Chapter 63
Recent Developments in Cryptography: A Survey

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

The field of cryptography has seen enormous changes ever since the invention of Public Key Cryptography by Diffie and Hellman. The algorithms for complex problems like integer factorization, Discrete Logarithms and Elliptic Curve Discrete Logarithms have improved tremendously making way for attackers to crack cryptosystems previously thought were unsolvable. Newer Methods have also been invented like Lattice based cryptography, Code based cryptography, Hash based cryptography and Multivariate cryptography. With the invention of newer public Key cryptosystems, the signature systems making use of public key signatures have enabled authentication of individuals based on public keys. The Key Distribution mechanisms including the Key Exchange protocols and Public Key infrastructure have contributed to the development of algorithms in this area. This chapter also surveys the developments in the area of identity Based Cryptography, Group Based Cryptography and Chaos Based Cryptography.

INTRODUCTION

The field of cryptography was characterized initially by the development of Classical Cryptosystems and later by the development of Symmetric Key Cryptosystems and Public Key Cryptosystems. The invention of Public Key Cryptosystems led to the development of number of Public Key algorithms with varying degrees of complexity and strength. While the Symmetric Key Cryptosystems and the Public Key Cryptosystems focussed on the security property of Confidentiality, the development of Hash algorithms focused on achieving Integrity of data. The invention of Public Key Cryptography also led to the use of Digital Signatures which provided a very important property of non-repudiation by combining the use of private keys and hash algorithms.

DOI: 10.4018/978-1-5225-5634-3.ch063

While there are a number of algorithms that exist that can perform encryption using public and private keys, it would be of interest to the researchers to develop algorithms based on different principles since they can provide a platform with which we can compare the performance of different algorithms and also we can choose from a variety of algorithms based on the nature of application in use. The public key encryption algorithms are usually based on a mathematically hard and computationally difficult problem. In this chapter, a survey of the developments that have taken place in Cryptography ever since the invention of public Key Cryptography by Diffie and Hellman (Diffie, et.al.,1976) is presented. There are many important classes of cryptographic systems beyond RSA (Diffie, 1988) and DSA (Kerry, et.al., 2013) and ECDSA (Hoffman, 2012). They are:

- **Hash Based Cryptography:** The classic example is Merkle's hash-tree public-key signature system (Merkle., 1989).
- **Code Based Cryptography:** The classic example is McEliece's hidden Goppa-code public-key encryption system (McEliece, 1978).
- **Lattice Based Cryptography:** The example that has attracted the most interest is the Hoffstein–Pipher–Silverman "NTRU" public-key-encryption system (Hoffstein et.al., 1988).
- **Multivariate Quadratic Equations Cryptography:** An example is the "Hidden Field Equations" by Patarin (1986).
- **Identity Based Cryptography:** A type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address. An example is the scheme proposed by Adi Shamir (Shamir, A.,1984).
- **Group Based Cryptography:** Based on use of Groups for constructing cryptographic primitives. An example is the public key cryptography which is based on the hardness of the word problem (Magyarik et.al, 1985).
- **Chaos Based Cryptography:** The application of the mathematical chaos theory to the practice of cryptography.

Here we look at each of the above classes of Cryptography and how they affect research and developments in the area of cryptography.

HASH BASED CRYPTOGRAPHY

Hash-based digital signature schemes use a cryptographic hash function like any other digital signature schemes. Their security relies on the collision resistance of that hash function. The existence of collision resistant hash functions can be viewed as a minimum requirement for the existence of a digital signature scheme that can sign many documents with one private key. Each new cryptographic hash function yields a new hash-based signature scheme. Hence, the construction of secure signature schemes is independent of hard algorithmic problems in number theory or algebra. The hash based signature schemes depend only symmetric cryptography. Hash Based signature schemes were invented by Ralph Merkle (1989). Merkle started from one-time signature schemes, in particular that of Lamport and Diffie (Lamport, 1979).

One-time signature schemes are really the most fundamental type of digital signature schemes. However, they have a severe disadvantage. One key-pair consisting of a secret signature key and a public