

Chapter 1

Introduction from the editors

Structure of this book

This introduction describes the structure of the book, and in particular how it is divided into sections and chapters. It gives an outline of what can be found in each chapter, and gives a description of the origin and structure of the organisation known as the Auto-ID Laboratories whose members have studied the anti-counterfeiting problem and have provided the material for this book.

The four sections of the book are, as shown in the Table of Contents, entitled: 1: “Anti-counterfeiting and RFID” with four chapters; 2: “Security and Privacy Current Status” with four chapters; 3: “Network Based Solutions” with three chapters and 4: “Cryptographic Solutions” with six chapters.

The Auto-ID Laboratories

The Auto-ID Labs is the research-oriented successor to the Massachusetts Institute of Technology (MIT) Auto-ID Center, originally founded by David Brock and Sanjay Sarma of MIT with funding from Procter and Gamble, Gillette, the Uniform Code Council, and a number of other global consumer products manufacturers. The MIT Auto-ID Center was created to develop the Electronic Product Code (EPC), a global RFID-based item identification system intended to replace the UPC bar code. In October 2003 the Auto-ID Center was replaced by the combination of the newly founded research network the Auto-ID Labs, and EPCglobal, an organization charged with managing the new EPC Network. The Auto-ID Labs are responsible for managing and funding continued development of the EPC technology.

From its foundation in 1999, the Auto-ID Center grew to become a unique partnership between almost 100 global companies and six of the world’s leading research universities: the Massachusetts Institute of Technology in the US, the University of Cambridge in the UK, the University of Adelaide in Australia, Keio University in Japan, the University of St. Gallen in Switzerland, and Fudan University in China. Together they were and still are engaged in assembling the building blocks needed to create an “Internet of things” which is a global infra-structure – a layer on top of the Internet – that will make it possible for computers to identify any object anywhere in the world instantly. This network will not just provide the means to feed reliable, accurate, real-time information into existing business applications; it will usher in a whole new era of innovation and opportunity.

The Auto-ID Labs in March 2005 added Daejoen ICU University in Korea to their network, thus completing their organisation as the leading research group in

the field of networked radio-frequency identification (RFID) and emerging sensing technologies. The labs now consist of seven research universities located on four different continents. The areas of expertise range from hardware through software to business research related to RFID.

The research can be grouped into three main areas: hardware, software and business layer. On the autoidlabs.org website, the Auto-ID Labs continuously publish their research results and provide an archive with over 150 whitepapers and academic publications. The following shows how the network and the research are organized.

- Members

The research network now consists of the following seven research institutions:

- The University of Adelaide (Australia)
- The University of Cambridge (United Kingdom)
- Fudan University (China)
- The Information and Communications University (South Korea)
- Keio University (Japan)
- The Massachusetts Institute of Technology (USA)
- The University of St. Gallen/ETH Zurich (Switzerland)

The research is organised as follows.

- Business processes and applications

- Focus group: The University of St. Gallen/ETH Zurich, Keio University, The University of Cambridge, The Massachusetts Institute of Technology, The University of Adelaide
- Business cases
- Business applications
- Privacy and security aspects
- Fundamentally new business processes and industries which include payment, leasing, insurance, quality management, factory design, 3PL-managememt, brand protection, and anti-counterfeiting amongst others

- Software and networks

- Focus group: Keio University, The Massachusetts Institute of Technology
- Future system architecture
- EPC network
- Middleware
- Integration with existing systems

- Hardware

- Focus group: The Massachusetts Institute of Technology, Fudan University, The Information and Communications University, The University of Adelaide
- RF and chip design

- Class 2 and higher tags
- Tags with memory, battery, sensors and actuators
- Enhanced reading rates in challenging environments
- External links

External web links related to the Labs are

- The Auto-ID Labs website is at <http://www.autoidlabs.org/>
- The EPCglobal website is at <http://www.epcglobalinc.org/home>

Section 1 Anti-counterfeiting and RFID

Chapter 2: “Anti-Counterfeiting and Supply Chain Security”

In Chapter 2 “Anti-Counterfeiting and Securing Supply Chains” can be found an overview of the anti-counterfeiting problem and what is needed to secure supply chains, and how this may be achieved. As its title suggests, the chapter deals with two issues: the problems raised by counterfeit products and the methods by means of which supply chains might be made secure.

The chapter makes at the outset an emphatic statement about intellectual property rights and their role in sustaining innovation and underpinning economic growth and employment.

The challenges for affected enterprises raised by the violation of intellectual property rights are described in detail. The requirements for Auto-ID based anti-counterfeiting solutions are derived from detailed studies of firstly attack models by means of which the behaviour of illicit actors may be understood, and the secondly the capabilities of low cost RFID transponders that may be used to counter such attacks.

A number of solution concepts, employing both RFID and optical technologies, are identified. These range from various forms of using unique serial numbers, through plausibility checks based on track and trace, to object specific security systems that are discussed in more detail in Chapter 13, to secure authentication systems based on enciphered responses to reader challenges. Such approaches are seen as providing motivation for the research that is the major topic of this book.

Then follow two chapters “Networked RFID Systems” and “EPC Network Architecture” that provide basic background on the context in which anti-counterfeiting security solutions must be devised.

Chapter 3: “Networked RFID Systems”

In Chapter 3 “Networked RFID Systems” the authors seek to identify concepts and operating principles of a modern RFID system. Although a wide range of operating principles for such a system, such as use of microelectronic labels, surface

acoustic wave labels, labels using multiple resonances to encode data and so on, are identified and referenced, the material presented in this chapter considers in detail RFID systems based on using microelectronic devices. It is noted that in general the operating principle and operating frequency are driven principally by the application of the labelling system and by the constraints provided by electromagnetic compatibility regulations, environmental noise, and the ability of fields to permeate a scanned region of space or to penetrate intervening materials.

All modern RFID system infrastructures are seen as consisting of the three primary components: (a) RFID labels (transponders); (b) RFID label readers or interrogators (transceivers); and (c) backend networks (electronic databases). The RFID labels can be distinguished based on their frequency of operation: (a) LF; (b) HF; (c) UHF; or (d) microwave, the latter category being considered to cover the frequency bands at 2.45 GHz and 5.8 GHz. Advantages and disadvantages of each of these bands are listed.

Labels are also categorised in terms of their powering techniques of: (a) passive; (b) semi-passive; or (c) active, and the general features and applications of each type are identified. In considering communication between labels and interrogators, it is noted that there are similarities and differences in the way communication is achieved in both the far and the near field by a label antenna, and it is also explained that the role of label quality factor changes significantly between the two situations.

The EPC concept is briefly described on account of its close relation to emerging applications, and a hierarchy of label functionalities is also introduced. A method, by which the dilemma of diverse functionalities may be resolved by means other than a rigid hierarchy of functionalities, is described.

In considering back end systems it is pointed out that the general design principle in EPC based RFID systems is to off load silicon complexity of the label to backend systems and to the reader in order that the cost of the labels may be kept to a minimum, but the discussion of such systems is left to a further Chapter 4.

The important aspect of anti-collision that arises in multiple label reading applications is considered and it is noted that as RFID labels are constrained by limited computational power, and memory, and the anti-collision algorithms embedded in multiple tag reading protocols take note of this, and that anti-collision methods used in RFID must consider the wireless and ad hoc nature of RFID networks along with the necessity to recover from sudden power loss in the almost invariably used passive RFID systems.

Among the anti-collision algorithms both deterministic and probabilistic schemes are recognised. In addition to features which reduce the frequency of collisions, the capacity to detect collisions is seen as a powerful addition to an anti-collision algorithm. The role of line coding schemes is analysed and those which may or may not detect invalid symbols caused by collisions of label reply signals of differing strengths is identified. The role of CRC schemes in detecting collisions is also discussed.

Also influencing the performance of tag reading protocols is the issue of tag confusion, under which tag receive conflicting command or response signals from more than one interrogator, and so-called ghost reads (a reader reporting an EPC

of a tag that does not exist in its tag reading range) can occur. The features of well designed protocols that reduce this phenomenon are described.

The chapter concludes with a summary of the issues covered and reminds readers that the following chapter will elaborate on the integration of backend systems to RFID technology, developed under the Auto-ID Center vision of a “Networked Physical World”.

