AFA-RFID: Physical Layer Authentication for Passive RFID Tags

Gregory Stuart Smith[1] Marijke Coetzee[2]
Academy of Computer Science and Software Engineering
University of Johannesburg
Johannesburg, South Africa
[1]hyperionza@gmail.com, [2]marijkec@uj.ac.za

Abstract—. **Radio Frequency IDentification, or RFID, is a ubiquitous technology found across many industries, but which is susceptible to breaches of information security. This research introduces analogue fingerprints as a means to authenticate passive RFID tags. An authentication model implemented at the physical layer of a passive RFID tag, using analogue fingerprints is proposed. The use of analogue computing principles increases the amount of potential authentication data whilst reducing the potential for counterfeiting.**

Keywords: authentication, passive RFID tag, physical layer security, analogue fingerprint

I. Introduction

Radio Frequency IDentification (RFID) [1] is an electronic means of identifying objects, in a manner similar to the ubiquitous barcode, though using radio transmissions as opposed to light. Passive RFID tags are a subset of RFID tags that do not contain their own power source and are extremely limited in their ability to store and process data. This limited nature renders them susceptible to many forms of attacks [2], [3] ranging from disabling attacks, unauthorised tracking and spoofing attacks.

Passive RFID tags are susceptible to being spoofed [2], [3] as they have little resources available and cannot provide any kind of strong authentication mechanism. Mimickery of one passive RFID tag by another is known as cloning [4]. To many RFID readers, cloned passive RFID tags are indistinguishable from their originals. These clones cause problems for industries and individuals that rely on passive RFID tags for secure and accurate tracking of products and other objects. To date, this challenge has not been resolved [5], [6], [7]. Thus, it becomes important to introduce a means not only to identify, but also to authenticate the passive RFID tag which identifies the product.

Product authentication and information security, in general, provide a challenging set of problems in the passive RFID environment. Implementing an effective authentication mechanism for passive RFID tags used in product identification would reduce not only the instances of counterfeiting passive RFID tags, but also reduce the impact counterfeit products have on legitimate businesses that employ an effective authentication mechanism.

Research points to the fact that the most successful authentication mechanism available for RFID tags to date exists in physical implementations, rather than through digital logic processing [8], [9], [10], [11]. The strongest authentication schemes are those that can use the random nature of imperfections within the manufacturing process to provide a unique electronic fingerprint for every device that employs a physical unclonable function, or PUF.

The aim of this research is to propose an authentication model that is hybridised from PUFs, as its implementation is physical, and it operates at the network-transmission layer using a boundless challenge-response mechanism. Because of the extremely limited nature of a passive RFID tag, the concept of analogue computers is investigated.

Next, in Section II, challenges of implementing product authentication with passive RFID tags is investigated and in Section III, current authentication mechanisms for passive RFID tags are described. The foundation for a more unconventional authentication model namely analogue computers and one-way functions are introduced in Section IV. Section V presents a new authentication model titled AFA-RFID and finally the paper is concluded in Section VI.

II. Challenges of Implementing Product Authentication in Passive RFID Tags

In an environment where a passive RFID tag is used to identify a product, the RFID reader is required to read only a unique product code from the passive RFID tag. The reader passes the unique product code to a back-end system, which uses the unique product code to retrieve or update relevant information about the product that has been stored by the back-end system. Thus, the identification of a product using a passive RFID tag is merely the retrieval of the unique product code and searching a data storage system for records matching the product code [12].

Due to the limited capabilities of passive RFID tags, communication occurs in a reader-talks-first fashion. As the passive RFID tag never initiates communications [13] the passive RFID tags cannot issue commands to the reader, and thus the tag cannot identify or authenticate the reader. This vulnerability allows any reader supporting the air interface protocol, legitimate or illegitimate, to access the tag and read its contents, leading to the threat where an attacker can create a clone or an identical copy of a passive RFID tag. Because of this threat, an RFID reader must be able to determine whether the passive RFID tag it is communicating with is an original, or

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

whether it is a clone containing a copy of the data of the original RFID tag. This is the fundamental question around which the concept of RFID authentication is based. There are many information security attacks such as cloning, man-in-the-middle and replay attacks to which passive RFID systems are vulnerable [2], especially when placed in a product identification role. With the resource limitations placed on passive RFID tags, there are three major challenges facing the implementation of strong information security to counter these attacks in passive RFID tags today, namely [11], [14] the number of electronic gates required to implement the information security feature, the high monetary cost of these additional electronic gates, and the high cost in terms of power consumption and often performance.

When systems communicate, the physical layer is responsible for transmission, reception and error correction, whilst information security is taken care of at the upper layers of the protocol stack [15]. Because passive RFID systems have limitations on hardware, power and performance requirements, the design of security mechanisms and cryptographic functions is challenging or almost impossible at upper layers. In order to address these limitations, the research focuses on security mechanisms at the physical layer.

