169 – 172, Oct. 2009.

[184] R. Vyas, V. Lakafosis, Z. Konstas, and M. Tentzeris, "Design of a novel, Battery-less, Solar Powered Wireless Tag for enhanced range remote tracking applications," in *Antennas and Propagation Society International Symposium, 2009. APSURSI '09. IEEE*, pp. 1 –4, June 2009.

[185] T. Le, V. Lakafosis, Z. Lin, C. P. Wong, and M. Tentzeris, "A Novel Graphene-Based Inkjet-Printed WISP-Enabled Wireless Gas Sensor," in *EuMC 2012*, 2012.

[186] T. Le, V. Lakafosis, T. Thai, Z. Lin, and M. Tentzeris, "Inkjet Printing of Graphene Thin Films for Wireless Sensing Applications," in *Electromagnetics in Advanced Applications (ICEAA), 2012 International Conference on*, pp. 954–957, Sept. 2012.

[187] T. Le, V. Lakafosis, Z. Lin, C. Wong, and M. Tentzeris, "Inkjet-Printed Graphene-Based Wireless Gas Sensor Modules," in *Electronic Components and Technology Conference (ECTC), 2012 IEEE 62nd*, pp. 1003–1008, June 2012.

[188] V. Lakafosis, R. Vyas, and M. M. Tentzeris, "A localization and position tracking solution utilizing solar-powered RFID tags," in *Antennas and Propagation (EuCAP), 2010 Proceedings of the Fourth European Conference on*, pp. 1 –4, Apr. 2010.

[189] Y. Kawahara, V. Lakafosis, Y. Sawakami, H. Nishimoto, and T. Asami, "Design issues for energy harvesting enabled wireless sensing systems," in *Microwave Conference, 2009. APMC 2009. Asia Pacific*, pp. 2248 –2251, Dec. 2009.

[190] V. Mukala, V. Lakafosis, A. Traille, and M. Tentzeris, "A novel Zigbee-based low-cost, low-power wireless EKG system," in *Microwave Symposium Digest (MTT), 2010 IEEE MTT-S International*, pp. 624 –627, May 2010.

[191] V. Mukala, A. Traille, V. Lakafosis, and M. Tentzeris, "Design and development of a novel wireless EKG system utilizing the low-power Zigbee standard," in *Antennas and Propagation Society International Symposium (APSURSI), 2010 IEEE*, pp. 1 –4, July 2010.

[192] A. Rida, V. Lakafosis, R. Vyas, M. Tentzeris, and S. Nikolaou, "Review of technologies for low-cost integrated sensors," in *RFID-Technologies and Applications (RFID-TA), 2011 IEEE International Conference on*, pp. 513 –520, Sept. 2011.

[193] X. Zhang, V. Lakafosis, A. Traille, and M. M. Tentzeris, "Performance analysis of fast-moving RFID tags in state-of-the-art high-speed railway systems," in *RFID-Technology and Applications (RFID-TA), 2010 IEEE International Conference on*, pp. 281 –285, June 2010.

VITA

Vasileios Lakafosis was born in Athens, Greece in 1983. He received the Diploma degree in Electrical and Computer Engineering from the National Technical University, Athens, Greece, in 2006 and the M.Sc. degree in Electrical and Computer Engineering from the Georgia Institute of Technology, Atlanta, in 2009. In August 2007 he joined the Ph.D. program at the Georgia Institute of Technology. Vasileios has held research positions at the Cisco Research Center (San Jose, CA), Microsoft Research (Redmond, WA), and the University of Tokyo (Japan).

Vasileios has been an author of three book chapters and has published five peer-reviewed journal papers and more than 30 papers in conference proceedings of international symposia. He is a recipient of the Best Paper Award at the 2012 ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MOBIHOC). He has also been awarded the EETT (Greeces National Telecommunications Regulatory Authority) prize for his senior undergraduate Thesis. Vasileios has been a Lilian Voudouri Fellow for 2011-2013 and has been awarded the Gerondelis Foundation Scholarship for academic excellence during PhD studies in November 2010.