

Preface

Radio frequency identification (RFID) is a type of automatic identification systems which has gained popularity in recent years for being fast and reliable in keeping track of the individual objects. In RFID systems, contactless object identification is achieved using radio signals without the need for physical contact as the case with other existing identification technologies such as barcodes. Therefore, a huge number of items can be identified in a short amount of time with high reliability and low cost which makes the RFID technology very attractive for a wide range of applications such as supply chain management, e-health, monitoring humans, pets, animals, and many other objects, toll control, and electrical tagging. Furthermore, RFID technology eliminates the human error and reduces the total cost of the products.

An RFID system typically consists of three main components: A transponder or tag which is implanted on the objects to be identified and stores the objects' identification information such as the object's identification (ID) number, the manufacturer name, and the product type; a transceiver or reader which provides an electromagnetic field in order to activate the tags and read their data through radio frequency waves; and a back-end server which receives and processes the data from readers.

Out of the three main components of RFID systems, tags have the more stringent implementation limitations. In general, there exists three types of tags: passive, semi-passive, and active tags. Active and semi-passive tags are equipped with their own batteries whereas passive tags rely on the radio frequency energy obtained from the reader. Compared to active and semi-passive tags, passive tags have longer lifetime and are smaller and lighter. However, their signal range is shorter than active tags. Passive tag systems are severely constrained in terms of chip area and power consumption as they do not have internal power source. This book focuses on the severely resource-limited passive RFID tags.

Unfortunately, RFID systems face several challenges in their quest to ensure the reliability of the system, quality of service, or reduced system cost. One challenge is the lack of global standardization. As a result of the existing numerous RFID applications, there are many standards for RFID systems. Each standard is designed

to fit a specific category of applications. This creates a problem in integrating several RFID systems with each other and makes the manufacturing process harder. Another challenge is maintaining the tag cost as low as possible to contribute in reducing the total cost of the product. However, security is one of the biggest challenges that face any RFID systems. The RFID technology is vulnerable to security attacks by unauthorized reader(s) which can interrogate or modify the information stored in the tags. Due to the limited available resources in RFID tags, providing privacy and security for RFID systems is more challenging than other traditional communication systems. This book is devoted for the security of RFID systems.

RFID security threats are categorized into two main groups: privacy violation attacks and security violation attacks. In privacy violation attacks, the attacker tries to harvest the information stored in the objects by eavesdropping on the communications between the objects and the reader or by tracking them. In security violation attacks, an adversary counterfeits the behaviors of legitimate tags or readers for making undesirable effects such as denial of service. Therefore, it is a necessity to develop mechanisms that provide privacy and security of the communications in RFID systems. This can be achieved via physical privacy protection solution, via authentication, or via cryptography.

Several RFID security physical solutions have been developed such as killing tags, blocking tags, Faraday cages, and active interference. Each of these methods has its pros and cons. For instance, killing a tag will cause the tag to lose its functionality, and hence, it cannot be reactivated. Thus, such a solution considerably reduces the lifetime of tags. Meanwhile, in the blocking tag approach, the attacker cannot have access to tags just in a defined range. Beyond this range, tags are not protected from attacks. In Faraday cage solutions, a wrapper shields the tag from the radio waves which imposes another cost to the system. Unauthorized readers are impeded to have communications with tags in active interference privacy protection solutions. However, sometimes some legal readers get blocked as well in the process. Based on the limitations and disadvantages of the physical security solutions stated above, such methods are only applicable for some specific applications.

Authentication is a process through which an object proves its claimed identity to another communication party by providing some evidence such as what it knows, what it has, or what it is. This process is applicable through only software solutions and it is not possible by physical solutions. In RFID systems, authentication is required in two phases. First, before beginning any communication, both the tag and the reader should verify their identity to make sure that they are contacting with the wished partner. The second phase is when data is exchanged between the two parties to ensure that the exchanged data is intact.