III. AUTHENTICATION FOR PASSIVE RFID TAGS

Unidirectional authentication [16] is when the initiator issues a request to the responder to authenticate itself, however, the initiator itself is not necessarily authenticated in return by the responder. It logically follows that unidirectional authentication is the typical authentication scheme used by passive RFID tags. For this research, product authentication is verifying the authenticity of an object, and is implemented using unidirectional authentication. This research assumes that the problem of attaching the RFID tag to the object it identifies, in such a manner that it cannot be removed intact, has been solved.

Authentication schemes using mechanisms such as username/password pairs, digital signatures and cryptography require a large number of digital resources. For example, EPC Class 1 Generation 2 tags allow for password-based access control [13]. These passwords are simple and susceptible to being eavesdropped by an attacker [17]. To add the necessary resources to passive RFID tags would increase the cost of the tags beyond an acceptable point. When given a choice, customers purchasing passive RFID tags and devices will probably prefer to adopt the less expensive, unsecured passive RFID tag [17]. Thus implementing cryptographic approaches to securing cheap passive RFID tags against counterfeiting is not feasible if the end user desires a cost-effective solution for their needs. In this regard, authentication schemes such as Zero-Knowledge Protocols (ZKP) [18] are designed to defeat some of the challenges described above. Here, a prover tries to demonstrate knowledge of a shared secret to a verifier, without revealing any information whatsoever about the proof itself, except that it is valid. A shared secret does not necessarily have to be a key, but can be of any form such as the unique physical characteristics found in passive RFID tags by recent research conducted in physical unclonable functions.

Physical unclonable functions [19], or PUFs, target information security at a hardware level, rather than logically at the application layers, and are therefore be more suited to securing passive RFID tags. The Integrated Circuit (IC) that contains the logic of an RFID tag has physical and electrical characteristics that exist as a result of the manufacturing process. Characteristics are a result of material imperfections and irregularities in the doping and etching process. A Physical Unclonable Function (PUF) is an implementation-specific circuit that has been designed to extract these features [19] and is added into the IC of the RFID tag whose characteristics are to be measured and used in authentication. The general qualities found naturally within PUFs are those of uniqueness, an inability to be physically cloned and that they are often tamper resistant making PUFs ideal for authentication A particular drawback of this method is that each RFID tag that is manufactured would have to be tested repeatedly.

Radio Frequency Fingerprinting (RFF) [20] is another technique that measures and records the analogue electromagnetic radio signals transmitted over the air rather than just the data that the signal carries. Various features and characteristics are extrapolated from the recorded analogue dataset. The collection of these features and characteristics together form the authentication data. RFF requires no additional electronic circuitry in order to generate the authentication data, however, it does require specialised equipment in order to capture and interpret the authentication data. In order to apply RFF to an authentication scheme, the tag needs to be interrogated at the manufacturing plant many times and under different environments in order to build up a library of radio transmission recordings. These recordings, through interpretation and analysis, provide a set of characteristics used to authenticate the origin of the radio transmission, which is the passive RFID tag. Any authentication process would, by necessity, need to be online.

For PUFs and RFFs, their greatest strength is thus also their greatest weakness. Before being rolled out, there is an enrolment phase, where responses are measured and recorded. In some cases, the enrolment phase needs to be repeated several times during the lifespan of the RFID tag on which it is implemented. The repeated enrolment may cause some inconvenience to its users, especially those in an environment where a tag is be challenged frequently. In each of the implementations mentioned above, the generated authentication data are compared with a known result. That result, or set of results, would from time to time be required to be re-mapped as the passive RFID tag ages or the set of available challenge-response pairs is depleted. This is not ideal where access to facilities that can perform the re-enrolment of the passive RFID tag might not be readily available.

From this stems the requirement for an authentication mechanism *that does not require an enrolment phase*. Authentication data must be dynamic, with challenges and responses generated and validated as required, and not pulled from a known pool.

Moving forward, this research considers an alternate technology stack with the aim of proposing an authentication scheme, which is hybridised from PUF in that its implementation is physical and operates at the network-transmission layer. It includes a challenge-response mechanism, one that is deterministic in both manufacture and operation but does not require an enrolment phase, its challenge-response pairs, therefore, are boundless.

IV. An unconventional authentication scheme

To enable a new authentication scheme for use in passive RFID tags, the manner of generation and computation of authentication data needs to be examined and challenged. It must be considered whether limited devices such as passive RFID tags should implement their authentication schemes digitally, using logic gates or software, or rather in the analogue spectrum, where complex, non-linear mathematical operations can be performed in constant time, regardless of complexity [21]. Given the nature of one-way functions, the limited nature of passive RFID tags and the concept of analogue computers, this research proposes the merger of these three items, into a challenge-response authentication model, to provide a robust mechanism to provide passive RFID environments with a means of product authentication rather than just product identification. Merging these principles together provides sufficient information security with the benefit of no sniffable key exchange, thus enforcing the concept behind ZKPs. Using analogue computers to implement a one-way function for providing an authentication service would require only the transmission of the challenge and the response. The algorithm itself becomes the shared secret in the two-factor authentication scheme, the first factor being the passive RFID tags' unique identifier.