Chapter 4: “EPC Network Architecture”

In Chapter 4 “EPC Network Architecture” the authors provide an outline of the structure and usage of the ubiquitous item identification network that originated at the former Auto-ID Center, now called the Auto-ID Labs, and currently managed by a number of working groups at EPCglobal Inc. The Auto-ID Center vision was to create a “Smart World” by building an intelligent infrastructure linking objects, information, and people through a ubiquitous computer network, leveraging the Internet for global connectivity.

Contrary to the component based EPC Network architecture developed initially by the Auto-ID Center, the more modern version is based on an N-tier architecture with an emphasis on defining interfaces. The interfaces define the required standard functionalities and methods by which optional functionalities can be accessed rather than defining components and their associated functionalities.

The N-tier layered service oriented architecture approach fits naturally with an object oriented modelling of the architecture because objects encapsulate information and state while offering functionalities through their interfaces. The modules also have a loose coupling due to the independence of different modules. This reduction in dependency implies that the system is easier to manage and enhance.

Web services are one method of implementing the Service Oriented Architecture (SOA) over standardised protocols and interfaces. There is a strong tendency and a technological trend driving the EPC network architecture towards a web services based SOA.

The EPC Network can be separated into six primary modules, some physical, some logical: (1) RFID tags; (2) RFID tag readers; (3) EPC; (4) middleware; (5) Object Name Service (ONS); and (6) EPC Information Service (EPCIS).

Middleware system provides real time processing of RFID tag event data. Conceptually the middleware occupies the space between a Reader (or multiple Readers) and the application systems.

The middleware has several fundamental functions, some of which are: data filtering of received tag and sensor data; aggregation and counting of tag data; and accumulation of data over time periods.

The middleware possesses two primary interfaces that allow it to communicate with external systems: the Reader Interface and the Application Level Event Interface. The former provides an interface between the middleware and readers, and the latter between the middleware and external applications.

An middleware is composed of multiple Services, each with their own functionality. The services can be visualised as modules in the middleware. The multiple services modules can be combined to perform certain functions for specific applications. Hence one or more applications may make method calls to the middleware resulting in an operation being performed (e.g. collection and return of temperature readings from a sensor), and the return of results.

Event management is a primary service provided by the middleware services. A common event management function is filtering, which is particularly useful in situations where there is heavy data traffic.

However, recent developments have retreated from such a rigidly defined schema to the characterization of two instances: ECSpec and ECRports instances using a standard XML depiction. Thus requests to the middleware are sent as ECSpec object, while data from the middleware is returned as an ECRports object.

The core XML schemas for these objects are defined with extensions and rules to accommodate application or manufacturer specific XML schema (such as that suited for a specific sensor application) or a number of such schemas to allow the capture and reporting of physical world events and measurements.

The functionality provided by the ONS system is similar to the services provided by the Domain Name System (DNS); however instead of translating host names to their underlying IP addresses for user applications, ONS translates an EPC into URL(s). The Object Name Service (ONS) in an EPC Network identifies a list of service endpoints associated to the EPC and does not contain actual data related to an EPC. These service endpoints can then be accessed over a network. However, unlike the DNS, ONS is authoritative, that is the entity that retains control over the information about the EPC placed on the ONS is the same entity that assigned the EPC to the item.

In the event that the local ONS server is unable to satisfy the requests it is forwarded to a global ONS server infrastructure for resolution.

It should be noted here that the ONS does not resolve queries down to the level of fully serialised EPCs. The depth of the query stops at the Object Class level (product type) of the EPC.

A possible interface for an EPCIS can be implemented by adopting web services technology. A web services technology based interface allows applications in the wider area network to utilise services provided by local EPC Information Services using a remote method invocation paradigm. Such an architecture has the advantage of leveraging standardised XML messaging frameworks, such as that provided by the Simple Object Access Protocol (SOAP), and a description of the available services defined in terms of a Web Services Description Language (WSDL) file.

Hence an application requiring information is able to access a WSDL file which has a description of the available service methods, the required input and output parameters to the methods and information to invoke those methods.

EPCIS provides a model for the integration of RFID networks across the globe. However it is important that EPCIS provides a secure communication layer so that local EPC Networks can retain the authority to determine access to information. WS-Security is a candidate proposal for enhancing web services security that

describes enhancements to SOAP messaging to provide message integrity and message confidentiality while proposed architectural extensions to the existing WS-Security profile could provide access control as well as a federated security model for EPCIS.

As stated above, the ONS does not resolve to the serial number level of the EPC and the DNS technology upon which the ONS is based also does not allow the fine grain resolution down to serial number levels. Resolution down to serial EPC level (to a specific object) is handled by the EPCIS Discovery Service (EPCIS-DS).

EPCIS-DS is best described as a “search engine” for EPC related data. EPCIS-DS provides a method for custodians of a particular RFID tag data to update a register within the EPCIS-DS to indicate that they are in possession of data related to an EPC.

The chapter also considers briefly supply chain management issues such as product recall, grey-market activity and counterfeiting, and describes the concept of the “electronic pedigree”, a term that has been coined to label the electronic history of an item’s life throughout the supply chain. However it is made clear that issues related to security are considered in more detail in later chapters of this book.

Chapter 5: “A Security Primer”

Finally, in this introductory section, there is provided in Chapter 5 “A Security Primer” an overview of state of the art cryptography that can be applied to communication over insecure channels. The chapter describes the range security objectives to be sought, the fundamental Kerckhoffs’ Principle that must be observed in designing defences, the types of attack that can be mounted by persons of ill will against cryptosystems, and gives a classification of the security levels that can be attained. Unkeyed and keyed cryptographic primitives are defined, the latter including both public key and secret key systems, and their use both in securing messages against eavesdropping and in detecting that messages are authentic is explained. The burdens of providing the computational resources for the implementation of known effective schemes are discussed and found to be excessive the RFID context, and the chapter concludes with a statement that resource constraints in RFID tags have introduced a need for new lightweight cryptographic primitives to be used in RFID technology.

Section 2 Security and Privacy Current Status

This second section of the book contains four chapters that describe the current status of attempts to produce security and privacy. They begin in Chapter 6 with a more detailed treatment of security and privacy concepts than has been presented in the Primer.

Chapter 6: “Addressing Insecurities and Violations of Privacy”

In Chapter 6 “Addressing Insecurities and Violations of Privacy” the authors examine the vulnerabilities of current low cost RFID systems and explore the security and privacy threats posed as a result of those vulnerabilities, and the quality of defences that may be deployed.

The chapter formulates a framework for defining the problem space constructed around low cost RFID systems, and considers the challenges faced in engineering solutions to overcome the relative defencelessness of low cost implementations. Security issues beyond and including interrogators are not considered, as such concerns may be easily resolved using existing technology and knowledge. There is a concentration on the systems that are advocated by EPCglobal as Class I and Class II, both in respect of published standards at UHF and emerging draft standards at HF.

It is noted that for a low cost tag any additional hardware required to implement security needs to be designed and fabricated, this incurring additional cost. Reducing dice sizes to very small levels is not seen as feasible to compensate for such costs as the increase in cost of handling smaller die must be considered. A more practical avenue for reducing costs is seen as the use of obsolete IC manufacturing processes and filling up such fabrication pipelines with RFID IC chips.

It is concluded that as, due to cost constraints, low cost tags do not utilize anti-tampering technology, the long-term security of label contents cannot be guaranteed.

In emerging standards labels within reading range are reported as having a means of revealing their presence, but not their data, when interrogated by a reader. The labels then reply with a non-identifying signal to an interrogation by using a randomly generated number. However, for HF tags, there is no such prevalent standard, although EPCglobal is currently developing an HF specification to complement its UHF air interface protocol. The existing standards most commonly in use for HF tags, other than the ISO 18000, are listed.

Two important and related performance parameters are the number of label reads per second and data transmission speeds. Performance criteria of an RFID system demand a minimum label reading speed in excess of 200 labels per second.

As near and far fields scale differently with distance, each frequency band is seen to provide its own set of advantages and disadvantages.

Anonymity desired by persons is discussed. The most important concept is probably the concealment of the identity of a particular person involved in some process, such as the purchasing of an item, visit to a doctor or a cash transaction. Another is the concept of untraceability (location privacy).

There is a discussion of “killing” a label. Killing involves the destruction of the label thus rendering it inoperable. An alternative idea to killing that has been entertained involves the removal of the unique serial number of the EPC code in articles that allows the label owners to be tracked, albeit with difficulty in practice. This does not remove all the privacy concerns as tracking is still possible by associating a “constellation” of a label group with an individual. This implies that a particular taste in clothes and shoes may allow an individual’s location privacy or anonymity to be violated. However “killing” a label will eliminate

privacy concerns and prevent access by unauthorized readers when combined with a password to control access to the kill command.

