Chapter 6
Post-Quantum Lattice-Based Cryptography: A Quantum-Resistant Cryptosystem

Aarti Dadheech
Institute of Technology, Nirma University, India

ABSTRACT

Quantum cryptography is a branch of cryptography that is a mixture of quantum mechanics and classical cryptography. The study of quantum cryptography is to design cryptographic algorithms and protocols that are against quantum computing attacks. In this chapter, the authors focus on analyzing characteristics of the quantum-proof cryptosystem and its applications in the future internet. Lattice-based cryptography provides a much stronger belief of security, in that the average-case of certain problems is equivalent to the worst-case of those problems. With the increase in cryptanalytic attacks conventional cryptographic schemes will soon become obsolete. As the reality of quantum computing approaches, these cryptosystems will need to be replaced with efficient quantum-resistant cryptosystems. We need an alternate security mechanism which is as hard as the existing number theoretic approaches. In this chapter, the authors discuss the security dimension of lattice-based cryptography whose strength lies in the hardness of lattice problems and also study its application areas.

INTRODUCTION

For a long history, we always tend to seek a safe way to exchange messages between each other, and prevent the others from gaining uninvited access to confidential information. Many mechanisms have been invented for this purpose in different time period. Historically, the study of cryptography focused on the design of systems that provide secret communication over an insecure channel. For example, people in Egypt's Old Kingdom carved non-standard scripts into stones to keep messages secure.

Recently, individuals, corporations, and governments have started to demand privacy, integrity, authenticity, and reliability in all sorts of communication, from e-commerce to discussions of national secrets. Therefore, the need for secure commercial and private communication has been led by the In-

DOI: 10.4018/978-1-7998-6677-0.ch006

formation age, which began in 1980s. Mathematical cryptography secretly used after World War I, when cryptosystems were widely used between armies. One of the most famous cryptosystem that influenced the world is the Germany's Enigma during the World War II. Cryptography has been an area of complex mathematical study for centuries that analyzes protocols that prevent third parties from reading private messages. Now, cryptography might better be defined as the design of systems that need to withstand any malicious attempts to abuse them.

A mechanism that exchanges information secretly is called a Cryptosystem. Such systems consist of two main algorithms: an encryption algorithm, which allows one entity to encode or "scramble" data, and a decryption algorithm, which allows another entity to decode or "unscramble" data. Each of these algorithms has an input called a key, which dictates some aspect of the algorithm's behavior. Before 1975, all cryptosystems are the Symmetric Cryptography, which required the sender and the receiver to agree on the same secret key. The Enigma Machine, for example, is a symmetric cryptography. In 1977, Rivest, Shamir and Adleman introduced to public the RSA Public Key cryptosystem, which was the first time that the concept of Public Key Cryptography (Diffie & Hellman,1976) circulated in the research community. In this cryptosystem sender and receiver uses two different keys; one for encryption and one for decryption. It solves the key distribution and scalability problems associated with symmetric systems. After the RSA cryptosystem, many Public key Cryptography were proposed, for example, the ElGamal Cryptosystem, the ECC Cryptosystem, and the GGH Cryptosystem and so on. Most common algorithms like RSA and Diffie Hellman key exchange scheme are computationally secured schemes and are based on the hard problem of factorizing a large number and solving the discrete logarithm problem respectively but with the invention of Shor's algorithm, it would solve both these hard problems in polynomial time using quantum computers, if built. A quantum computer making use of large qubit registers that can put the RSA and DH algorithms out of practice as theoretically, Shor's algorithm (Bernstein et al., 2009) with large number of quantum gates of quantum computer can solve the factorization problem in $\log N^3$ time approximately which is a polynomial factor. This would put the entire internet domain at risk along with usage of user data at major risk. As the reality of quantum computing approaches, these cryptosystems will need to be replaced with efficient quantum-resistant cryptosystems.

There are important classes of algorithms which are considered to be quantum attack resistant based on the underlying problems.

- **Hash-based cryptography**; based on one-way functions that map bit-strings of an arbitrary length to short fixed-length bit strings. It is based on the usage of hash trees coupled with one time signature schemes
- **Code-based cryptography**; based on error-correction codes to detect and correct bit errors when messages are transmitted over an unreliable channel,
- **Lattice-based cryptography**; based on high dimensional lattices and presumed hardness of lattice problems
- **Multivariate quadratic (MQ) cryptography**; based on solving multivariate (many unknown variables) quadratic equations over the finite field (large quadratic tuples, cyclic rings, etc.) is NP-hard. This has been one of the most recently developed classes of algorithm.

Lattice-Based cryptography is one of the most important classes. There are problems based on lattices that are NP-hard and have no known efficient quantum solutions, unlike both the integer-factorization and discrete logarithm problems that have known quantum solutions. Hence there are two motivations