A. Electronic Analogue Computing

The physical difference between Analogue and Digital Computing is not substantial. At their core, both rely on currents and voltages to represent data; they both have a set of inputs, some form of processing and a set of outputs; they even share a common set of physical components [21] [22]. Their difference is that an analogue computer treats its variables as continuous data, whilst a digital computer makes use of discrete data within its variables. The other fundamental difference is the constraints under which the computer operates. A digital computer must, by the very nature of its being, count and obey logic rules exactly [21]. An analogue computer does not have this restriction when implementing a mathematical model. Currently, RFID tags are digital in nature.

Analogue Computing is a method that can be used to extend the concept of a PUF, though rather than an unintentional measurable side effect, analogue computers can be used to create an intentional deterministic fingerprint. The focus of this research is thus to create an electronic fingerprint for the purpose of authenticating passive RFID tags, where the electronic fingerprint is a complex mathematical function implemented in an analogue computer. To add analogue circuitry to a passive RFID tag is inexpensive and it would function similar to a digital implementation. The greatest drawback to using analogue computing is that analogue computers are not general purpose [22]. It is for this reason that analogue computers have broadly been abandoned except in specialised applications. An analogue computer is built to perform a specific function, to change its programming means to rebuild it. However, in creating an electronic fingerprint, the purpose is to create the fingerprint in such a manner as to prevent it from being changed in the useful lifetime of the product to which it is attached.

B. One-Way Functions

Needham and Schroeder [23] point out that, in 1978 at least most, if not all, authentication protocols commonly used shared secrets or encryption keys. In 2011 Burr et.al. [24] show that not much has changed. However, there is a school of thought [25] that puts one-way functions forward as lighter-weight and easier-to-design components of an authentication service. Because the primary intent of authentication is to provide proof of identity, that is integrity, rather than confidentiality, one-way functions, rather than encryption services, are thus more suited to the application of authentication. Functions that are easy to check and yet difficult or impossible to solve, when combined with analogue computing techniques, lead naturally to the concept of using such functions as an authentication mechanism for use in extreme resource-constrained devices such as passive RFID tags. Using an analogue implementation of one-way functions, the limitations of digital implementations in passive RFID tags can be overcome. Compared to digital implementations in a passive RFID tag, stronger and more complex mathematical functions can be implemented by an analogue circuit. The composition of authentication data would be an infinite series of challenge-response pairs rather than a static response. The implementation of a one-way function as an analogue circuit will require additional electronic components and hence negatively affect the cost of an RFID tag, though reproducing the equivalent computational capacity and speed digitally would cost even more. The impact to the digital resources of a passive RFID tag that implements an analogue one-way function should be negligible, requiring only that the digital circuitry manage when the analogue circuit is active according to existing states within the passive RFID tag.

The next section proposes an authentication model, using passive RFID tags in combination with one-way functions implemented as analogue computers. It also details various processes, operating environments and protocols within which the authentication model operates.

V. AFA-RFID Model

The model for physical layer authentication for passive RFID tags is entitled *Analogue Fingerprint for Authentication in RFID tags* (AFA-RFID). The authentication model is presented at a high level and is abstract in nature. The AFA-RFID model is described by first discussing the concepts employed by the model. Thereafter, architectural components are introduced and described. The authentication model and its operation is formally described and all interactions between parties given. More details on aspects relating to the analogue implementation of one-way functions and passive RFID tag circuitry and authentication data are described.

A. AFA-RFID Design Concepts

The concepts of RFID, PUFs, one-way functions, and analogue computers are not new, with PUFs being the most recent development, however, a detailed search of available literature has failed to reveal whether these disparate concepts have ever been merged into a single concept such as this. These concepts are now defined for this research. Finally a definition of an AFA-RFID Analogue Fingerprint is given.

1) Product Authentication

The focus of this research is limited to product authentication in passive RFID tag environments, where the reader issues a request to the passive RFID tag to authenticate itself. However, the reader is not necessarily authenticated in return by the passive RFID tag.

2) Physical Unclonable Functions

Two primary styles of PUF exist: namely, measuring tag characteristics or relying on additional circuitry on the passive RFID tag. A drawback of PUFs is the enrolment phase in the manufacturing process, which generates a set of authentication data that can be used at a later stage. As the components can suffer natural degradation, alterations in the resultant authentication data will occur, or the recorded challenge-response pairs may be depleted. In order to address these issues, this research extends the concept of arbiter-based PUFs [11] in that it makes use of an additional circuit to provide a fingerprint. A break from arbiter-based PUFs that require pre-recorded, single-use challenge-response pairs is made. The mechanism utilised by a challenge-response-based product authentication model without an enrolment phase, is defined next.

3) One-Way Functions

The one-way functions employed by AFA-RFID are the shared secret between the passive RFID tag and the authentication provider. Each company, brand or entity wishing to implement AFA-RFID, is required to apply to an issuing authority to obtain and register a unique one-way function for its use. As digital implementations of one-way functions such as MD5 or SHA-1 would consume more resources than are available to a passive RFID tag, an alternative means to provide the computational capacity, in the form of analogue computers, is proposed. As one-way functions are deterministic, this eliminates the need for an enrolment phase during production on which PUFs' are reliant. However, registration of the passive RFID tags' unique identifier against the one-way functions' known algorithm will be necessary.