The security risks that arise with low cost RFID labels are seen as arising from: (a) communication between a tag and a reader taking place over an insecure channel; (b) tags being accessible by any reader implementing the air interface protocol; (c) tags being not tamper proof and allowing a channel for physical access to tag contents and circuitry (as a result, tags cannot be expected to secure information for long periods); (d) integrated circuit designs being constrained by cost and being thus minimalist implementations; (e) air interface protocols being designed to reduce tag complexity; and (f) design flaws in reader implementations due to cost constraints.

It is noted that transmissions from a reader and a tag take place over a clear communication channel which may be observed by a third party. In this context the classification of eavesdropping range concepts: (a) operating range; (b) backward channel eavesdropping range; (c) forward channel eavesdropping range; and (d) malicious scanning range is offered. Passive eavesdropping and scanning (active eavesdropping) concepts are discussed.

Attacks on security are classified as: (a) cloning; (b) man-in-the-middle; (c) denial of service; (d) and code injection. Communication layer weaknesses of: (a) physical attacks; (b) non-invasive attacks; (c) invasive attacks; (d) privacy violations; (e) profiling; and (f) tracking and surveillance concepts are also defined and explained.

In addressing vulnerabilities, sources of unreliability are identified as: (a) effects of metal and liquids; (b) effects of permeability of materials on tag antennas; (c) interference and noise from other users; (d) tag orientation; (e) reading distance; (f) Electromagnetic Compatibility (EMC) regulations; and (g) cost and power constrained implementations of tag chips.

In addressing security issues the list of security objectives identified and explained are: (a) confidentiality; (b) message content security; (c) authentication; (d) access control; (e) availability; and (f) integrity. Tag and interrogator authentication is addressed. Tag and product authentication issues are also discussed.

In the context of addressing violations of privacy, relevant concepts are elaborated as: (a) privacy of personal behaviour; and (b) privacy of personal data. The number of privacy violations RFID technology can potentially cause are said to be numerous, so the reader is referred to specific literature. Significant issues that must be dealt with by policy formulation or amendment in relation to RFID practice are stated as those generated by the following items: (a) unique identification of all label items; (b) collection of information; (c) dissemination of that information; and (d) mass utilization of RFID technology.

Achieving the privacy objectives discussed so far is seen as to be sought by the deployment of cryptography, so discussion of how those objectives may be achieved begins with a discussion of cryptographic tools. Concepts identified and elaborated into subcategories are (a) primitives without keys; (b) symmetric key primitives; and (c) asymmetric key primitives.

Attacks on cryptographic primitives are classified as: (a) ciphertext-only attacks; (b) known plaintext attacks; (c) chosen plaintext attacks; (d) adaptive chosen ciphertext attacks; and (e) adaptive chosen ciphertext attacks. Attacks on protocols are classified as: (a) replay attacks; (b) known key attacks; (c) im-personation attacks; and (d) dictionary attacks.

In considering levels of security the levels are defined as: (a) unconditional security; (b) computational security; (c) ad-hoc security; and (d) provable security. An explanation is given for each.

The chapter then turns to a consideration of low cost RFID cryptography for which the challenges are defined as: (a) cost; (b) regulations; (c) power consumption; (d) performance; and (e) power disruptions. The impact of all these challenges is discussed.

This chapter also provides a survey of appropriate solutions. These include: (a) use of cryptographic hash functions; (b) use of linear and non linear feedback shift registers; (c) the NTRU cipher; (d) the Tiny Encryption Algorithm (TEA); (e) the Scalable Encryption Algorithm (SEA); and (f) an unorthodox re-encryption mechanism for securing a banknote, employing on the label a cipher text and a random number and on the banknote a serial number and a digital signature.

Lightweight cryptography and lightweight protocols then receive consideration, this material leading to a discussion of minimalist cryptography. Concepts identified and explained are (a) pseudonyms; (b) one time pads and random numbers; (c) exploiting noise; (d) distance implied distrust; and (e) authentication protocols and particularly the YA-TRAP protocol, in various versions, that provides location privacy and allows the authentication of the tag by using monotonically increasing timestamps stored on the tag which are in synchronicity with timestamps on a secure backend database.

The chapter concludes with the notion that security comes in many flavours and strengths, but that low cost implies that we find mechanisms that are generally “good enough” as deterrents rather than mechanisms that are impossible to crack. However, the use of one time codes does allow a great strength over a limited number of reader and tag authentications.

Chapter 7: “Security Vulnerabilities in RFID Systems”

Then Chapter 7 “Security Vulnerabilities in RFID Systems” outlines a weakness, known as an SQL attack that is present in some simple software systems. It is shown that this weakness can fortunately be avoided by good software design, and generally now is. Other forms of attack, such as engineering buffer overflow are also studied, but it is shown that the architecture commonly adopted for an RFID reader will provide protection against such attacks. Finally, various denial of service attacks, that may be mounted through the introduction of broadband noise or unauthorised transmissions, are considered and are warned against. For such attacks the appropriate defence appears to be the identification of their sources and their silencing through the deployment of appropriate legal means.

Chapter 8: “An Evaluation Framework”

In Chapter 8 “An Evaluation Framework” there is presented a framework against which the success of attempts to provide security is later to be evaluated. The problem space is constructed around low cost RFID systems, so as to enable the engineering of solutions to overcome the defencelessness of low cost RFID systems and to be able to evaluate those solutions for their effectiveness. The chapter develops simple evaluation criteria for security mechanisms and a simple, yet sufficient model of a low cost RFID system for analysing security mechanisms.

The chapter provides an outline of low cost RFID system characteristics according to: (a) class; (b) length of unique identifier; (c) read range; (d) read speed; (e) hardware cost; and (f) power consumption. The chapter summarises the important aspects of low cost RFID, that need to be understood and provides reasonable assumptions that need to be made prior to implementing any cryptosystems to address the vulnerabilities implied by the non-achievement of defined security objectives.

There is provided a security evaluation matrix to appraise the suitability of various mechanisms for providing security and privacy to low cost RFID and various applications constructed around low cost RFID.

In the matrix there are to be achieved security objectives of: confidentiality; message content security; tag authentication; reader authentication; product authentication; access control; availability; and integrity. In the matrix there are also to be achieved privacy objectives of: confidentiality; message content anonymity and untraceability. In the matrix there are also cost and performance estimates of: tag implementation cost; back end resource requirements (on line or off line); overhead costs (initialisation cost or time); time estimates (time to complete a process or clock cycles); and estimated power consumption.

Criteria for evaluating security mechanisms and hardware costs are also given. In estimating hardware costs it is common to express the area evaluation in terms of the number of gates (NAND) required. Implementing a NAND gate in hardware requires at least four FETs. Typical cost estimations in terms of the gate count are given for various cryptographic hardware elements.

It is recognised that it is difficult to implement a security mechanism without the aid of proxy systems or a secure backend system for storing secret information such as keys. Security mechanisms of this kind are recognised as requiring online and real time access to secure resources. The monetary and time cost of implementing such mechanisms is considered in the evaluation process. Observing constraints placed on RFID security mechanisms may require expensive database system implementations and expensive networking infrastructure. Backend resource costs are expressed as those requiring online access or those that can be performed off-line.

Overhead costs may result from the need for initializing tags with secure information, or the need for performing some operations prior to their use, or periodically during their use. For instance a security mechanism may require the replenishment of secret keys on a tag.

Under power consumption costs it is recognised that any security mechanism design will eventually involve an IC implementation. Currently, static CMOS is the choice of most digital circuit designs built for low power consumption and robustness.

An important aspect of the design process and the establishment of its suitability is to ensure that the power dissipation of the integrated circuits do not exceed that outlined in the consideration of low cost RFID system characteristics.

Chapter 9: “From Identification to Authentication”

Finally in this group of papers there is presented in Chapter 9 “From Identification to Authentication” a description of how RFID can be used for product authentication in supply chain operations. A review of existing approaches is provided. These approaches are analysed in the context of anti-counterfeiting needs, and fields where future research is needed are identified. It is pointed out that the effort that an illicit actor has to undertake to break or by pass the security mechanisms implemented has a major impact on the cost of product authentication system.

The general requirements of authentication systems in supply chain applications are identified. They include that: the system needs to be used by multiple parties from multiple locations; authentication of products that are unknown to the system should be supported; the cost and effort to perform a check need to be low; and the optimal solution should allow also the customers to authenticate products.

