Chapter 5
An Overview of Cryptography

Ehsan Vahedi
University of British Columbia, Canada

Vincent W.S. Wong
University of British Columbia, Canada

Ian F. Blake
University of British Columbia, Canada

ABSTRACT

As Radio Frequency Identification (RFID) devices become ever more ubiquitous it is very likely that demands on them to provide certain types of security such as authentication, confidentiality, and privacy and encryption for security, depending on the application, will increase. This chapter gives a brief overview of cryptographic techniques and protocols. Given the often limited complexity and power of RFID devices, much effort has been devoted to devising so-called "lightweight" cryptographic techniques for such devices, and a few of these are considered in this chapter. Even public key techniques to provide services such as identification and digital signatures have been proposed for some scenarios involving RFID devices, although such devices will obviously require significant computing power. While such applications are seemingly beyond currently available technology, given the speed at which technology is able to yield computational increases at reasonable cost and device size, it seems prudent to consider such protocols at this point.

INTRODUCTION

Radio frequency identification (RFID) devices are finding ever increasing applications, a trend that is likely to grow in the years ahead. Such devices vary in complexity from a few gates for such applications as grocery item identification, costing a few pennies, to several thousand gates for more sophisticated applications such as passports, costing a few dollars. It is likely that as the number of applications grows, the need for some form of security for many of them will become important. If past experience is a guide, it is also likely that the cost of these devices will decrease and their complexity/capabilities will increase.

Thus the problem of devising suitable cryptographic algorithms for these devices has been widely considered. Such work often goes under

DOI: 10.4018/978-1-4666-4707-7.ch005

the name of *lightweight cryptography*, meaning the investigation of techniques to lower the number of gates required on the RFID chips to implement variations of standard algorithms while not sacrificing too much in the way of algorithm security. The purpose of this chapter is to provide a very brief overview of those cryptographic techniques that seem likely to find application in such efforts. A few of the more promising results on lightweight cryptography are then discussed.

The next section gives a brief outline of those results from number theory that are essential for an understanding of cryptographic techniques, especially those of public key cryptography. The following section gives a brief outline of the standard elements of a cryptographic toolkit i.e. the set of cryptographic primitives that are available to a cryptographer to implement security in a given scenario. Virtually all of these algorithms have been incorporated into standards, a subject that will be mentioned again later. These elements include in particular such systems as stream and block ciphers as well as hash functions. A discussion of one-way functions then follows. These are the standard functions that are easy to compute but computationally infeasible to invert and include the standard functions of discrete logarithm and integer factorization. The notion of public key systems that use the one-way functions are introduced, followed by a description of certain standard cryptographic protocols that are likely to be useful in situations involving RFID devices. Of course the more sophisticated protocols will require a higher gate count and hence be applicable only for the high end applications. These last two sections are included as much for providing a standard notation as providing a framework for the next sections on lightweight cryptography. The chapter concludes with comments on the future research possibilities for these interesting devices.

Throughout the chapter extensive use has been made of two important sources. The first is the website of the National Institute of Standards and Technology (NIST), the arm of the US government that is concerned with providing security services and specifying standards for those communicating with any of its agencies. NIST has been providing an invaluable service in establishing national cryptographic standards, through their Federal Information Processing Standards (FIPS) publications, that have invariably been adopted by other countries around the world. The standards go through a rigorous process of evaluation by other government services and open discussion. As noted, virtually all of the important primitives and protocols have been included in these standards and these will be noted when discussed. In addition they are eminently readable documents providing essential reading for cryptographers.

The other important source for this work is the book (Menezes et al., 1996), a remarkable work that has provided researchers and practitioners alike an invaluable source for cryptographic theory and implementations. It will be referred to frequently as needed.

NUMBER THEORETIC PRELIMINARIES

The notion of public key cryptography relies very heavily on certain number theoretic ideas. It is beyond the scope of this chapter to present these in detail. A brief overview of the necessary facts is given, without any proofs, in the hope the reader will be able to appreciate the basic ideas behind the concepts and how they relate to the cryptographic systems described later, as well as their potential value to RFID systems. This is of course a tall task since it amounts to a review of public key cryptography. More complete treatments of the material are given in many books (e.g. Menezes et al., 1996; Hoffstein et al., 2008; Katz et al., 2008; Smart, 2003; Stinson, 1995). Much material is omitted.