4) Analogue Computers

Owing to the limited nature of passive RFID tags, the digital implementation of a strong authentication scheme using discrete computational techniques is not feasible. As such, analogue computational techniques are better positioned to handle the complexity and computational requirements of authentication in passive RFID tags. A very simple mathematical function, known as an elliptic curve*,* offers permutations which are theorised to be one-way functions [26]. Figure 1 shows the common basic form of an elliptic curve, as per equation 1, as it would be implemented using analogue function primitives in an analogue computer. An elliptic curve is not the only type of mathematical function that is implementable in an analogue computer. However, the elliptic curve family of mathematical functions are strong candidates for consideration when designing an analogue fingerprint. An analogue computer, in the case of this research, is implemented as an application-specific integrated circuit (ASIC), which is an electronic circuit where all the elements of the circuit are integrated into a medium and which functions as a unit. The reasons for implementing an ASIC side by side with the digital logic are to maintain forward- and backward-compatibility; the composition of authentication data processed by the ASIC will thus be an infinite series of challenge-response pairs rather than a static, or pre-recorded, response; additional electronic components negatively affect the cost of an RFID tag, though reproducing the equivalent computational capacity and speed digitally would cost even more and the impact to the digital resources of a passive RFID tag implementing an analogue one-way function must be negligible, requiring that the digital circuitry is used only when the analogue circuit is active, according to existing states within the passive RFID tag.

$$y^2 = x^3 + ax + b \text{……………………..(1)}$$

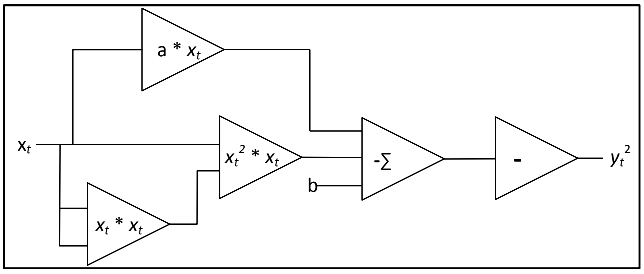

Figure 1. Flow diagram for an analogue implementation of an elliptic curve

The formal definition of an analogue fingerprint as described and presented in the context of this research is now given.

5) Definition: AFA-RFID Analogue Fingerprint

An analogue fingerprint is an embedded, tamper-resistant circuit that implements a one-way function, F, using analogue signal processing and analogue computational function primitives for the purpose of authenticating passive RFID tags at the physical layer by representing a shared secret.

Next, the architectural components of the AFA-RFID authentication model are described.

B. AFA-RFID Architectural Components

The primary components of the architectures are shown in Figure 2. Each component is now described and detailed information is provided on the design and creation of tag circuitry and authentication data used in the model.

1) AFA-RFID components

This section identifies and discusses the primary architectural components and entities that would interact within the AFA-RFID model, namely the passive RFID tag, the RFID reader, local back-office ecosystem, third-party authentication providers and central design and issuing authority. The roles and functions of each of these five entities are now discussed at a high level.

Passive RFID Tag: The passive RFID tag is the entity whose identity is trying to be proven. Securely embedded in the passive RFID tag, is the analogue fingerprint circuit, which will operate independently of the passive RFID tag's normal operation. The analogue fingerprint circuit accepts an authentication challenge and returns a response to the RFID reader.

RFID Reader: The RFID reader generates the challenge issued to the analogue fingerprint embedded in the passive RFID tag. The RFID reader receives authentication data from this tag and sends it to the local back-office application servers for further processing. The RFID reader is considered to be part of the local back-office ecosystem's infrastructure.

Local Back-Office Ecosystems: The local back-office ecosystem consist of the back-office applications and supporting infrastructure. The back-office applications accepts authentication data from the RFID reader to store and process it, and to issue subsequent requests to the authentication provider to authenticate the passive RFID tag. Additionally, within the back-office applications, the back-office ecosystem can implement an audit log trail to establish a history and timeline over the lifespan of the passive RFID tag.

Authentication Provider: The authentication provider stores the instance of the analogue fingerprint that is associated with the passive RFID tag's unique ID. It accepts the authentication data from the back-office application and authenticates the passive RFID tag. An authentication provider can be maintained either in-house for small local analogue fingerprint deployments or possibly at an online trusted third party for larger scale distributed deployments to ensure accessibility by all parties.