Cryptography solutions keep the communication between two parties private in the presence of third parties. An encryption scheme is composed of five components: a plaintext, an encryption algorithm, a secret key, a ciphertext, and a decryption algorithm. Several encryption solutions have been developed for wireless communication systems to address such security challenges. On one hand, there exist several asymmetric or public key encryption algorithms that use two keys

to secure data in networked systems. However, such solutions are not applicable to RFID systems—despite their high security performance—due to the limited processing and power capabilities of the RFID tags. Even existing highly optimized hardware implementation of such algorithms is way beyond what a typical RFID system can afford, such as the hardware implementation of Rabin cryptosystem which offers the best compromises between speed, area, and power consumption. Hence, RFID encryption algorithms must be light enough in terms of area and power to satisfy the resource limitations of RFID systems. Likewise, using hash functions is not suitable for constrained environments since they require significant amounts of resources in their designs, and hence, they are not hardware friendly. On the other hand, several symmetric or private key encryption algorithms have been developed, which are less resource hungry compared to public key encryption algorithms. Even though private key security algorithms promise reasonable security and meet the low resource requirements of RFID systems, they are required to be integrated with other algorithms, such as message authentication code (MAC) algorithms, in order to provide the targeted authentication and integrity services.

In this book, after presenting the RFID security preliminaries, we present the redundant bit security (RBS) lightweight symmetric encryption approach which is suitable for RFID resource-constrained applications. In RBS, the message is intentionally manipulated by distributing redundant bits among plaintext bits, and the location of the redundant bits inside the transmitted data represents the secret key between the sender and the receiver. Meanwhile, there is a relationship between the plaintext data and the redundant data in the RBS algorithm. These redundant bits are generated by a MAC algorithm whose input is the plaintext data. Therefore, these redundant bits can be used for authenticating the message as well. The security level of the RBS approach is adjustable through the number of redundant bits. In other words, there is a dependency between the provided security and the authentication part of the system which distinguishes the RBS algorithm from other existing algorithms. To have flexibility in the number of redundant bits, the implemented MAC algorithm generates variable length outputs. In addition to the number of redundant bits, their values and their positions in the ciphertext are also determining factors in the security of the generated ciphertext. Furthermore, some plaintext bits are also altered based on the value of the encryption key and the redundant bits in order to make the generated ciphertext more secure against attacks. The security of the algorithm is analyzed against existing well-known attacks such as known plaintext, known ciphertext, chosen plaintext, and differential attacks. Experimental and simulation results confirm that the RBS implementation requires less power and area overhead compared to other known symmetric algorithms proposed for RFID systems, especially when the authentication is essential as in harsh operating environments.

RFID Security: A Lightweight Paradigm targets a wide range of readers including but not limited to researchers, industry experts, and graduate students. This book presents the fundamental principles of RFID cryptography that the interested reader will be able to glean information not only to incorporate into his/her own particular RFID security design problem, but also most of all to experience an

enjoyable and relatively effortless reading, providing the reader with intellectual stimulation. This book also offers the reader a range of interesting topics portraying the current state of the art in RFID technologies and how it can be integrated with today's Internet of Things (IoT) vision. Readers with theoretical interests will experience an unprecedented treatment of RFID security that takes into account the practical limitations of today's technologies. Meanwhile, readers interested in real-life RFID security implementations will be exposed to a first-of-its-kind lightweight implementation that results in a significant multi-faced performance improvement compared to existing cryptosystems. In simple terms, while several existing RFID cryptography solutions have been developed, they are challenged by the inherent constraints of practical implementation. Analyzing these constraints and proposing an attractive and practical solution to counter these limitations are the basic aims of this book.

Cairo, Egypt
Santa Clara, CA, USA
Santa Clara, CA, USA
Lafayette, LA, USA

Ahmed Khattab
Zahra Jeddi
Esmail Amini
Magdy Bayoumi

RFID Security

A Lightweight Paradigm

Khattab, A.; Jeddi, Z.; Amini, E.; Bayoumi, M.

2017, XXII, 171 p. 80 illus., 61 illus. in color., Hardcover

ISBN: 978-3-319-47544-8