The general attack scenarios of illicit players are described, and range from: taking no explicit action, but relying instead on consumer demand for counterfeits; through the use of misleading bogus security features that are designed to deter closer inspection; through also the removal of authentic security features for genuine products and re-applying them to fake products; to the cloning and imitation of security features.

RFID product authentication techniques are discussed in detail. Particularly promising are the methods that use the unique factory programmed chip serial number (TID) of EPC Class-1 generation-2 tags. However, it is shown that such schemes are not proof against attackers who have access to hardware manufacturing. Tags with cryptographically protected secrets, particularly where the secrets are shared within groups of tags, are vulnerable to those secrets being stolen and sold out by insiders.

There is also discussion of other forms of attack such as denial of service attack of the types discussed in earlier chapters, but such attacks are not considered as realistic threats against RFID product authentication which is mostly performed under the surveillance of authorised personnel or by the customer.

The chapter contains an extensive review of product authentication approaches and their advantages and disadvantages, a section deducing tag requirements for authentication, and concludes that the role of standards is of primary importance in product authentication and should be taken into account in solution design.

This chapter is notable in that it contains 67 references and, in an Appendix, a comprehensive table summarising the requirements of different product authentication approaches.

Section 3 Network Based Solutions

Section 3 contains three chapters that outline solutions to the authentication problem by exploiting characteristics that can be introduced into the communication network.

Chapter 10: “EPC System for Safe and Secure Supply Chain and How it is Applied”

The material in Chapter 10 “EPC System for Safe and Secure Supply Chain and How it is Applied”, while being drawn from Japanese experience, can be considered to be applicable everywhere. The overall aim of the chapter is to explain how EPC systems improve safety and security.

The chapter begins with gray markets and black markets being defined, paths into an out of legitimate market being identified, and short term issues (expired products, wrong handling of products) and long term issues (product recall arising from later discovery of defects) issues being described.

Five stages of the supply chain from manufacturer, through wholesaler, repackager, and retailer to the consumer are defined.

The view of the Chapter is summarised in six tables all well supported by text argument.

Tables 1, 3, and 4 all consider threats classified as: fake label; adulteration; relabelling; substitution; fake product; stolen; gray market; scrapped; and recall; and these nine items are grouped into the three classes of: counterfeit; illegal trade; and wrong status.

The six tables describe in order: threats and entry points; basic applications (one physical and three informational) for securing a supply chain; threats and entry points, now revised to exclude out of scope items such as fake labels or adulteration by the manufacturer; measures that may be deployed to secure the supply chain, grouped as to whether they are covered by the EPC system or not; mapping of security measures to EPC systems components such as EPC, Tag, Reader, Middleware, EPC-IS or ONS; and network availability influence of security measures.

The Chapter considers that EPC components being standardised currently may not be sufficient to realise all the security measures required. Potential research topics arising from that fact include: ID encryption; access control to the tag; management of exposure of tag identifiers; electronic document validation (not yet sufficiently pervasive); business processes to manage product status beyond EPC-IS; need for ONS security; and need for a tamper evident tags.

Chapter 11: “The Potential of RFID and NFC in Anti-Counterfeiting”

In Chapter 11 “The Potential of RFID and NFC in Anti-Counterfeiting”, the authors investigate how RFID and Near Field Communication (NFC) could improve current customs processes to fight illicit trade.

In current import processes, customs officers have to evaluate which consignments are inspected and, when an inspection takes place, whether intellectual property rights have been infringed. The authors propose and evaluate new micro processes that leverage the dual-existence of products and logistic units in order to enable easier, faster and more reliable inspection of goods.

The significance of the work rests on the fact that the majority of counterfeit products in the Western countries are imports and the most important means of transport of counterfeit products is by sea.

Customs are responsible for about 70% of all seizures of counterfeit products in the world [2]. The role of customs is especially important in protecting the European Union and the U.S. because the vast majority of counterfeit products in those markets are imports and, after entering the market, subject to free circulation within the community.

Customs authorities fail to seize large amounts of counterfeits either because they do not know how to recognize the fakes or because the process of gathering statements from trademark owners is too time-consuming.

While controlling the trade, however, customs also work to facilitate the trade and seek not to disturb import and export. These two objectives conflict, and thus customs always have to balance between control and facilitation. Given also that the vast majority of goods that pass through customs are legal and should not be disturbed, finding counterfeit goods is not among customs’ top priorities.

Customs use RFID also to strengthen the security of consignments. To guarantee the integrity of cargo, shippers install electronic seals, or *e-seals*, into their containers. The role of RFID in the e-container is to provide connectivity and real-time telemetry.

One consequence of this trend is the emerging of *green lane* programs where shipping companies gain lighter inspections when they conform to certain additional regulations, such as in the Smart & Secure Tradelanes (SST) initiative or the Customs-Trade Partnership Against Terrorism (C-TPAT).

Customs conduct risk analysis to identify high-risk consignments in pre-hand. Regarding counterfeiting, the country of origin is the most important criteria in the risk-analysis and, consequently, it is often attempted to be disguised by the carriers of counterfeit goods. Careful selection of inspected containers can provably provide considerable improvements in the detection rates of counterfeit products.

The authors propose the use of Near Field Communication devices, and in particular RFID tags operating at 13.56 MHz. The devices apply touch to read principle which makes communication easy and intuitive, and the typical reading ranges vary from 0 to 20 cm. Besides reading NFC tags, the protocol allows for secure two-way communication between the reader devices. This differentiates

NFC from RFID technology used in supply chain applications, where the goal is mostly to read multiple tags at once without line of sight.

The authors propose new micro processes that can be used to improve the existing customs import process to find and seize more counterfeit goods. The enabling technology of the proposed processes is any hand-held NFC device with a network connection, such as already available NFC mobile phone. This device allows the customs officers to read tagged items in their field work. It is taken into account that in a modern customs process, the flow of information and the flow of goods are separated and therefore the customs officers need to move to the warehouse to conduct the physical inspections. In a very lean and automated import process, the time that the products spend in the customs warehouse can be very small and measured in tens of minutes, which can set rigid time-constraints for the inspections.

The process steps are the following: (i) identify the product by reading the tag; (ii) obtain the network address of the authentication server using a network address resolution mechanism (e.g., Object Naming Service); (iii) establish a secure connection with the authorized server (e.g. EPC PAS); (iv) establish which authentication protocol, if any, the tag supports; (v) automatically authenticate the product (tag) using the supported protocol; and (vi) verify the tag-product integrity.

It should be kept in mind that usually it is actually the tag that is authenticated and not the product itself. Therefore verification is required to make sure that the authenticated identity really matches the physical product (step vi). Omitting this verification makes the system vulnerable to simple attacks where fake goods are equipped with any authentic tags.

Though RFID is already used in customs logistics in different ways today, it still has unused potential to help customs in the fight against illicit trade. In this Chapter, the authors have presented how, together with NFC enabled mobile reader devices, RFID enables product authentication applications that make inspection of tagged cargo faster and more reliable.

Chapter 12: “Improving the Safety and Security of the Pharmaceutical Supply Chain”

Chapter 12 “Improving the Safety and Security of the Pharmaceutical Supply Chain” discusses various techniques that may be used to combat counterfeiting in the pharmaceutical supply chain. These include the use of electronic pedigrees (to ensure the integrity of the supply chain), together with mass-serialization (to provide for a unique lifecycle history of each individual package) and authentication of the product (to check for any discrepancies in the various attributes of the product and its packaging are as intended for that individual package). Management of the pedigree process and product authentication is discussed in some detail, together with various other learnings from the Drug Security Network, including identification of some remaining vulnerabilities and suggestions for tightening these loopholes.

The Drug Security Network (DSN) was formed as a forum for a number of major players in the pharmaceutical industry to consider the major changes and challenges to business practices which will result from the enforcement of pedigree legislation and introduction of mass-serialization, which are being introduced imminently in order to make the pharmaceutical supply chain safer and more secure.

The paper discusses in turn the primary deliverables (three papers) of the DSN activities.

The purpose of a pedigree is stated as providing legal proof of a secure chain of custody from the originator of the pharmaceutical package (usually the manufacturer or wholesaler) through to the organization that sells or dispenses the pharmaceuticals.

Three key issues needing to be considered are: Pedigree Data Content/Format; Pedigree Processing; and Pedigree Transmission Mechanism.