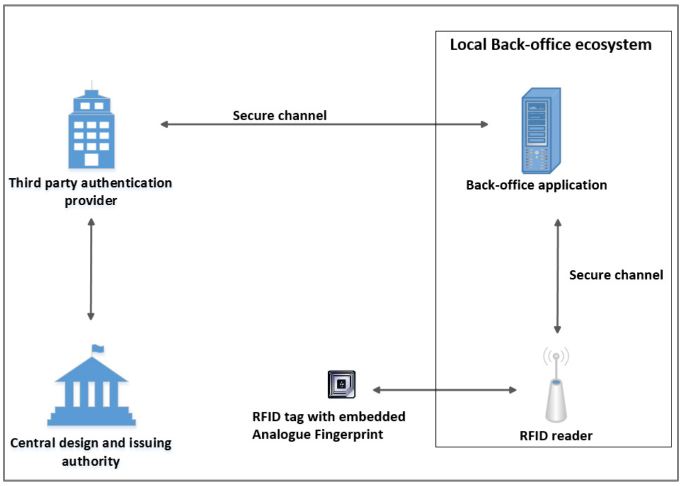
Local Back-office ecosystem
Secure channel
Third party authentication provider
Back-office application
Secure channel
RFID tag with embedded Analogue Fingerprint
RFID reader
Central design and issuing authority

Figure 2. AFA-RFID architecture

Central Design and Issuing Authority: The central design and issuing authority controls a registry of all existing fingerprints to ensure that each implementation of an analogue fingerprint is uniquely able to authenticate the passive RFID tag, or group of tags. This entity must, at the very least, be able to approve an analogue fingerprint design and register it to the applying entity. Preferably, the entity controlling the registration of analogue fingerprints must also have the capability to design an analogue fingerprint that will be issued or licensed to applicants. Such as central design and issuing authority for analogue fingerprints, need to put controls and quality assurance in place to ensure that strength and complexity of the analogue fingerprints under design are sufficient. It would also fall under the purview of the central design and issuing authority to license and approve manufacturers of passive RFID tags to allow them to manufacture passive RFID tags with analogue fingerprints embedded legally within them.

The risk of not having a central design and issuing authority is that there may come about the less-than-desirable scenarios whereby two companies are using identical analogue fingerprints or that illicit passive RFID manufacturers begin to manufacture the analogue fingerprint-enabled passive RFID tags through lack of regulation.

Although a single central design and issuing authority is considered in this research, it has the potential to become a bottleneck. As AFA-RFID grows in market penetration and usage, consideration should be made for the scalability of this component. Multiple design and issuing authorities may co-exist, however, to eliminate the possibility of duplicate fingerprints being issued, a centralised registry should be maintained and queried before any fingerprint is issued.

When the cost of AFA-RFID is considered in this research, the primary measure is the manufacturing cost per individual passive RFID tag. However, a holistic cost model, inclusive of infrastructure, subscription fees and registration fees, would realise a higher total cost per individual passive RFID tag.

Next, a high-level formal description is given of the AFA-RFID model.

C. AFA-RFID Model

AFA-RFID combines two authentication frameworks, namely a challenge-response framework and an online authentication framework, into its authentication model. The challenge-response segment is used to retrieve the data required to authenticate the passive RFID tag. However, as the reader is not allowed to perform the authentication step, the challenge-response authentication data are sent online to an authentication service to verify their authenticity. The advantage of this is that the distribution of the algorithm, which is the shared secret implemented as the analogue fingerprint, is kept to a minimum.

The proposed model consists of a number of phases namely:

1. The Analogue Fingerprint Design And Registration phase,
2. The Inventory phase,
3. The Concurrent Challenge phase,
4. The Authentication phase.

Next, the notation used to describe the AFA-RFID model is given, thereafter important concepts are defined using the notation.

1) Notation

$\boldsymbol{Y}$ denotes the RFID tag
$\boldsymbol{UID_Y}$ is the unique identifier associated with tag Y

$\boldsymbol{H_{UID_Y}}$ denotes the reference one-way function for the tag with UID *Y* that is stored and used for verification at the authentication provider

$\boldsymbol{F_Y}$ denotes the implemented one-way function as an analogue circuit

R denotes the RFID reader

x is the challenge in the form of a continuous time signal, $x_{0\ldots n} \in \mathbb{C}$

NG is the *noise generator* which resides on reader, *R*, and creates the challenge, *x*

$\boldsymbol{F_Y(x)}$ is the response from the one-way function F_Y

$\boldsymbol{T_H}$ is the allowable tolerance for variation from the expected result

P denotes the comparator function which accepts $F_Y(x)$, $H_{UID_Y}(x)$ and T_H in order to determine the authentication result

$\boldsymbol{R_p}$ the Result of *P*, $R_p \in$ *[True, False]*

2) Concepts

Using the notation, important concepts are now defined in more detail i.e the one-way function and authentication data.

One-way function: For this research, a one-way function is seen as a light-weight and easier-to-design component of the product authentication mechanism. Because the one-way function operating on the challenge received from the RFID reader is deterministic in its behaviour, a given input consistently provides the same output.

For this research, a one way function F_Y is defined as follows:

- F_Y represents a shared secret,
- Given *x*, it is easy to compute $F_Y(x)$,
- Given *z*, in the range of F_Y, it is hard to find an *x* such that $F_Y(x) = z$. More precisely, any efficient algorithm solving a P-problem succeeds in inverting F_Y with negligible probability.