A number of key requirements are identified for a standardized format for electronic pedigrees. These are: completeness; global scope; suitability for legal or government audit; and integrity, authentication and non-repudiation.

A number of key requirements are identified for the transmission mechanism for electronic pedigrees. These are: timely access to data for verification and certification processes; robust access to data for verification and certification processes; authentication, integrity and non-repudiation; and suitability for legal/government audit.

The Propagating Document Approach and the Fragmented Data Approach are identified with the former being the most favoured.

In that approach, each subsequent custodian verifies the signed content of previous custodians, then amends and re-signs the data, before transmitting the pedigree to the next custodian when the goods are shipped onwards. As the pedigree document moves across the supply chain, additional outer layers are added. This approach offers a double-linked chain of security, since each custodian can verify all the inner layers of the pedigree document, then signs to confirm that they have done so (the reverse link). At the time of shipping, they then add additional data about the next recipient and sign this (the forward link).

It is pointed out that a pedigree document primarily records a chain of transactions. It does not warrant that the package itself is the genuine product. For this, authentication is required. Two kinds of authentication are discussed: authentication of the identity, since the identity provides the 1–1 link to the pedigree data; and authentication of the product itself, in case the identity of the package has been copied or the details about the product have been falsified.

It is explained that a key feature of the Safe and Secure Supply Chain is the emphasis on authenticating the object, as well as the pedigree trail. A networked information system, such as one complying with the future EPC Information Services (EPCIS) standard, would provide a mechanism for a manufacturer or labeller (or other authoritative party) to be able to validate a number of properties specific to a particular serial number. These might include an independent hard-coded read-only tag ID, the product class and/or details of customized security features, either covert or overt.

It is further explained that when validating the authenticity of the product, it may be necessary to check the following criteria: authenticity of the tag; authenticity of the pedigree ID; authenticity of the serialized identifier; authenticity of the product's packaging; checking the current state; and authenticating the trail.

Three groups of use cases are considered.

In the discussion on security of business documents in general, the following five key security requirements are identified: authentication; authorization; confidentiality; integrity; and non-repudiation

The concept of a Pedigree Business Document is introduced, and the risks of paper pedigree are considered in some detail. The paper identifies a number of potential loopholes of paper-based pedigree documents. These include that: a fraudulent wholesaler can sell counterfeit items with legitimate paper-based Pedigree documents; and a fraudulent wholesaler may forge paper-based Pedigree documents and sell counterfeit items saying they are returns from the retailer. Thus it is explained that using paper-based Pedigree documents increases the risks of entry of counterfeit drugs.

Cross-border shipments and diversion are also discussed. Vulnerabilities in the form of potential loopholes in the security of proposed pedigree legislation are discussed, and the need for certification authorities is also established. Enforcing a change of serial ID and labeller code on repackaging is seen as essential.

Section 4 Cryptographic Solutions

Section 4 consists of six chapters that describe solutions to the provision of authentication services by exploiting cryptographic concepts that may be introduced within RFID labels.

Chapter 13: “Product Specific Security Features Based on RFID Technology”

In this chapter, the authors propose a security solution based on Radio Frequency Identification (RFID) technology, using low-cost transponders that contain item-specific information to avert removal-reapplication attacks. The proposed solution aims at providing unique and secure authentication.

The approach utilizes RFID technology in which transponders hold unique and cryptographically secured data that uniquely binds a given instance of product to a given tag, and thus makes duplication or re-application of tags difficult.

A solution based on signed product characteristics is proposed. The main components of the architecture are an RFID tag containing product specific validation data introduced by a branding machine, explained below, and a product verifier containing an RFID reader, a crypto engine and a communications interface to a key data base.

The system allows setting up a secure and authentic binding between a product and a passive RFID tag residing on that product.

The Branding Machine is mainly responsible for computing and writing of the unique and secure product validation data to the tag. The component called product verifier is able to determine whether the product validation data delivered by an RFID tag is authentic and thus indicates the tagged product's authenticity. The product verifier will have the modules RFID reader, a crypto engine, and a communication interface.

In operation, the RFID reader component requests the RFID tag for the product validation data stored on that tag. The crypto engine is responsible for checking the authenticity of the product validation data read by the RFID reader and also for determining whether the product validation data has been altered by an impostor which event would be an indicator for a faked product. The communication interface can be used to determine authentic cryptographic keys from the (optional) component called key database. The usage of the key database can be eliminated by storing known verification keys either on tags or on product verifiers.

The unique product identifier contains, as well as cryptographic parameters, a bit sequence that uniquely characterizes the given product. Typically, this information is determined by the product's vendor. Depending on the specific type of product, different physical, chemical, etc. properties that can be verified, i.e. detected or measured, by a (human or machine) observer. Example properties that – either altogether or in a subset – can uniquely characterize a product with a certain high probability are weight, electric resistance, geometry, or a serial number printed on the product itself or its packaging, etc. This data will typically be written on the tag by the product's vendor before product delivery, for example during packaging. It is also possible to place a reference here, such as an URI that specifies a dataset stored on a remote database. This may help to save tag resources, but will make product validation dependent on the availability of that external storage.

In summary in this Chapter, the authors propose an anti-counterfeiting security solution based on RFID and EPC technology, which is applicable for passive, hopefully low-cost transponders. The exceptional feature of the approach is that the tags contain verifiable, item-specific information. Thus, a tag which is applied to a product is tightly bonded to that item, providing a measure to avert cloning attacks. The solution is also adaptable for offline checks if no network connection is available. However, the applicability of the proposed solution depends very much on the availability of unique, product specific properties which are easy to observe.

Chapter 14: “Strengthening the Security of Machine-Readable Documents”

Chapter 14 “Strengthening the Security of Machine-Readable Documents” considers the on-going trend towards turning paper documents that store personal information or other valuable data into machine-readable form, an example being the electronic passport that will become common in the near future.

The Chapter shows how the security of these machine readable documents could be improved by combining RFID with optical memory devices, integrating an optical memory device into the RFID enabled smart document to produce methods by means of which these two storage media can be combined to secure the document against threats like illicit scanning, eavesdropping and forgery.

The approaches described make use of the optical document-to-reader channel which is considered to be more secure than the radio-frequency communication interface. They are relevant to numerous applications where tagging physical documents would be interesting. Besides e-passports and other travel documents, customs freight papers, security papers (e.g. gift certificates, jewellery appraisals), driver's licenses and vehicle registration papers that would benefit from being machine readable through radio-frequency (RF) communication provide examples. A common factor of these documents is that they all relate to a physical entity that is not very well suited to being tagged to become a data carrier itself.

Four different approaches, defining how this combination of an optical and rf channel could be used to overcome existing security threats of machine readable documents, in terms of more secure communication protocols and resistance against forgery and cloning, are described. Instead of establishing security based on sharing secrets between the reader device and document before the communication, the approaches make use of optical memory devices which cannot be read or eavesdropped without a line of sight.

Machine readable documents are defined and discussed. All physical documents that carry a digital memory device are considered as machine readable documents. The typical instance of these kinds of documents is an RFID tagged paper, but another way to make documents machine readable is to use optical character recognition (OCR) to read data printed on the document. Machine readable travel documents (MRTD) comprise e-passports, visas and special purpose ID/border-crossing cards. Because of their similar nature, driver's licenses are also included within this group.

The benefits of having RFID transponders in physical documents come from the simple and fast read process that does not demand a line of sight connection. Depending on the grade and price of the chip, the contactless memory device can also contain support for re-writable memory and logical functions like cryptographic primitives. Therefore machine readable documents can provide high level of security and counterfeit resistance.

The significant components of an RFID enabled machine readable document application are the document itself, the reader device and the reader's control and crypto unit. Typically the transponder stores at least a unique identifier (UID) number. In addition, the transponder can provide logical functionalities like access control (through key comparison), random number generation and data encryption. Thus, the transponder serves as more than a mere barcode label.

Without specific encrypted addressing, the RFID air interface is not secure and the transponder is vulnerable to clandestine scanning (or *skimming*) and eavesdropping.

The reader device is responsible for the wireless communication. It is connected to the control and crypto unit through a closed, secure channel.

The role of the digital memory devices in the authentication processes of travel documents is twofold: on the one hand they help authenticating the traveller and on the other hand they help proving the authenticity of the document itself.

E-passport design has to address needs for individual privacy and national security and thus it poses severe security and privacy requirements. First of all, the integrity and authenticity of the data the passport stores has to be guaranteed. Second, the data has to be kept confidential from non-authorized parties. Third, the passport must not pose privacy threats for its carrier and, furthermore, all these have to be fulfilled in a public system during up to 10 year long life-span of the passport.

The authors describe the studies of Juels et al. who have discussed the security issues of e-passports and in which the following four threats, among others, were brought into light: (a) clandestine scanning; (b) clandestine tracking; (c) eavesdropping; and (d) cryptographic weaknesses. Moreover, those authors concluded that the e-passports do not provide sufficient protection for their biometric data.

The last of these concerns is relevant regarding forgery because without this connection, the system can be fooled, for example by putting a valid transponder into a fake paper.

Scarce resources on the chip limit the use of cryptographic primitives and the goal of the design is often low-cost low-security features.

The chapter then considers how optical memory devices can be combined with RFID to overcome some of the security threats of machine readable documents. The addressed security issues comprise: (a) no connection between chip and paper; (b) data integrity; (c) clandestine scanning; (d) clandestine tracking; and (e) eavesdropping. The first two issues are seen to relate to the security of the overall system and the latter three to the unsecured wireless communication.

Integrating an optical memory device into the RFID enabled machine readable document is proposed. What is common to all optical memory devices is that they need a line of sight connection for reading, making them resistant against clandestine reading and eavesdropping. Therefore it can be assumed that this channel is secure. The addition of an optical memory device extends the communication channel between machine readable document and a reader device to provide the combination of an insecure (RFID) channel and a secure (optical) channel.

Four approaches showing how the combination of RFID and optical memory devices can be used to increase the security of machine readable documents are described. The first two approaches address data integrity and bind the chip and the document, while the two other approaches aim at securing the communication.

Because machine readable documents often relate to a physical entity, it is assumed that data of interest that the document stores relates to this entity. That data is denoted as *object specific data* and it can be used for example in authentication. In addition, the documents can store any other application specific data which is merely referred to as *other data*. This other data can be static or dynamic. The way in which data can be used are: (a) storing object specific data in the optical memory; (b) storing a hash of object specific data in optical memory; (c) storing access keys in the optical memory; or (d) storing session keys in optical memory.

In the first approach static object data is stored in both the RFID transponder and the optical memory. This mirroring of the data increases the reliability of the overall document and provides a mechanism to tell if one or other device has been

tampered with. However, the optical memory does not provide access control and is vulnerable to skimming if the document falls into the wrong hands.

In the second approach the optical memory device stores only a hash value of the data. The used hash function needs to be known by the party performing the data integrity check so the specification of the hash function is stored on the chip. A smaller optical storage is needed.

In the third approach the RFID transponder does not reveal the object specific data if no correct access key has been transmitted in advance, which approach prevents clandestine reading. The access key is stored on the optical device and can only be read with line of sight connection. This means that, proved the document is safeguarded by its owner, the document owner can control who has access to the contactless memory.

In this approach the RFID reader initiates a reading session by asking the transponder for an index i between 1 and N , where N indicates the number of access keys stored in the document. Because single access keys can be still obtained by eavesdropping the radio channel between the reader and the transponder, the number of access keys N needs to be large enough to make the malicious use of compromised keys infeasible and spoofing of access keys difficult.

In the fourth approach the transponder challenges the reader for a response to be read from the optical device. A challenge response operation is initiated by the tag transmitting a pseudo random challenge and an integer in the range 1 to N , where N is the number of session keys held in the optical memory device. To authenticate itself to the transponder, the reader device sends a response which is the challenge encrypted by the session key obtained by reading the optical device. The session key is also used to encrypt the following wireless communication of object specific data.

Most importantly, the session key is never transmitted in the insecure radio channel as this key is only optically accessible, which overcomes the weakness of an approach that may involve compromised access keys. On the other hand, this approach requires the transponder to support data encryption.

The authors see the main benefits of combining RFID with optical memory devices as lying in the field of document security. The use of two memory devices adds complexity to the system and thus makes the documents harder to be cloned or forged. Even though this conflicts the fundamental security doctrine of Kerckhoffs which says that the security of a system should depend on its key, not on its design obscurity, it is believed that it can provide effective ways to combat counterfeits.

Chapter 15: “Enhancing Security of EPCglobal Gen-2 RFID against Traceability and Cloning”

In Chapter 15 “Enhancing Security of EPCglobal Gen-2 RFID against Traceability and Cloning” the authors present a synchronization-based communication protocol for EPCglobal Class-1 Gen-2 RFID devices. The proposed protocol is secure in a sense that it prevents the cloned tags and malicious readers respectively from impersonating and abusing legitimate tags. In addition, the protocol provides that

each RFID tag emits a different bit string (pseudonym) or meta-ID when receiving each and every reader's query. Therefore, it makes tracking activities and personal preferences of tag's owner impractical and thus ensures the user's privacy.

As background, the authors observe that despite many prospective applications, RFID technology poses several security and privacy threats which could harm its global adoption. Ironically, the security weakness of RFID technology comes from the most basic operation of an RFID tag, that is to release a unique and static bit string known as the Electronic Product Code (EPC) identifying the object associated with the tag upon receiving a query request from a reader. Using the unique EPC as a reference, someone (equipped with a compatible reader) can track the moving history, the personal preferences and the belongings of a tag's holder. Even worse, absence of secure authentication results in revealing the EPC to malicious readers under a skimming attack. Once capturing an EPC, an attacker can duplicate genuine tags and use the cloned tags for its malicious purposes. A natural solution to the aforementioned security problems is to employ cryptographic protocol in the RFID system. Unfortunately, the cost of manufacturing a tag has to be extremely low, e.g., less than 30 cents (according to RFID journal, one RFID tag is expected to cost 5 cents by 2007). Therefore, the computationally intensive security protocols widely known in cryptographic literature cannot be incorporated into a small chip with tightly constrained computational power (at least in the foreseeable future).

The authors point out that the latest RFID standard ratified by EPCglobal is named EPCglobal Class-1 Gen-2 RFID specification version 1.09 (Gen-2 RFID for short). with the properties: (a) tags are passive; (b) communication is in the UHF band with range up to 10 m; (c) tags support on-chip PRNG and CRC computation; (d) privacy protection mechanism is to make the tag permanently unusable once it receives the kill command with a valid 32-bit kill PIN; and (e) read/write to memory is allowed only after it is in secure mode after receiving access command with a valid 32-bit access PIN

The authors argue that that privacy protection mechanism suggested in the specification is inappropriate, and many scenarios the tag should never be killed. Therefore, in designing a new protocol, they have avoided this kind of mechanism and, make a new use for the *kill* PIN.

For the *access* PIN, the authors point out that it is ineffective from a security point of view since the 16 bits of PIN is XORed with a 16-bit pseudo-random number sent by the tag in a session. Just by eavesdropping the 16-bit pseudo-random number and the XORed PIN, an attacker can easily recover the access PIN. Losing the access PIN is very dangerous because it allows a malicious reader to read/write the entire memory of a tag.

Although researchers have proposed protocols making use of a hash function, such protocols are seen as still beyond current capability of low-cost RFID tag. Thus, the authors have sought another solution which should use only the available functionalities of current RFID standards.

Although Juels has suggested such a scheme to prevent the legitimate tags from being cloned, it is pointed out that his protocol does not take eavesdropping and privacy issues into consideration, and thus provides no protection against privacy invasion and secret information leakage. In their paper, the authors present another scheme targeting most of security features for a RFID system including authentication,

traffic encryption, and privacy protection. An important feature is that the only trusted party in the proposed RFID system is the backend server and all the secrets are kept only at the tags and the backend server's database. In addition, the RFID reader is not be able to learn any secret information including PIN and EPC itself from data called *meta-ID* sent by a tag.

In the proposed protocol the meta-ID is forwarded to the backend server and the backend server can retrieve detail object information keyed by that meta-ID. The advantage of this approach are described as being: (a) the approach enables easy accountability and access control; and (b) instead of reader to tag authentication, the protocol requires the reader to authenticate to the backend server before sending a meta-ID.

There is a discussion of random numbers and their generation leading to the conclusion that the Gen-2 standard should support 32-bit PRNG to take full advantage of 32-bit PIN currently supported by Gen-2 specification. In the proposed protocol, use is also made of checksum code to provide security and resolve possible collisions at the backend server's database. To avoid a problem with checksums on all zero strings, a bit string is required to start with a bit 1.