Authentication data: This research proposes that authentication data must be dynamic, variable length challenge-response pairs, with challenges and responses generated and validated as required, and not taken from a known pool. The authentication data associated with AFA-RFID is a tuple $\{UID_Y,\ x,\ F_Y(x)\}$ comprising of three components:

- The passive RFID tag's unique identifier $\boldsymbol{UID_Y}$ is the unique identifier saved within the passive RFID tag's memory.
- The *challenge* $\boldsymbol{x}$ issued by the RFID reader is a continuous time signal transmitted from the RFID reader.
- The *response* $\boldsymbol{F_Y(x)}$ received from the analogue fingerprint circuit embedded on the passive RFID tag is the transmission, as recorded by the RFID reader, of the result of processing the challenge via the analogue fingerprint embedded within the passive RFID tag.

3) AFA-RFID Model Operation

The operation of the model is now described by the following steps.

- RFID tag *Y* implements a one-way function F_Y, as an analogue circuit.
- RFID tag *Y* is interrogated by reader *R*, which issues a challenge, in the form of a continuous time signal, *x*, as generated by *NG*.
- Reader *R* captures the response $F_Y(x)$, which is calculated by the analogue fingerprint on the passive RFID tag in constant time.
- Reader *R* consolidates the authentication data $\{UID_Y,\ x,\ F_Y(x)\}$ and transmits it to the back-end software to store and forward, based on the environmental configuration.
- The back-end software transmits $\{UID_Y,\ x,\ F_Y(x)\}$ to a third-party authentication provider, which uses UID_Y as a key lookup in order to retrieve the algorithm of the one-way function. The retrieved algorithm, H_{UID_Y}, is given the challenge, *x*, to recalculate the result of the one-way function, $H_{UID_Y}(x)$.
- $H_{UID_Y}(x)$ and $F_Y(x)$ are passed to another function, *P*, which accepts both $H_{UID_Y}(x)$, $F_Y(x)$ and a third parameter, T_H, which represents the allowable tolerance in the variance between the digitally calculated $H_{UID_Y}(x)$ and the analogue $F_Y(x)$. If the results match within the allowable tolerance, then a successful response, indicating that the passive RFID tag and associated one-way function have passed authentication, will be returned to the back-end software.

To formalise the message flows of the authentication process in each of the four phases of the model, the message protocol is given in Table 1. The protocol below uses the same notation as defined before.

TABLE I. AFA-RFID AUTHENTICATION PROTOCOL

Central Design and Issuing Authority	Authentication Provider	Reader and Back-Office	Tag
Design and Registration Phase			
Design → Registration	Store:H_{UID_Y}		
Inventory Phase			
		←	Inventory
Concurrent Challenge Phase			
		NG()	x →
		←	[FY(x)], [UIDY]
Authentication Phase			
	←	{UIDY, x, FY(x)}	

	Search:H_{UID_Y}
	Rp = P($H_{UID_Y}(x)$,
	FY(x), T_H)		

	Rp →		

The passive RFID tag is embedded with a secret, the analogue fingerprint, which can be verified by a trusted authority as being the secret belonging to that particular passive RFID tag. This secret must be protected against active attacks, meaning that if an adversary attempts to look inside of the passive RFID tag where the secret is generated, the physical properties of the passive RFID tag will change and the secret will become unrecoverable.

D. *Analogue Implementation of One-Way Functions*

Now that the model operation has been formalised, more detail is provided on the shared secret, how its secrecy is protected and who shares it in the following section.

1) *Protection of the Analogue Fingerprint*

The one-way function on the passive RFID tag and its interaction with the challenge to produce a response is analogous to stream-based cryptography. The challenge, in this instance, is analogous to the plain text, the response is likewise analogous to the cipher text. The one-way function is analogous to both an encryption algorithm and encryption key combined. Hence the need to protect access to the analogue fingerprint and limit its distribution. The more entities that are aware of its implementation, the weaker a specific analogue fingerprint becomes.

The one-way function implemented in the analogue fingerprint can be protected through several means. Obfuscating the function through filtering and intentionally introducing error into the circuit is but one means of doing so. Others, outside of the scope of this research, include obfuscating the physical design and layout of the circuit, including layering which actively destroys part of the circuit when tampered with, including fuses and time-stamps [27], [28]. Goetzel et al [29] provide details of several types of security threats against the physical structure of an integrated circuit against which future research into hardening an analogue fingerprint should take into account.

Next, the challenge generated by the RFID reader and the responses of the analogue fingerprint on the passive RFID tag are discussed.

2) *Composition and Creation of the AFA-RFID Challenge*

An analogue fingerprint acts and performs its calculations on a continuum of data, colloquially known as a signal. Owing to the deterministic behaviour of the analogue fingerprint, a predefined set of authentication data need not be generated, stored and then later retrieved in order to challenge the authenticity of the passive RFID tag. Rather, the challenge is generated and captured on the fly by the RFID reader. There are many kinds of signals that can be generated such as square waves, saw-tooth waves, triangular waves and sine waves, though these are all predictable. The most effective signal will be one that appears chaotic in nature and unpredictable. Should an attacker attempt to sniff the signal, it must be difficult to distinguish it from electrostatic noise. Such signal generators are called noise generators, and should such a signal be audible, it would sound like the static hiss from a radio that is not tuned to a radio station.