In explaining their main ideas, the authors describe first protecting data transmitted between the tag and reader against eavesdropping. The obvious way to them is to utilize encryption/decryption and the most simple encryption function useable is XORing. The problem now turns to the key management issue: that is to ensure that a new encryption key is used in every session. Solving this issue turns out to be a solution to privacy protection as well since RFID tag can XOR EPC with different key in every session, thus, preventing malicious readers from tracking the tag. They suggest that the simplest, yet most efficient way of key sharing in this scenario is to use the same PRNG with the same seed at both RFID tag side and backend server. The session key can be computed by generating a new pseudo-random number from a current session key after every session. Importantly, this computation is required to be done at both RFID tag and reader/backend server in a synchronous way. Otherwise, subsequent traffic cannot be understood by both sides.

The next security problem discussed is the need for authentication. It is argued that in most cases, a reader just needs to know EPC stored in a tag and then eventually contact the backend server to get/update information about the object carrying the tag. Keeping this in mind, it is proposed that reader-to-tag authentication can be delegated to tag-to-backend server authentication. More specifically, a reader can only receive an EPC from an RFID tag in an encrypted form. It needs to authenticate itself to the backend server first, and then, depending on its privileges, that backend server can decide what kind of information to send back to reader (for example, in case of a public reader, only information describing what the referenced object is; and in case of a manufacturer's reader, the actual EPC and PIN associated with that tag can be sent). Actual reader-to-tag authentication needs to be carried out when reader wants to access (read/write) other sections of tag's memory bank. To do so, it is stated that the protocol can use a PIN-based approach just like in the original Gen-2 RFID specification.

A detailed discussion of the protocol and its sub protocols is provided. A possible synchronization issue with the protocol is recognised in that a false

‘End Session’ message might be sent by a malicious reader, and a method to prevent such interference is proposed.

In summary, the authors have presented a simple communication protocol for RFID devices, especially EPCglobal Class-1 Gen-2 RFID devices. The proposed protocol achieves desirable security features of a RFID system including: implicit reader-to-tag authentication, explicit tag-to-reader authentication, traffic encryption and privacy protection against tracking. The scheme makes use of only PRNG and CRC which are all ratified in the current Gen-2 RFID specification. It is claimed that there should be little overhead in adapting the proposed protocol into the Gen-2 RFID specification.

Chapter 16: “A Random Number Generator for Application in RFID tags”

In Chapter 16 “A Random Number Generator for Application in RFID tags” the authors observe that in current RFID technologies, pseudo random number generators (PRNG) serve as random number sources, but claim that their output numbers can show poor statistical properties, and that less than properly random secret keys reduce the security of data transmission. The objective is to show that an oscillator-based Truly Random Number Generator (TRNG) provides a better solution.

The TRNG exploits thermal noise of two resistors to modulate the edge of a sampling clock. The white noise based cryptographic keys prevent potential attackers from performing any effective prediction about the generator’s output even if the design is well-known. The objective of this chapter is to discuss how to realize a TRNG in an RFID tag system.

Due to the confidential nature of most cryptographic systems, relatively few hardware RNG designs have been published. Designs available in the literature reveal three different IC-compatible methods for producing truly random sequences: (a) direct amplification; (b) oscillator sampling; and (c) discrete-time chaos. In the work reported here, several TRNGs were modelled, analysed and compared with the method of direct amplification. The results show that the oscillator-based TRNG is almost free from $1/f$ noise and periodic influences of substrate and power supply. These advantages make the oscillator-based TRNG a desirable solution for RFID tag application.

In an oscillator-based TRNG, a jittered low-frequency clock is used to sample a high-frequency clock. Two resistors’ thermal noise is amplified to dither the edges of the low-frequency clock. The high-frequency clock is derived from the tag’s analog front-end. According to EPCglobal RFID Class-1 Generation-2 Protocol, it should be n times of 1.28 MHz, where n is an integer.

An operational amplifier is used as a noise amplifier. The noise of a noise resistor is amplified by the operational amplifier and added to a triangular wave. The amplified noise output follows a Gaussian probability density and of variance proportional to the value of its resistance.

The Chapter contains extensive analysis of circuits and probabilities of output values. In designing the oscillator-based TRNG, a main factor which influences the

statistical properties of the output sequence is the sample rate. In the finite bandwidth system proposed, the highest sample rate is limited by the noise amplifier.

In order to eliminate the correlation between the 16 bits of the output random number, it is shown that the sample rate must be roughly less than 1.5 times the bandwidth of the noise amplifier. Because the bandwidth of an operational amplifier is a function of power consumption, the highest sample rate is actually limited by the total power available.

The lower limit of sample rate is determined by the period of tag to reader communication cycle. The TRNG must provide 16 bits of truly random number within this period of time. According to EPCglobal RFID Class-1 Generation-2 Protocol, the minimum time of this period equals to 465 microsecond.

To implement TRNG in the RFID tag, there exist two main constraints: power consumption and chip area. In the proposed scheme, the most important factor is to keep the total power consumption of the low-frequency oscillator at around 1 microwatt. With the state of art, at a power supply voltage to 0.8 V, the total current consumption should be no more than 1.3 microamp.

For low power consideration, the output white noise needs to be as small as possible. In respect that the oscillator-based TRNG shows good quality against $1/f$ noise and some periodic influences, the lower limit of the output white noise is the resolution of the hysteresis comparator. Therefore, it is recommended that the noise magnitude be higher than 3 mV. The difference between the threshold voltages of the hysteresis comparator should be big enough to overcome the input offset, but it may not be too big as to increase the power consumption. Here, the value of 50 mV is chosen.

In exploring trade-offs of power consumption and chip area some new structures of low power operational amplifiers using subthreshold techniques were explored and four options emerged. There exists a trade-off between power consumption and a resistance. In order to control the current consumption of the operational amplifier, more chip area is needed for a large resistance value. Fortunately, accurate absolute resistance is not a rigid requirement, so well resistors with relatively high resistance can be used.

The constraints relating power consumption and chip area appeared to lead to a large chip area and a lower random number output rate. In order not to make these sacrifices, two system level optimization methods were employed to improve the overall performance.

One is a method of combining a TRNG and PRNG in which a 1-bit truly random number is added in the cycle ring of a PNRG so that the output sequence of the LFSR will also be as unpredictable and irreproducible as a TRNG.

By incorporating a 1-bit truly random number in the random number seed instead of generating 16 bits within the time limit, the lower limit of sample rate can be decreased to 2.2 kHz, thus remarkably cutting down the power consumption.

Power-on generation is another solution to deriving high quality random numbers with limited power consumption. The basic idea of power-on generation is to generate all the random numbers that will be used according to security protocols before other circuit blocks are awoken. Right after power on, the tag is set to random number generation mode. During this period of time, the TRNG is turned on, and most of the other circuit blocks in the tag are in sleep mode. The

tag will not respond to the “Query” command sent by the reader until all the random numbers are prepared.

In summary, this Chapter introduced the principle of an oscillator-based TRNG. By characterizing the TRNG’s power consumption, sample rate, chip area, and the quality of the output, the authors show that it is possible to implement a TRNG in the RFID tag system as a solution to security problems. Finally, two system level optimization methods were proposed to reduce the power consumption of the TRNG.

Chapter 17: “A Low Cost Solution to Cloning and Authentication Based on a Lightweight Primitive”

In Chapter 17 “A Low Cost Solution to Authentication Based on a Lightweight Primitive” the authors explain how a Physically Uncloneable Function (PUF) generated within an RFID tag may be used for lightweight encryption, permitting both reader and tag authentication.

The Chapter observes that the lowest cost tags pose, because of their wide scale deployment, the greatest threat to security and privacy because constraints of silicon area and circuit complexity pose severe limitations on the possible solutions to the implementation of cryptographic primitives.

A primary concern with current low-cost RFID systems is the cloning attack, which operates to defeat the track and trace features so often desired in RFID systems. This is particularly so when there is no mechanism for a reader to verify that it is communicating with a genuine label, not a fraudulent label. It is noted that labels and readers are constantly in an un-trusted environment where the integrity of messages is doubtful.

The paper discusses briefly the use in authentication of public and private keys, and hash functions operating on strings of plain text, but is unable to offer mechanisms that can be implemented with sufficiently small silicon area.

The goal of an authentication scheme in RFID is seen as preventing an adversary from creating a fake tag to misrepresent a legitimate tag.

Challenge and response protocols are discussed. While it is possible to construct a challenge and response protocol using a variety of cryptographic tools, the currently available solutions are expensive in terms of silicon area.