3) *Authentication Data*

As analogue fingerprints perform calculations on a continuum, the number of bits harvested from the challenge and response is time-dependent. Therefore, the greater the duration of the challenge, the greater the duration of the response, which results in a proportionally larger set of bits used for the authentication data when recorded and sampled by the reader. Equation 2 shows the general form of the equation used to calculate how many bits the generated challenge and resultant response comprises of.

$$f(x) = \textit{Sample rate/second} \;*\; \textit{duration} * \textit{bits/sample}\,\ldots\ldots\ldots(2)$$

For example, the following parameters are substituted into equation 2: the environment is set up to allow a reader 2 ms of access to each tag – which is roughly the same amount of time an EPC tag takes to be read; The reader is set to sample the response at a rate of 96 000 samples per second and each sample is 16 bits in size.

$$\begin{aligned} f(x) &= \textit{Sample rate/second} \;*\; \textit{duration} * \textit{bits/sample} \\ &= 96\,000 * 0.002 *16 \\ &= 3072 \textit{ bits} \end{aligned}$$

Thus analogue fingerprints have the potential to far outstrip the length of authentication data generated and used by arbiter-based PUFs, being 256 bits at most, where a greater number of bits is taken as an indicator of the strength of a model.

Now that the model operation has been formalised, more detail is provided on technical and other aspects of passive RFID tag circuitry design and operation.

E. *Passive RFID tag with an Analogue Fingerprint circuit*

Analogue and digital electronics can occupy the same circuit board or integrated circuit die, as depicted in Figure 3, where the analogue fingerprint at the top left is embedded in the circuit. However, they may not directly act or influence each other as their data is represented either as a continuum in analogue electronics or as discrete data in digital electronics. In order for one to communicate or transfer data to the other, it must first be passed through a converter, either an analogue-digital converter (ADC) or a digital-analogue converter (DAC), which transforms the data from either analogue (as with the ADC) or digital (as with the DAC) to the opposite representation. In Figure 3, these functions are performed by the *demodulator* and the *modulator*, respectively.

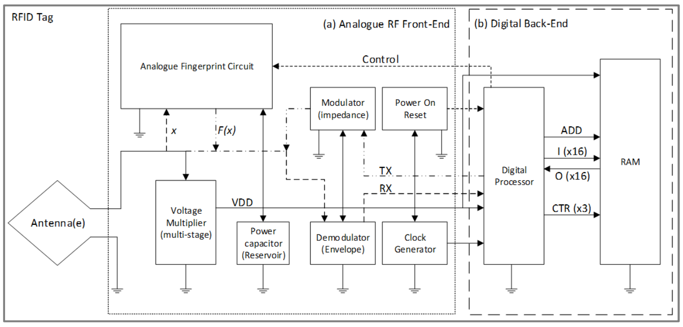

Figure 3. Passive RFID tag with an Analogue Fingerprint circuit

Because of the incompatibility of their data representations, and the intention to have both analogue and digital circuitry operational concurrently, the data for each will be required to be transmitted at different carrier frequencies. Beyond the limitations of data representation, analogue and digital circuitry share the same components, and can also share a single source of power.

VI. Conclusion

The AFA-RFID model is an unconventional solution to the problem of authentication of extreme resource-constrained devices such as passive RFID tags. Rather than looking for new solutions using new technology, AFA-RFID is a solution that uses established and mature technology in a new manner. AFA-RFID diverges completely from existing on-tag digitally implemented authentication services as it provides the on-tag authentication services through analogue circuitry. Because passive RFID tags do not have independent communications channels available to them to authenticate the reader that is querying them reliably, AFA-RFID has not been designed for mutual authentication. Nor is it intended for use as such between tag and reader. Rather, it is designed to perform product authentication, where the passive RFID tag authenticates itself to the reader. A second limitation is that, in its current state, the AFA-RFID model does not support privacy or confidentiality applications, unlike models which employ encryption mechanisms.

This research has proposed a theoretical model only, without simulation or prototype, to support its feasibility and viability. Future research aims to perform simulations in order to study the viability and prove claims made regarding the feasibility of this model.

References

[1] Juels, A. 2006. RFID security and privacy: A research survey. Selected Areas in Communications, IEEE Journal on. 24(2): 381-394.

[2] Finkenzeller, K. 2009. Known Attacks on RFID Systems, Possible Countermeasures and Upcoming Standardisation Activities. Dresden, Germany: Gisecke & Devrient.

[3] Burmester, M. & de Medeiros, B. 2007. RFID security: attacks, countermeasures and challenges. In: 5th RFID Academic Convocation, The RFID Journal Conference. Orlando: RFID Journal and Massachusetts Institute of Technology.

[4] Abawajy, J. 2009. Enhancing resistance against cloning attack. In: Third International Conference on Network and System Security, 2009. 19-21 October 2009 Gold Coast, QLD : IEEE Computer Society.

[5] Alteen, N. & Zalewski, J. 2012. RFID Security Experiment. Fort Myers, FL: Florida Gulf Coast University. Available: http://satnet.fgcu.edu/CEN3213/resources/module-5-rfid-security/RFIDexperiments.pdf [Accessed: 2013 February 2].

[6] Li, Y., Deng, R. & Bertino, E. 2013. RFID security and privacy. Synthesis Lectures on Information Security, Privacy, and Trust. 4(3): 1-157.

[7] Zanetti, D., Capkun, S. & Juels, A. 2013. Tailing RFID tags for clone detection. 20th Annual Network & Distributed System Security Symposium (NDSS '13). San Diego, CA: Internet Society.

[8] Holcomb, D.E., Burleson, W.P. & Fu, K. 2007. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In: Conference on Radio Frequency Identification Security (RFIDSec '07).

[9] Lim, D. 2004. Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems. 13(10): 1200-1205.

[10] Bertoncini, C., Rudd, K., Nousain, B. & Hinders, M. 2012. Wavelet fingerprinting of Radio-Frequency Identification (RFID) tags. In: IEEE Transactions on Industrial Electronics. 59(12): 4843-4850.

[11] Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T. & Khandelwal, V. 2008. Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications. In: 2008 IEEE International Conference on RFID. Las Vegas

[12] Weis, S.A. 2006. RFID (Radio Frequency Identification): Principles and Applications. Cambridge, MA: Massachusetts Institute of Technology.

[13] GS1 EPCglobal. 2008. Specification for RFID Air Interface EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.2.0. GS1. Available: http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf [Accessed: 2014, August 09].

[14] Garcia-Alfaro, J., Barbeau, M. & Kranakis, E. 2010. Security threat mitigation trends in low-cost RFID systems. In: Data Privacy Management and Autonomous Spontaneous Security. Heidelberg: Springer. 193-207.

[15] Mitrokotsa, A., Rieback, M.R. & Tanenbaum, A.S. 2010. Classifying RFID attacks and defenses. Information Systems Frontiers. 12(5): 491-505.

[16] Moskowitz, R. 2002. Authentication Types. San Francisco, CA: IEEE 802.1 Link Security Study Group

[17] Aigner, M., Burbridge, T., Ilic, A., Lyon, D., Soppera, A. & Lehtonen, M. 2009. RFID Tag Security BRIDGE White Paper. Available: http://www.bridge-project.eu/ [Accessed: 2011, November 20].

[18] U. Feige, A. Fiat and A. Shamir, "Zero-knowledge proofs of identity", J. Cryptology, vol. 1, pp. 77–94, 1988

[19] Nohl, K. 2008. Bold Security Claims about PUFs on RFID. Charlottesville, VA: Jefferson's Wheel – University of Virginia

[20] Hall, J., Barbeau, M. & Kranakis, E. 2003. Detection of transient in radio frequency fingerprinting using signal phase. In: Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC). Banff, Canada 13-18.

[21] Johnson, C.L. 1956. Analog Computer Techniques. New York, NY: McGraw-Hill.

[22] Beneš, K. 1984. Simulation of analog computer in solving non-linear differential equations by a digital computer. In: Acta Universitatis Palackianae Olomucensis Facultas Rerum Naturalium Mathematica. 23(1): 141-151.

[23] Needham, R.M. & Schroeder, M.D. 1978. Using encryptions for authentication in large networks of computers. Communications of the ACM. 21(12): 993-999.

[24] Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S. & Nabbus, E.A. 2013. Electronic Authentication Guideline. Gaithersburg, MD: National Institute of Standards and Technology. Technical Report: SP 800-63-1.

[25] Gong, L. 1989. Using One-Way Functions for Authentication. ACM Computer Communications Review. 19(5): 8-11

[26] Kaliski, B.S. Jr. 1991. One-way permutations on elliptic curves. Journal of Cryptology. 3: 187-199.

[27] Byrne, R.C. 1994. Patent No. US 5369299 A. – Tamper Resistant Integrated Circuit Structure California: United States Patent and Trademark Office. Available: http://patft.uspto.gov/netacgi/nph-Parser? Sect2=PTO1&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN/5369299 [Accessed: 2014, August 21]

[28] Desai, A. R., Ganta, D., Hsiao, M. S., Nazhandali, L., Wang, C. & Hall, S. 2013. Anti-counterfeit integrated circuits using fuse and tamper-resistant time-stamp circuitry. In: Technologies for Homeland Security (HST), 2013 IEEE International Conference on. Waltham, MA: IEEE. 480-485.

Goertzel, K. M., & Hamilton, B. A. (2013): Integrated Circuit Security Threats and Hardware Assurance Countermeasures. CrossTalk, The Journal of Defense Software Engineering, 33-38, U.S. Air Force Software Technology Support Center