Physically Uncloneable Functions (PUF) are then defined. They have the properties that it is easy to compute a response to a challenge, but it is difficult to model the behaviour of the circuit that generated them. It is easy to construct on standard CMOS processes circuits that generate those functions. The PUF generating circuits are stated as being immune to discovery by physical attacks as they would be destroyed by the attack. They are also seen as having the property that it is not possible to tamper with the measurement data.

The idea behind the circuits to make use of process variations, which are beyond the control of the manufacturer, in wires and transistors on an integrated circuit to obtain a characteristic response from each circuit when a given input is applied. Circuit implementations for an arbiter-based POF are shown.

It is pointed out that even if a single bit responses from different circuits on a single wafer are somewhat correlated, about 800 challenge response pairs are sufficient to distinguish one billion chips with a probability of $1 - 5 \times 10^{-10}$. Such an identification scheme can be implemented with less than 1000 gates.

A block diagram of a label with a puff circuit block is provided. In the security engine there is an input and output buffer for storing the next challenge to be sent to the circuit while the output buffer will buffer up to 100 response bits. The idea is to compare responses to randomly selected challenge sets with expected responses that have been obtained from a secure database.

Some techniques in which XOR operations are conducted between different bits of a long response to produce a shorter response are described. These can have the effect of making it difficult for an attacker to analyse the content of the challenge-response pairs unless that attacker can arrange to eavesdrop on a number of different authentications in different environments.

Authentication schemes to authenticate a reader and for a reader to authenticate the tag are also described. In this scheme the tag stores a one-time pad and a secret key and the reader has access to the tag related information stored on a secure database. Again about 800 challenges are need to be able to effectively identify billions of chips.

There is also description of the tag authentication scenario when the physical implementation of the hash function achieves a critical cost effectiveness required for low-cost RFID, but regrettably it appears that there are no suitable candidates for such hash functions, and that material is seen as supporting the argument for the PUF circuit solution.

There is an evaluation matrix for schemes based on physically uncloneable functions. In that matrix the security objectives are tag authentication and reader authentication. Items quantified are: gate count in the combination of puff block, buffers and a challenge set storage; and performance in terms of the authentication speed showing about 400 milli seconds for completion. Reducing the number of challenges to 128 instead of 800 and using a LFSR arrangement to feed the PUF circuit allows the authentication speed to rise to about 600 tags per second.

In considering overhead costs it is noted that tags need to undergo a verification phase prior to deployment to generate an adequate number of challenge-response pairs for each tag, and of course that implies storage costs within the database.

Practical issues such as sensitivity to environmental conditions are also considered. It has been shown that the circuits are robust against environmental variations for realistic changes of temperature and regulated voltage. The output noise remains below 9%, such variations being significantly less than the between-chip variation.

References to probable attacks are given, but the attacks themselves are not discussed.

In conclusion it is stated that the PUF is considered to provide a cost-effective solution to authentication in low-cost RFID systems. It is considered that future work should be on elaborating common RFID protocols to allow the incorporation of authentication commands of the type discussed in this chapter.

Chapter 18: “Lightweight Cryptography for Low Cost RFID”

This chapter proposes a number of practicable solutions, based on lightweight cryptography, that address the security objectives and privacy goals outlined in Chapter 6 of this book and in the low cost RFID framework outlined therein. The proposed solutions are then evaluated for their merits using the evaluation framework developed in Chapter 8.

The majority of the proposals aim at removing complexity from the label to other proxy systems and limiting any security related computation on the chip to simple operations.

Implementations of the mechanisms are considered in the context of the C1G2 air interface protocol.

Notational aspects to improve the clarity of the discussions are reviewed, and the properties of a cycling redundancy check (CRC) of a number are discussed in detail.

Four essential approaches to stream cipher design are listed. The term linear complexity, which is an important concept in the study of stream ciphers, is defined and discussed. It is stated that since no mathematical proof of security can be found for feedback shift register based key-stream generators, system theoretical designs based on established guidelines and testable security properties are to be reviewed.

Linear Feed Back Shift Registers (LFSRs) are discussed in detail. It is noted that the output bit string of LFSRs are not secure even if the feedback scheme is not known.

Based on a system-theoretic approach the most common practices in making LFSRs secure is to use a nonlinear Boolean function to generate nonlinearity in the output, or employing irregular clocking of LFSRs. Two generators based on the previous ideas and suitable for RFID applications are considered.

Various stream ciphers based on non linear feedback shift registers, linear combination generators (the use of several LFSRs to build a single stream cipher), nonlinear filter generators and clock controlled generators which eliminate the linearity properties of the LFSRs, are discussed. The shrinking generator, implemented using a pair of simple shift registers, is considered to provide such a stream cipher and is said to be secure provided that it is implemented prudently. Its properties are reviewed. It is stated that these generators have survived much public scrutiny and they can be concluded to be computationally secure.

A number of practical guidelines that should be followed to avoid stream ciphers based on LFSRs falling to the prey of adversaries are discussed.

Two generators based on LFSRs, the nonlinear filter generator and the clock controlled generator, are discussed. The key stream generator called the knapsack generator based on the summation of a set of weights selected based on the register values of a LFSR to generate an integer sum S , is discussed and it is stated that provided that such a sub set exists the problem has been proven to be NP-hard.

In clock controlled generators the idea is to use a combination of LFSRs so that the output of one LFSR controls the clocking of a second LFSR. This stream cipher attempts to defeat attacks based on the regular clocking of LFSRs. The

previously mentioned shrinking generator provides an example of a clock controlled generator that is suitable for implementation on an RFID label. The security of the generator has survived many known attacks on LFSR based systems, especially due to the very long period of the generator.

The order of complexity of known attacks is a function of the length of both LFSRs in the generator and has exponential time complexity. Shrinking generators are considered resistant against efficient cryptanalysis attacks due to the difficulty of the attack scenarios and the time order complexity of the algorithms. It is stated that for maximum security the following implementation considerations should be satisfied: (i) use of secret connection polynomials that are not sparse; (ii) use of maximum length LFSRs; and (iii) the lengths of LFSR should have no common divisor other than 1. The irregular output of the shrinking generator may be solved by buffering the key stream prior to its use.

Techniques for reducing power dissipation in CMOS circuits are discussed.

Although the underlying concepts and the use of Physically Unclonable Functions (PUF) have already been illustrated in Chapter 17 of this book, the use of PUF is further extended in this chapter to provide a confidentiality service.

It is shown that the combination of a PUF circuit block with a stream cipher can create a practicable and a powerful solution capable of delivering both an authentication service and an encrypted communication channel. The mechanism is suitable for both Class I and Class II tags, especially Class II tags requiring an encrypted communication channel.

It is observed that an RFID label implementing the C1G2 protocol will scroll out its EPC when queried after being singulated by any transceiver implementing the C1G2 air interface protocol. This unique identity carried by the RFID label poses various security threats and privacy violations illuminated in Chapter 6 of this book.

Two methods to achieve anonymity and untraceability, the use of pseudonyms and re-encryption, are discussed. It is stated that the proposed mechanisms are able to satisfy a majority of the security objectives and all of the privacy objectives considered necessary in Chapter 6 and outlined in the framework provided in Chapter 8.

The use of random tag identifiers provides anonymity by altering the tag response to a query command and thus never transmitting a predictable response. It is shown that a mobile adversary who may be passive or malicious and who is able to collect all the relevant information still has the task of breaking the stream cipher given only the ciphertext.

It is noted that the chapter has outlined a scheme for providing anonymity and untraceability, and separately outlined methods of authentication. A scheme aimed at combining the previous solutions to provide, in addition, a product authentication service is then described. The proposal introduces the concept of an electronic maker. Each tag attached to a product will contain an Electronic Product Authentication Code (EPAC) with the various data fields: (i) Product Identifier, (ii) Product Signature; (iii) Signature Calculation Method; and (iv) Signature Verification Key. An evaluation of the product authentication mechanism defined here is provided.

In its conclusions the chapter states that it has used lightweight hardware and lightweight protocols to address various vulnerabilities identified in Chapter 6, as strong cryptographic solutions are too area or power hungry to satisfy the limitations of RFID systems, and much of the encryption hardware available for smart card technology is therefore inapplicable.

Networked RFID Systems and Lightweight Cryptography

Raising Barriers to Product Counterfeiting

Cole, P.H.; Ranasinghe, D.C. (Eds.)

2008, VIII, 355 p., Hardcover

ISBN: 978-3-540-71640-2